DOCTORAL SCHOOL
UNIVERSITA' *MEDITERRANEA* DI REGGIO CALABRIA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE, DELLE INFRASTRUTTURE E DELL'ENERGIA SOSTENIBILE (DIIES)

PHD IN
INFORMATION ENGINEERING

S.S.D. ING-INF/03
XXXIV CICLO

Network Security: A Buzzword in the Revolution Process towards 6G

CANDIDATE
Chiara Francesca SURACI

ADVISOR
Prof. Giuseppe ARANITI

COORDINATOR
Prof. Tommaso ISERNIA

REGGIO CALABRIA, APRIL 2022

Finito di stampare nel mese di **Aprile 2022**

Edizione 

Quaderno N. 55
Collana *Quaderni del Dottorato di Ricerca in Ingegneria dell'Informazione*
Curatore *Prof. Tommaso Isernia*

ISBN 9788899352653

Università degli Studi *Mediterranea* di Reggio Calabria
Salita Melissari, Feo di Vito, Reggio Calabria

CHIARA FRANCESCA SURACI

NETWORK SECURITY: A BUZZWORD IN THE REVOLUTION PROCESS TOWARDS 6G

The Teaching Staff of the PhD course in
INFORMATION ENGINEERING
consists of:

Tommaso ISERNIA (coordinator)
Pier Luigi ANTONUCCI
Giuseppe ARANITI
Francesco BUCCAFURRI
Salvatore COCO
Giuseppe COPPOLA
Mariantonia COTRONEI
Lorenzo CROCCO
Dominique DALLET
Claudio DE CAPUA
Francesco DELLA CORTE
Giuliana FAGGIO
Fabio FILIANOTI
Patrizia FRONTERA
Sofia GIUFFRE'
Giorgio GRADITI
Voicu GROZA
Antonio IERA
Gianluca LAX
Aime' LAY EKUAKILLE
Giacomo MESSINA
Antonella MOLINARO
Andrea Francesco MORABITO
Giacomo MORABITO
Rosario MORELLO
Domenico ROSACI
Giuseppe RUGGERI
Mariateresa RUSSO

Abstract

The evolution of mobile networks has now reached the gates of the Sixth Generation (6G) and, together with the continuous boost required in terms of latency and data rate, security has also become a fundamental requirement to meet for the optimization of the quality of the services offered to users. Guaranteeing the security of different applications requires the implementation of different mechanisms and countermeasures, therefore, this thesis has the purpose of introducing suitable security solutions for the protection of communications established in different scenarios and use cases. Starting with a general security analysis for virtualized 5G environments, this work, then, proposes the implementation of security mechanisms for the protection of Device-To-Device (D2D) communications established with the aim of improving the performance of multicast transmissions in 5G networks. The same goal is to be achieved through the subsequent proposal of an innovative trustworthiness model for evaluating the reputation of the network nodes based on both the information obtained from the behaviour that the node exhibited in the network and the specific characteristics of the node. A protocol for the management of massive Machine Type Communications (mMTC) among Internet of Things (IoT) devices in 5G networks is also introduced in this thesis work, evaluating the advantages offered in terms of energy consumption to resource-constrained IoT devices. Finally, the problem of the security in 6G-oriented networks deployed in support of a use case of paramount importance for 6G and for the current times is addressed, through the proposal of a lightweight authentication protocol suitable for Internet of Medical Things (IoMT) devices employed in the transmission of extremely sensitive health data. Furthermore, a brief digression on the phenomenon of the Digital Divide highlights the importance that this has reached, to date, particularly revealed following the need for digitization required to numerous sectors due to the spread of COVID-19, and how the advent of the next generation of mobile networks could help reduce the gap between those who have access to the digital world and those who have not.

Italian Abstract

L'evoluzione delle reti mobili ha ormai raggiunto le porte della Sesta Generazione (6G) e, insieme al continuo miglioramento richiesto in termini di latenza e velocità, anche la sicurezza è diventata un requisito fondamentale da soddisfare per l'ottimizzazione della qualità dei servizi offerti agli utenti. Garantire la sicurezza di diverse applicazioni richiede l'implementazione di diversi meccanismi e contromisure, pertanto, questa tesi ha lo scopo di introdurre soluzioni di sicurezza adeguate alla protezione delle comunicazioni stabilite in diversi scenari e casi d'uso. Cominciando con un'analisi di sicurezza generale per ambienti 5G virtualizzati, questo lavoro propone, poi, l'implementazione di meccanismi di sicurezza per la protezione di comunicazioni Device-To-Device (D2D) stabilite con lo scopo di migliorare le performance di trasmissioni multicast in reti 5G. Lo stesso obiettivo si vuole raggiungere anche attraverso la successiva proposta di un modello di trustworthiness innovativo in grado di valutare la reputazione dei nodi della rete sulla base sia di informazioni ottenute dal comportamento che il nodo ha esibito nella rete sia da caratteristiche specifiche del nodo. In questo lavoro di tesi viene anche introdotto un protocollo per la gestione di massive Machine Type Communications (mMTC) tra dispositivi dell'Internet of Things (IoT) in reti 5G, valutando i vantaggi offerti in termini di consumo energetico ai dispositivi IoT resource-constrained. Infine, viene affrontato il problema della sicurezza in reti 6G-oriented impiegate a supporto di un caso d'uso fondamentale per il 6G e per i tempi attuali, attraverso la proposta di un protocollo di autenticazione lightweight adatto a dispositivi dell'Internet of Medical Things (IoMT) impiegati nella trasmissione di dati sanitari estremamente sensibili. Inoltre, una breve digressione sul fenomeno del Divario Digitale mette in luce l'importanza che questo ha raggiunto, ad oggi, rivelata soprattutto in seguito alla necessità di digitalizzazione richiesta a numerosi settori a causa della diffusione del COVID-19, e come l'avvento della prossima generazione di reti mobili potrebbe contribuire a ridurre il divario tra chi ha accesso al mondo digitale e chi no.

Dedicated to my family, my safe haven

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Telecommunications networks are increasingly pervasive. Several reports show how quickly the data relating to connectivity to mobile networks constantly grows, to reflect the fact that by now they have taken the world by storm. According to the publisher of [1], the speed at which Fifth Generation (5G) is spreading around the world is significantly higher than that of Fourth Generation (4G), to say nothing of Third Generation (3G). To be clear, the number of 5G subscribers is estimated to reach 1 billion two years earlier than 4G. COVID-19 partly has contributed to the acceleration that the technological progress is undergoing, in fact, nowadays, connectivity support has become indispensable in various sectors, especially education and health. Despite the countless benefits that Information and Communications Technology (ICT) is bringing to the daily lives of many people, to date, the services that consumers demand from mobile network operators are closely related to the personal sphere and the data that goes across the network can mostly be categorized as sensitive, therefore, there is one aspect of paramount importance that cannot be overlooked: *Network Security*. This thesis work examines the topic of network security from various viewpoints and in different contexts, starting with 5G networks up to the study of a use case of Sixth Generation (6G) networks.

In detail, Chapter 2 includes a security analysis formulated to investigate the vulnerabilities encountered by implementing the main 5G virtualization technologies, i.e., Multi-access Edge Computing (MEC), Software Defined Networking (SDN), Network Function Virtualization (NFV), and network slicing. The definition of the

main stakeholders and business models of 5G networks is provided and, for each analyzed virtualization technology, a risk assessment is provided considering the business models that can be established among the stakeholders possibly involved.

In Chapter 3, a secure and effective solution is provided for improving the performance of multicast transmissions in 5G networks. First of all, one of the major 5G enabling technologies, which is Device-To-Device (D2D), is proposed as a means to efficiently deliver multicast data to network nodes with worst channel conditions and to improve the quality of service offered to all requesting devices. After that, a security protocol is presented which, through the use of existing mechanisms, allows to protect the privacy of the nodes involved in D2D communications and the data exchanged. Given the distributed nature of these communications, in fact, they represent the segment most vulnerable to any security attacks.

A similar scenario is considered in Chapter 4, in which an innovative trustworthiness model is introduced in order to provide a useful way for evaluating candidate nodes to transmit data in D2D communications. The proposal presented in the Chapter has the same goals as that of the previous Chapter 3 that mainly consist in the protection of D2D transmissions from security breaches but, thanks to the trustworthiness model, a preventive measure can be applied, as it allows to select reliable nodes to act as D2D transmitters, in order to avoid any attacks that would compromise the outcome of the multicast transmission.

Chapter 5 focuses on a specific type of 5G network traffic, that is massive Machine Type Communications (mMTC). Also in this Chapter, D2D communications are proposed as an effective solution for improving the performance of a multicast transmission but the scenario considered in this case includes Internet of Things (IoT) devices as data receivers. Mechanisms of security and trust are implemented in an innovative protocol formulated to secure mMTC communications but, in this Chapter, the operations are carried out with the aim of preserving the limited resources of the IoT devices, therefore to optimize their energy consumption.

Chapter 6 differs from the previous ones in that it analyzes the security topic in a 6G-oriented scenario and in the specific use case of eHealth. Given the high sensitivity of health data, a security proposal is presented that includes an archi-

tecture for managing secure communications thanks to the implementation of an innovative authentication protocol. Furthermore, a discussion on the phenomenon of the Digital Divide is debated since the advent of 6G and the spread of COVID-19 represent potential turning points. In fact, while COVID-19 has brought to light the extent of the gap between who have access to digital services and who have not, 6G could represent a solution to the problem thanks to the use of technologies able to facilitate the Internet access for everyone.

The conclusions on the thesis work are elaborated in the Chapter 7.

Chapter 2

A security analysis for 5G systems

Besides significantly outperforming past generations in terms of capacity and throughput, 5G networks and systems will provide an infrastructure for the support of highly diversified services and "verticals". Indeed, the major paradigm shift with respect to previous cellular network generations, specifically oriented to one class of terminals (namely, people's cell phones), is the largely heterogeneous nature of the multiplicity of end systems supported. Within a 5G infrastructure, playing the role of "network of networks", traditionally independent technical and business stakeholders are now called to cooperate in the deployment of crucial infrastructure components relying on innovative (for the Telecom world) technologies such as virtualization, not in the traditional operators' portfolio, and eventually placed in security-critical parts of the network - think e.g. to MEC systems. Goal of this Chapter is to analyze the complex threat landscape of 5G systems, by taking the point of view of the involved stakeholders. The motivation behind this proposed analysis revolves on the observation that, in complex and virtualized systems such as the 5G infrastructure, an attack to a system component under the responsibility of a given stakeholder may yield a dramatic impact to a completely different player. Therefore, while reviewing the many 5G security risks and relevant threats which the main stakeholders operating in virtualized 5G cellular networks are exposed to, the sometimes non-obvious relation between impact and responsibility will be showcased, as well as shared responsibilities will be identified.

2.1 Introduction to Chapter

There is a shared belief in the scientific and industrial community that the ongoing 5G deployment is bringing about two different "flavors" of innovation. One is of course the improvement of the network infrastructure itself, where legacy technologies derived from previous generations of mobile and wireless networks are now enhanced with new features and protocols to achieve previously unthinkable performance targets. But there is also a second factor: while cellular infrastructures until 4G were mainly ruled by Telecom Operator, 5G distinguishes from its predecessors in the not any more marginal involvement of Information Technology / Cloud stakeholders, and their relevant disruptive business models.

From the literature, the concept of virtualization clearly emerges as the main factor that discriminates the new 5G network from what has been developed in the past. In fact, SDN, NFV, Network Slicing, and MEC are identified among the enablers of a major shift from traditional network architecture as they allow: network functions not tied to specialized hardware, a high degree of separation among different service layers on the same physical network, the provision of enhanced functionality at the edge of the network, and a less centralized architecture than in previous generations of mobile networks.

The obvious consequence of the introduction of the cited game-changing paradigms for the provision and consumption of services is the rising of new business models and the flanking of new stakeholders to the old ones. Their coming into play to provide services over the future platforms will expose 5G cellular system to a series of risks that will likely suffer a significant increase in number and intensity.

Along these lines, the European Community has recently released a document, which provides an EU coordinated risk assessment of the cybersecurity of 5G networks [2] and identifies the main 5G stakeholders that will play a key role in terms of security, both as contributors to the cybersecurity of 5G infrastructures and as potential entry points or vectors for attacks.

The document provides a thorough list of possible threats and related involved actors. Several "external" actors are considered, ranging from individual hackers to

organized crime groups, state actors or state-backed actors [2]. Reported motivations to threats are manifold: accidental (events that result from human error, natural phenomena, and systems failures), criminal (motivated by financial gain), political (finalized to distribute propaganda), or economic (gaining competitive advantage in the technological area through Intellectual Property theft).

In such a complex ecosystem, substantially different from the one characterizing previous generations of cellular networks, also a new model of trust among the "internal" stakeholders must be defined to protect the privacy of their data and of the customers' data. This trust model for 5G will be more complicated than the current one, since new actors must be considered. As an example, the authors of [3] highlight that a trust relationship need to be established between the Hardware and Software Vendors and the 5G Infrastructure Provider (InP). Vendors and InPs must guarantee assets which are anomaly-resistant and vulnerability-free, and, at the same time, they have to respect the trust that a Mobile Service Provider (MSP) places on it, by guaranteeing honesty in the treatment of the information that the provider processes on the infrastructure. According to the model in [4] a mutual trust relationship exists between Subscribers and Service Provider (SP), as the users count that the SP undertakes to offer them the requested services and to respect the rules of the subscription contract; in turn, the SP relies on the fact that Subscribers pay the due billing price. In some cases, the relationships between the actors may be characterized by a non-blind trust, in the sense that some stakeholders may have the possibility to verify the validity of the received asset (e.g., in the case of open-source software supply)

It is therefore undeniable that in 5G cellular systems each stakeholder will have different levels of involvement in various security threats, both as a victim of threats and as the entity that will have to take responsibility in contrasting the threats. It is easy to hypothesize that the resulting framework will enable strong interactions among the involved players heavily dependent on the specific business model implemented and on the distribution of the risks and responsibilities.

Based on these considerations, this Chapter gives a thorough description of the key roles of 5G stakeholders and of the new business models, with the twofold ob-

jective of: *(i)* conducting a security risk analysis that addresses the major security threats to virtualized 5G systems and classifies them based on stakeholders' involvement in terms of responsibility and vulnerability; *(ii)* surveying the most common defence measures that can be implemented to face and thwart these threats. In detail, in Section 2.2 the 5G stakeholders and business models are described, while the risk analysis is conducted in Section 2.3 and defence mechanisms are identified in Section 2.4; a discussion on the applicability of the model analyzed in this Chapter to the real world is conducted in Section 2.5. Conclusive remarks are given in Section 2.6.

2.2 Stakeholders and Business Models in 5G

This Section provides a brief overview of the main 5G stakeholders and lists some business models involving them that have been identified in the literature.

2.2.1 5G Stakeholders

The problem of defining all the key players expected to be entailed in 5G ecosystems have been faced by several papers available in the literature [3], [5], [6], [7], by reports of government institutions [2], and by industrial alliances [8]. In particular, an interesting list of 5G actors is provided in [7] wherein the new stakeholders are compared to those of 4G. Despite this, the various documents are sometimes incomplete and not even similar to each other. The Table 2-1 summarizes what is reported in these documents, giving a list of the various stakeholders and briefly describing their roles.

Two important sources of information on the topic are [9] and [10], both written by the 5G Infrastructure Public Private Partnership (5GPPP). In [9], a full list of the main 5G stakeholders is provided along with a brief description of each of them. In particular, this document shows the complexity of the 5G environment and the high number of actors involved, among which several business relationships can be established based on the granularity of the context and on the virtualization levels nested on the network. The concept of nesting different virtualization levels

in networks emerges from [11], where it is stated that network services can include other network services. Authors in [10], describe some possible business roles for the new 5G actors. According to them, the introduction in the 5G value chain of stakeholders from vertical industries, such as healthcare, transportation, automotive, and aeronautics, represents the most important change with respect to 4G. Other prominent differences should be highlighted. First of all, although the role of the Mobile Network Operator (MNO) in 5G could be quite complex, based on the reported literature, it can be more simply considered as split into InP and MSP roles, which means that anyone owns the network infrastructure (i.e., the InP) is not always the same entity that provides mobile services to consumers (i.e., the MSP). Notwithstanding, from the Tenant's viewpoint, the MNO is the only significant entity, as it combines the two parties of MSP and InP, making the distinction between the two roles transparent for the Tenant. Another aspect that is worth considering for the purposes of a complete research on security threats, concerns the Tenant's role towards its users or Subscribers. The Tenant can be seen as a service provider by its Subscribers, since it acquires the virtual network services to make them available to its users. Thus, Subscribers are the final users of the services offered by the MSP and the Tenant acts as an intermediary in the delivery of MSP services to users. It can be considered as the entity that represents the needs of its users; not by chance, the Tenant is the customer accounted for in the design of the services that the network shall offer.

The model that will be used as a reference for the security analysis is based on the three main players, namely MNO (sometimes split into InP and MSP), Tenant, and Subscriber, and on the specific role that they will play in 5G networks, wherein the network virtualization technologies will take on an increasingly important role. Obviously, this is a simplified model that, however, allows to clearly provide indications on how to approach the security problem in a 5G environment. The three-player abstraction allows to keep the complexity of the risk analysis at a low level without losing generality in addressing the major security threats and stakeholders' involvement, responsibility, and vulnerability in reference to the main technologies used in virtualized 5G systems.

Stakeholder	Description
Hardware and Software Vendors / Telecom Equipment Manufactures	They are responsible for the hardware and software resources that compose the network infrastructure
Infrastructure Provider (InP) / Supplier of Mobile Network Operator (MNO)	The InP is the owner, in whole or in part, of the network infrastructure, and makes its assets available "as a service"
Mobile Service Provider (MSP)	The MSP exploits the resources offered by one or more InPs to offer telecommunications services to Tenants
Mobile Network Operator (MNO)	The MNO operates its mobile network infrastructure to provide connectivity to end-users; it merges the roles of MSP and InP
Tenant	The Tenant is service provider for its Subscribers, since it acquires the virtual network services to make them available to its users
Service Provider (SP)	A Service Provider is the entity that offers services to consumers. This role can be played by several entities, such as the MNO, the MSP, the Software Network Function Providers, the IT-SP (IT Service Provider), the NSP (Network Service Provider), the CSP (Communication Service Provider), the OSP (Online Service Provider)
Developers	They can develop software for the creation of applications for different stakeholders (e.g., network functions for MNOs, applications directed to consumers)
Over-The-Top (OTT)	OTTs could be defined as service providers responsible for providing the most popular multimedia traffic on Internet. Their name indicates that they operate on top of the network. Some examples of OTTs services are YouTube, Netflix, and Facebook
Brokers	They act as intermediaries between the various stakeholders. For example, resource brokers can be mediators between InPs and customers, able to provide the latter with the resources they required according to the negotiated service level agreement (SLA)
Subscriber / End-users	They are the users of mobile services
Others: • Verticals (e.g., Automotive, Healthcare, Energy, Transportation); • Small and Medium Enterprise (SME), Startups ; • Public Administrations and Infrastructure Owners, and Regulatory and Standardization Bodies; • Industry Players (e.g., Standard Developing Organizations (SDOs), Certification Bodies); • User Equipment Manufacturer.	They can benefit from 5G services or participate in their development

Figure 2-1: The 5G stakeholders

2.2.2 5G Business Models

According to [12] a Business Model (BM) can basically be defined as a paradigm for the representation of the business dynamics established between an organization and its customers in the supply of services. Several business models have been described in the literature involving technologies that are significant for 5G ecosystems. As an example, in [13] authors classify business models according to the provided resources. First of all, different business models may arise by differentiating the *connectivity* service offered to the diverse applications. With the *Data-as-a-Service* BM the network operator can provide data produced in its network to traffic, logistical, and manufacturing systems with the aim of improving their productive processes. Another noteworthy business model is the *Network-as-a-Service (NaaS)*, through which operators can offer virtual networks to various service providers. This model fosters the development of multi-tenancy, thanks to which different Tenants operating in various vertical markets can exploit the virtual network created ad-hoc for them by the operator while sharing the same physical network infrastructure.

With reference to network slicing, the authors of [14] address the business models enabled by the Network Slicing as Service (NSaaS) model. Three options are identified depending on the relationship between service provider and consumers: *Business to Business (B2B)*, *Business to Consumer (B2C)*, and *Business to Business to Consumer (B2B2C)*. As it will be explained later, the choice of BM configuration can have impact on the security of the involved stakeholders.

The role of a new stakeholder, that is the micro operator for 5G mobile networks, is presented in [12] together with the description of three business models promoted by it in order to complement the classic models centered on the offers of the MNO. In the *Vertical BM*, the micro operator provides tailored services in limited areas; in this case, the role of the micro operator could be performed by different actors, such as an MNO, a network constructor, or a factory owner. With the *Horizontal BM*, the micro operator locally hosts the services of an MNO, thus extending its connectivity and ensuring the service continuity in its network; in the business ecosystem of this model the main actor is the MNO. Finally, with the *Oblique BM*, the micro operator can establish diverse collaboration to deliver local mass services.

In [8], the new business models expected to be supported by 5G are outlined and classified into three groups, based on the type of offered service. According to the authors, the next generation of cellular networks will open up to new customers and partnerships, reason why new business models are waited. According to the *Asset Provider* BM, the involved actors establish relationships based on the services of Anything as a Service (XaaS) and Network Sharing. Infrastructure is the main asset of a network operator and, based on the different components that the operator offers to third party, different models can be identified. Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) can all be generically identified as XaaS and concern the supply by the operator of parts of its infrastructure as network capabilities to third party. With Network Sharing, two or more operators can share the same network infrastructure, according to static or dynamic policies. Within the *Connectivity Provider* group, two options can be possibly offered: Basic or Enhanced Connectivity. The former is equal to the 4G business model of providing the best effort IP connection to consumers. Rather, the latter adds something more to the offer, allowing to differentiate some characteristics of the connectivity (e.g., Quality of Service (QoS), latency) and admitting configuration options to consumers. The last group of business models is the *Partner Service Provider*, which comprises Operator Offer Enriched by Partner and Partner Offer Enriched by Operator. According to the first option, operators offer services enriched thanks to collaborations with external partners. In the second case, the partners offer services improved by the capabilities exposed by the network operators.

The categories introduced in [8] are well described in a table realized by the authors and will be referred to in the remainder of the paper, when identifying the kind of business relationships established between the examined stakeholders.

2.3 Risk analysis

This Section identifies the main security risks that may affect the key virtualization technologies employed in 5G cellular networks, namely MEC, SDN, NFV, and Network Slicing. A peculiarity of the risk analysis produced in this Chapter is that it is

conducted in order to determine the possible risks for each threatened stakeholder and considering the impact of possible business models on risk distribution.

2.3.1 The main security attacks on virtualized systems

Several types of traditional attacks can exploit the vulnerabilities of the major 5G virtualization technologies. The following list of risks is inspired by the report released by the Cloud Security Alliance (CSA) on the most frequent attacks on Cloud Computing of the last years [15], where each attack is described with an industrial insight.

Data Breaches

This category includes a wide variety of attacks on data security. In any network environment, *data confidentiality* must be ensured to maintain the secrecy of information and *data integrity* has to be protected to prevent malicious attackers from tampering data they should not access. These are the two most important guidelines that should be respected to guarantee the isolation of data, that is critical for network providers,tenants, and users involved in multi-tenant virtualized environments. The relevance of these principles is outlined, for example, in [16] for MEC and in [17] for the network slicing paradigm.

Insufficient Identity, Credential and Access Management

This group includes attacks caused by a misuse of login credentials and a wrong authentication and authorization management. The identity of each consumer is associated with its privileges within a virtualized environment. It is of paramount importance that a service provider traces changes in the role and responsibility of consumers associated with each identity in order to be constantly aware about the authorized actions within the system. In addition, the identity of each entity should not reveal sensitive information about it in order to protect its privacy. Examples of attacks against privacy and authentication which can target virtualized 5G cellular environments are reported in [18]. In [19] authentication and authorization are

identified as two important security challenges in SDN domains.

Insecure Interfaces and Application Program Interfaces (APIs)

Consumers can access and interact with services offered in the virtualized system through the APIs that are easily hackable if not adequately protected. In fact, they are exposed to any external entity, which could abuse its privileges. An attack to APIs could jeopardize the security of the whole network. In fact, in [20], attacks to insecure APIs are classified as network security issues, since they could involve the entire network and its configuration.

System Vulnerabilities

Obviously, also in virtualized digital ecosystems, bugs or flaws in the developed software, can be targeted by attackers. Examples of software vulnerabilities in NFV are reported in [21]; these could be implementation flaws, design flaws, and update or upgrade of software.

Hijacking attacks

As previously said, identity management is crucial in order to assign the proper authorization to each entity within the virtualized system. An attacker can impersonate another entity to obtain its credentials, thus manipulating its behavior. This is what happens when an Account Hijacking is performed. The attacker pretends to be the legitimate owner of data, thus breaching data security and jeopardizing the entity's reputation [22]. Generic Hijacking Attacks may consist of redirecting behavior to certain elements of the network infrastructure. As an example, the problem of SDN Controller and switch hijacking is faced in [23].

Malicious Insiders

Whoever commits a malicious action is not necessarily an outsider to the virtualized system. Accidentally or intentionally, even an insider, such as a system administrator, could behave incorrectly. For example, in [24], two attack scenarios are described

in which an attacker manages to obtain confidential information about a user thanks to some badly implemented virtualization procedures in an NFV context.

Data Loss

This category of attacks concerns the lack of data availability for consumers, which is one of the prominent requirements of 5G virtualized mobile networks. Data Loss can be caused by either intentional attacks or accidental events. In any case, the service provider should store copies of data to bypass or contain the problem. Furthermore, the version of backup has to be controlled and a dynamic adaptation to data updates should be performed by service provider to maintain data integrity [15].

Abuse and Nefarious Use of Services or Resources

In this case, the consumer of services or resources does not behave diligently. It could carry out some attacks that damage not only the provider but also other consumers. According to [15] attacks of this kind often result in denial of services for other consumers in Cloud environment, like the MEC one. In this work, any attack that involves a malicious use of services and resources offered by the service provider is considered to belong to this category.

Denial of Service (DoS)

A malicious consumer could flood some elements of the system with junk requests, thus depriving other consumers of storage, compute or network resources. A good explanation of DoS attacks is reported in [25], where some examples of Distributed DoS (DDoS) are also described, which consist of attacks coming from several hosts handled by one malicious entity. This survey focuses on DDoS attacks that can affect SDN elements.

Shared Technologies Vulnerabilities

The isolation between environments offered to different tenants could have some vulnerabilities. An attack to the hypervisor of the virtualized system, which has the task of managing the mapping between physical and virtual resources, could break

the isolation between multi-tenant environments. Through a *Virtual Machine (VM) Escape*, an attacker could succeed in penetrating the common network infrastructure by breaking the isolation between the host machine and the breached VM; in this way, it could access some central node and execute arbitrary code to manipulate it [24]. Other common attacks that exploit multi-tenant VMs isolation vulnerabilities are the *VM Side Channel attacks*. They are mentioned among the security risks for network slicing in [26]. Finally, isolation between multi-tenant environments can be breached caused by *Outdated VMs* not patched for recent vulnerabilities [20].

2.3.2 Multi-access Edge Computing

The technology

MEC has been standardized by the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) for MEC [27]. Main purpose of ETSI was to introduce an edge computing paradigm to provide Cloud Computing capabilities in the location closest to the end users so as to meet the requirements of 5G mobile networks [28]. As an added value, MEC servers can gather information about users and cell that can be harnessed by application providers to enrich the offer to consumers so that they can enjoy top notch applications. MEC technology uses servers installed at the edge of the network [29]; therefore, the Telco operators are the owners of resources employed [30]. In 2017, ETSI ISG officially changed the name of the paradigm from Mobile Edge Computing to Multi-access Edge Computing in order to open to different communication technologies and non-cellular operators [31].

The risks

Authors in [32] state that, in the general context of Cloud computing, security issues arise both for consumers and providers owing to the outsourcing of the own assets, for the former, and the opening of infrastructure, for the latter. The boundaries of the security checks that each stakeholder can apply throughout the MEC environment depend on the implemented service model. According to [33], MEC

can implement the same service models as those described by National Institute of Standards and Technology (NIST) for Cloud Computing [34]. As a matter of fact, ETSI exposes some Proof of Concepts, developed according to the ETSI ISG MEC Framework, in [35] and many of them are Software as a Service (SaaS) and PaaS implementations. The three MEC service models are represented in Figure 2-2, which illustrates the management boundaries of MNO and Tenant.

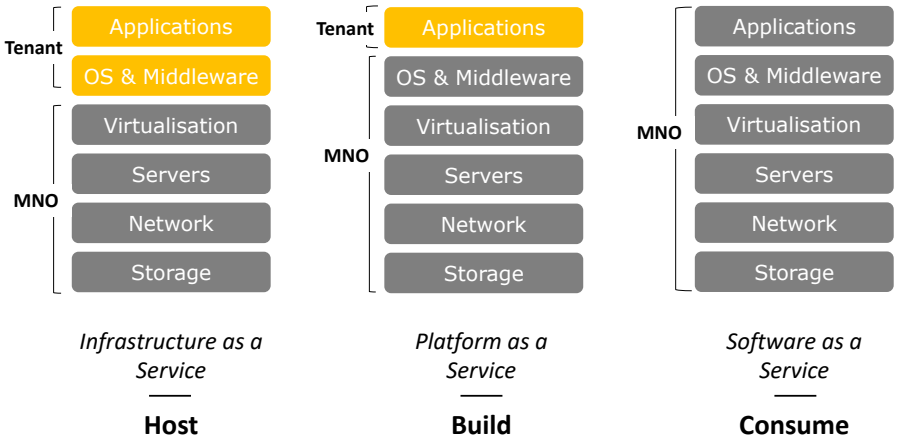


Figure 2-2: MEC service models

In this Section, the MNO is assumed to be the sole MEC service provider, as in [28] [36] [37], and the entity responsible for managing the security of the offered MEC services. Tenants and their Subscribers are considered as consumers. In particular, Tenants are the customers that require network services from the MEC service provider, while the Subscribers use the services delivered by means of the Tenants [30]. In [38], the major state-of-the-art MEC security attacks are described but no emphasis is placed on the 5G actor actually involved in the attack. Below, the main MEC security risks are classified based on the stakeholders involved and the implemented service model. The resulting classification is depicted in Figure 2-3.

SaaS

Through the *SaaS* model, the MNO provides complete software solutions to consumers remotely hosting the entire application stack. The MNO must cater for the most of the risks and it has to implement security measures to protect: applications,

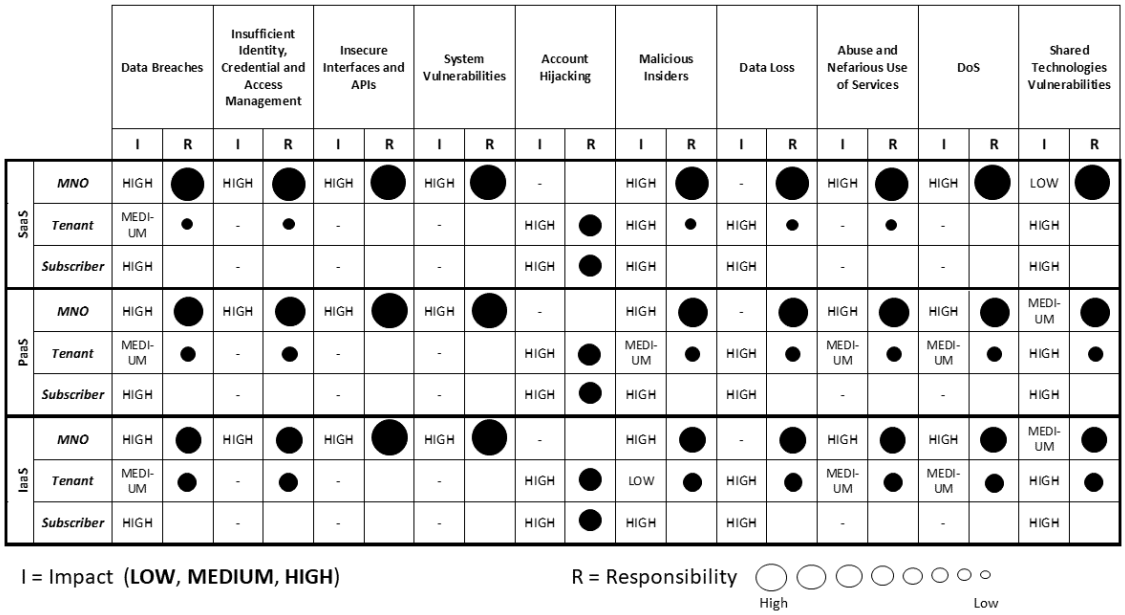


Figure 2-3: Stakeholder-based classification of MEC risks for different service models. I=Impact; R=Responsibility for attacked assets

operating system, virtual resources, and physical infrastructure. The Tenant has no control over the MEC infrastructure and it is only responsible for the security of data. The Subscribers have to rely on the security policies implemented by the Tenant for the protection of their data.

Together with its own data, the MNO stores information on the Tenant and its Subscribers and, thus, it is of paramount importance that strong security measures are applied. It has to put a keen attention to both Data Loss prevention, due to failure or attacks, and to Data Isolation, especially when data belonging to different Tenants share the same MEC server. *Data Breaches* can happen both when a malicious Tenant violates the MNO's data or when the Tenant's data are violated by a malicious or compromised MNO. For its part, the Tenant has to properly safeguard the data of its Subscribers both from other Tenants and from other users.

The MNO must also implement robust *Identity, Credential and Access Management* policies to protect its assets and prevent attacks such as Man-in-the-Middle, whereby an attacker (e.g., a malicious or compromised Tenant) illegitimately accesses the offered service. Obviously, effective mutual authentication mechanisms could help also the Tenant to avoid services provided by malicious MNO. Each Tenant must safely guard its identity and those of its Subscribers.

Malicious insiders in MNO system administration represent a further risk of compromising the MNO reputation [39] and exposing to security risks the Tenant, which may receive compromised services that may violate its data. In SaaS, this threat is much more dangerous than the PaaS and IaaS cases because the MNO has greater control over the network [15]. Similarly, a malicious entity inside the Tenant's system could breach the security of Subscribers.

With SaaS, consumers usually access the offered services through Web Browsers, thus, the MNO has not to overlook vulnerabilities in the offered software and in the used protocols (e.g., HTTP) in order to protect its network from attacks. A typical category of attack is the *Abuse and Nefarious Use of Services*, performed for example by a consumer that executes a Malware Injection attack to the MNO's MEC server profiting from the services offered.

Last but not least, *DoS* attacks represent a threat to the whole MNO's network, as MEC server usually shares the same physical machines with other important network functions that risk starve when a DoS attack to an offered application occurs.

PaaS

PaaS is the model that allows Tenants or third parties to develop their applications over the MEC platform that is provided by the MNO. The supplied platform includes the operating system and the infrastructure necessary for Tenants to build and run their applications. Therefore, the MNO must protect the platform, while Tenants are in charge for defending applications, data, and user access. While Subscribers are susceptible to the same vulnerabilities as for the SaaS model, both Tenants, developing their applications on the PaaS, and MNO are exposed to additional risks.

Being an application developer and no longer an intermediary of the services developed by the MNO, the Tenant must avoid software vulnerabilities to prevent a Subscriber or an attacker from taking advantage of vulnerabilities and making a *Nefarious Use of Services*. The MNO must avoid software flaws in the operating system and in the virtual resources offered to Tenants while guaranteeing them

access to the MEC platform through secure APIs to prevent Malware Injections.

Due to weak isolation among resources of the MEC platform assigned to applications belonging to diverse Tenants, attacks like Side Channel or VM Data Theft may occur. At the same time, the applications running on MEC server and located in different VMs may be developed by non-trusted Tenants; in this case, the MNO's platform can be accessed by an attacker that manages to exploit a *Lack of Isolation* between a vulnerable VM and the host machine.

IaaS

Offering *IaaS*, the MNO leaves to the Tenant the task of deploying its own operating system and applications, thus executing arbitrary software on its infrastructure. In this case the MNO is in charge of protecting its assets, which include data and servers underlying virtual resources offered as MEC services. The Tenants have to face the security assurance for access, data, applications, and operating systems. The MNO may be victim of additional threats compared to the previous cases, due to the facts that: *(i)* a greater control is given to Tenants on data management (*Data Breaches* risks); *(ii)* usually the Tenant has the power to control the infrastructure offered by the MNO through APIs (*Interfaces and APIs* risks) and execute arbitrary code (*Hijacking* risks); *(iii)* Tenants could have a limited control over some network functionalities (e.g., host firewall), thus influencing some RAN configurations by exploiting a VM Escape attack (*Abuse and Nefarious Use of Services* risks);*(iv)* a Tenant could run malicious code through the operating system of its VM or could fail in updating its VM, thus exposing it to attacks. Tenants and Subscribers could be victims of the same vulnerabilities reported for the SaaS and PaaS cases, with the difference that the *Malicious Insider* threat within the MNO's system is less dangerous than in SaaS and PaaS because the access of the MNO to sensitive Tenant's data is at the lowest level [15].

Other risks

A threat to MEC environment, possible with any type of service model and common to MNO and Subscribers, is represented by *billing risks* [16]. Roaming scenarios are

susceptible to this kind of attacks since the MNO managing the home network must trust information collected by the MNO that owns the edge of the visited network. The attack perpetrated against the "home" MNO occurs when a Subscriber manages to manipulate the "visited" MNO by breaching the serving MEC server; in this way, the attacker can communicate to its home network a smaller amount of data than actually consumed, through the compromised MNO. On the contrary, damage to a Subscriber is caused by a malicious or compromised serving MEC server, which communicates an over-the-top consumption of data to the home network of the Subscriber.

MEC server could be also a good solution to provide Enhanced Connectivity to consumers, offering them the resources to optimize their connection settings. According to the authors of [37], a possible use case of MEC consists in the allocation of the optimal amount of bandwidth resources to each application running on the MEC server; it falls into the "Network performance and Quality of Experience (QoE)" category because aimed at improving the performance of mobile networks. MEC can optimize the connection of the application to the cellular network by exploiting collected real-time information, which could also be a valuable means for MNO to become a Partner Service Provider by supplying various actors, such as Tenants or generic application providers, with the information collected on users and cell. As explained in [40], MEC can offer local context-awareness to application providers to enhance services they deliver to consumers. In [28], the MEC for Industrial IoT use case for 5G networks is described, where MEC servers are used to collect data from devices and extract meaningful preliminary information before sending it to the central server, located outside the mobile network. This information can be provided as a service to third party vendors.

In all of these cases the security of users could be at risk. In fact, the information that MEC servers gather on users must be kept safe in order to avoid Data Breaches by malicious entities.

2.3.3 Software Defined Networking

The technology

The hallmark of SDN is the possibility it offers to overcome the difficulties in flexibly managing traditional IP networks through the decoupling of the *data plane* and *control plane* [41]. In the SDN architecture, the interfaces take on a prominent role. The Southbound Interface (SBI) defines the forwarding rules for the network devices and the protocol which regulates the communication between control and data planes, while the Northbound Interface (NBI) is offered by the SDN Controller to the application developers [42]. The *application plane* can be defined in an SDN architecture, which includes applications that establish network policies through the NBI (e.g., firewalls, routing), thus producing a translation in southbound-specific rules used to instruct the data plane devices [19]. Besides the traditional solution of centralizing control in an SDN network, some distributed solutions are also possible. In [43], a distributed and hierarchical SDN architecture is presented, in which a different level of control is implemented in each part that composes a 5G network: Radio Access Network (RAN), Transport Network (TN), and Core Network (CN). Opportunities and challenges of a distributed SDN architecture are explained in [44].

In the developed risk analysis, the main business models enabled by the typical use cases of a SDN-based-5G network are examined [45].

Flexible *routing* is a use case representative of the advantages offered by SDN. The routing policy is usually managed by an MNO in 5G cellular networks to offer an off-the-shelf solution to a Tenant (Case 1, labelled as C1 in Figure 2-4). Alternatively, this use case can enable an Asset Providing BM, when the entity in charge of managing the network exploits the infrastructure made available by a dedicated InP; in this case, the MNO role is taken by MSP and InP (C3 in Figure 2-4). Control and data plane functionalities can be implemented by diverse entities in SDN [45] [46], therefore the MSP could be the supervisor of the control plane functionality, while a third-party-InP could provide the physical resources that compose the data plane.

According to the *network management* use case, a Tenant declares its service re-

quirements via the NBI in order to allow the MNO to adapt its network policies. An Asset Providing BM can be implemented, where the SDN Controller, for example, is used to recognize the Tenant's traffic and instructs SDN switches to route it to the proxy used to protect the security of applications [47]. This BM can be replicated in 5G cellular networks if the MNO that manages the SDN network provides service to diverse Tenants.

Differently, the *application-awareness* use case can enable typical business models of the Enhanced Connectivity Provider type, as the MNO responsible for the management of the Controller can adapt the network behavior to the connectivity requirements of Tenant's applications (C2 in Figure 2-4). As an example, the proper amount of SDN switches can be allocated to different services to meet their QoS requirements, based on the assigned priority class, and dedicated Controllers deployed to manage the diverse priority groups [48].

The *monitoring and measurement* use case enables a Partner Service Provider BM in a 5G cellular SDN-network, when the information on the network collected by the SDN Controller, used by the MNO to improve the service quality offered to consumers, is harnessed also by an external partner to enhance the services it provides. An example is given in [49], where the framework application providers can use exposed API to access "as a service" the information on the perceived QoS gathered by an SDN Controller and a measurement controller in the underlying infrastructure. We consider this case different from the Asset Providing BM, as the consumers exploit only collected information but do not directly use the assets of the MNO (i.e., the SDN controller).

The risks

The main security risks that affect SDN technology are reported in various works in the literature, including [50] [51] [52], that analyze the diverse security threats impacting on the 5G systems. An analysis of the risks related to the application of the SDN technology to 5G cellular networks is obtained, in this work, by considering the existing literature. Figure 2-4 summarizes the risks classification.

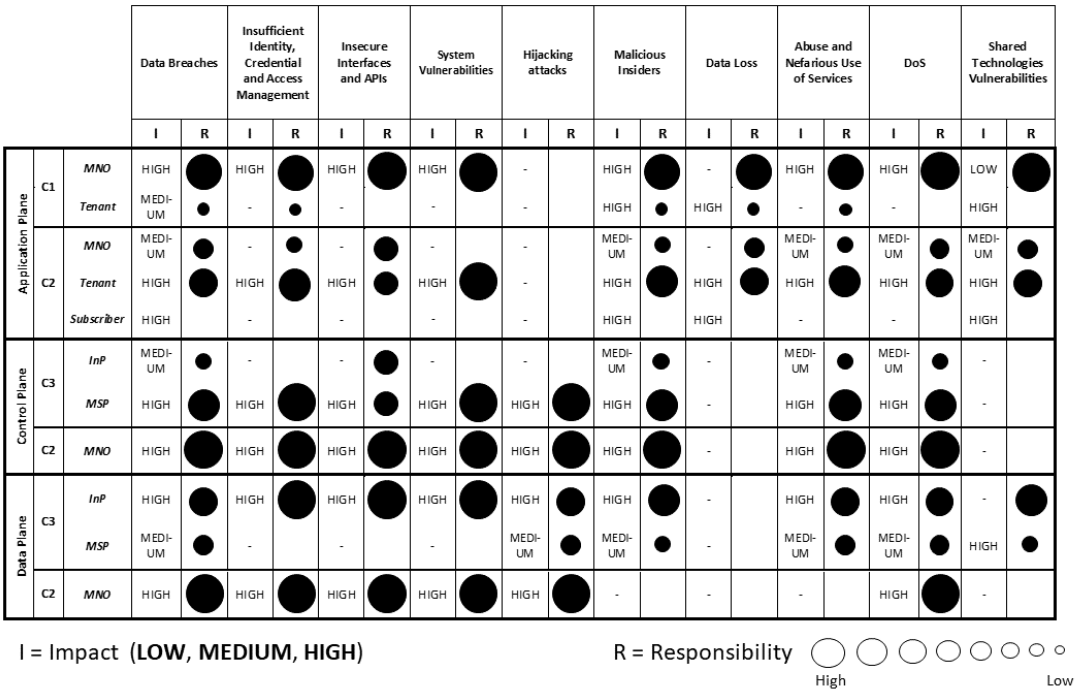


Figure 2-4: Stakeholder-based classification of SDN risks for different planes. I=Impact; R=Responsibility for attacked assets; Ci=Case i

Control Plane (CP)

At the control plane, *InP* and the *MSP* (or the *MNO*) can be victim of different attacks, depending on the implemented business model. Specifically, the MSP can play the role of consumer of a service offered by an InP (e.g., it uses the infrastructure provided by the InP to develop its routing application); furthermore, the MSP or the MNO could be provider of services to external consumers (e.g., when they offer to external Tenants either the SDN network or just information collected through this network).

Centralization of control decisions in the Network Operation System (NOS) is a point of strength of SDN, but it represents also its main vulnerability to security attacks (of the type of those reported in Section 2.3.1).

Control channels need to be protected as they are susceptible to message tampering attacks that could both damage the NOS, which may lose the control of the network, and jeopardize the trust relationship established between the MSP and the InP providing the infrastructure. For its part, the InP must properly manage the access to the offered infrastructure to shield its assets from being compromised and

damaged.

When the MNO own and manages the CP, it has to implement strict NBI security control, effective access and authentication mechanism to protect itself and especially the Controller from threats when it exposes its assets or information to external consumers. Also in case the MSP uses the infrastructure provided by an external InP, adequate mutual authentication mechanisms should be performed, together with protection measures for the SBI (against Eavesdropping or untrusted InP).

The SDN technology allows an MNO to offer its Network as a Service to Tenants or generic third party developers which want to implement their applications [42]. Such players, outsider to the network, could flood the Controller with junk requests, saturating its resources and making them inaccessible to any other applications running on it. Fake or manipulated switches could do the same thing against the MSP managing the Controller in the case they are provided by an untrusted InP renting its infrastructure.

Data Plane (DP)

Attacks affecting the data plane primarily concern either the *InP* or the *MNO*, depending on the entity owning the network infrastructure.

An issue in common with the previous case is the necessity to secure data and SBI to prevent *(i)* configuration attacks on forwarding devices that are more likely when different entities manage the control and data planes, as well as *(ii)* Eavesdropping, Replay Attacks, and Flow Modification that can breach the confidentiality and integrity of data transmitted to forwarding elements. Furthermore, the Controller identity has to be checked through robust Identity, Credential and Access Management policy to prevent Man-in-the-Middle attacks performed by fake Controllers against data plane elements.

DoS attacks can also affect network devices, since the flow tables, received from the Controller and stored in order to direct traffic, are limited in capacity. A malicious or breached Controller could saturate the flow tables of the data plane devices by sending them bogus forwarding rules.

As for the consumers of network services (namely, *Tenants*, *Subscribers* and also *MSP* when the infrastructure is provided by a dedicated InP), they all suffer the consequences of possible attacks on the data plane, since the protection of their data can be breached and the requested services may not be provided correctly.

Application Plane (AP)

Applications running on the SDN network architecture may be developed by the *MNO*, administrating the network, or by external *Tenants*. Obviously, all attacks affecting the control and data planes are also dangerous for applications, which could not work in the event of network failure or malfunction. However, a noteworthy threat to the application plane is that of Shared Technologies Vulnerabilities as in 5G cellular systems SDN supports multi-tenancy [53]. In this regard, the authors of [54] explain how the division of resources in a multi-tenant SDN network can be done. One possibility is that each Tenant has to install its own SDN Controller in charge of instructing the SDN switches assigned to its virtual network. A proxy Controller exists between the Tenant's controllers and the physical switches and represents the data plane for the former and the control plane for the latter. This is inspired by [55], where authors state that diverse Tenants can run their own network operating systems and operate their virtual SDN networks, thanks to the combination of NFV and SDN technologies and the implementation of an hypervisor in charge of managing the different virtual networks. As regards the flow tables of the shared switches, different policies can be applied to separate the entries of different Tenants. Authors of [54] propose a Soft-Partitioning Resource Manager in order to overcome the limitations of existing Hard and Soft partitioning strategies.

It follows that applications belonging to different entities could be run on the same network and it is important that each of them is well isolated from the other. Authentication mechanisms should prevent untrusted applications to become part of the network share. This threat is a risk for *Tenants*, their *Subscribers*, and for the *MNO* that provides the network. All the actors involved in the system could suffer Data Breaches and Loss.

2.3.4 Network Function Virtualization

The technology

NFV, described by ETSI in [56], is considered a key enabling technologies for 5G mobile networks [57]. Main challenge of NFV is to overcome the dependence of network functionalities on proprietary and dedicated hardware [58], thereby reducing the time and complexity required to update and develop new network services.

A typical NFV system includes the following components. A *Virtualised Network Function (VNF)* is a software implementation of a network function (e.g., firewalls, Evolved Packet Core (EPC), Mobility Management Entity (MME)) running on the NFV Infrastructure (NFVI) with the aim of accomplishing a certain task required by the network. A VNF can run on a single Virtual Machine or on more than one, each hosting a different component of the VNF. The *NFVI* is the environment where VNFs are made available and includes the compute, storage and network hardware resources, the VMs, and a hypervisor responsible for abstracting and partitioning the physical resources and making them available to the VNFs, thus managing the mapping of network functions onto logical resources. The *NFV Management and Orchestration (MANO)* is in charge of orchestrating and managing network resources; it contains: NFV orchestrator, VNF manager, and Virtual Infrastructure Manager (VIM).

Based on the major use cases of NFV reported by ETSI in [59], specific business models can be derived. *NFVI as a Service (NFVIaaS)* is the first noteworthy use case listed by ETSI that foresees a service provider offering its NFVI as a service to another service provider, which is relieved from managing the NFVI deployment and thus can concentrate its efforts on a better services provision to consumers. In [59], NFVIaaS is considered, to some extent, comparable to IaaS and NaaS service models of Cloud Computing, since the execution environment of the VNFs is provided together with the necessary network connectivity. Based on [59] and [56] and according to the ETSI view of a single entity both managing infrastructure resources and providing connectivity, we consider MNO as the player entirely responsible for the NFVI. Consumers of NFVIaaS are the Tenants that deliver services to users via

the offered NFVI (C5 in Figure 2-5). This is a clear example of Asset Provider BM. *Virtualisation of Mobile Base Station* use case represents a possible implementation of a Connectivity Provider BM, since an MNO can create new VMs to face hardware resource congestion problems in the RAN, thus offering connectivity services to users. *Crypto as Service* and *Security as a Service* are two examples of the *VNF as a Service (VNFaaS)* use case [60], which allows to implement a Partner Service Provider BM. In fact, third party applications developers or MNO (C4 in Figure 2-5) can offer VNFs to support Tenants requesting security services [59].

The risks

By virtue of the discussion on feasible business models via NFV, a risk classification according to the threatened domain is introduced and summarized in Figure 2-5.

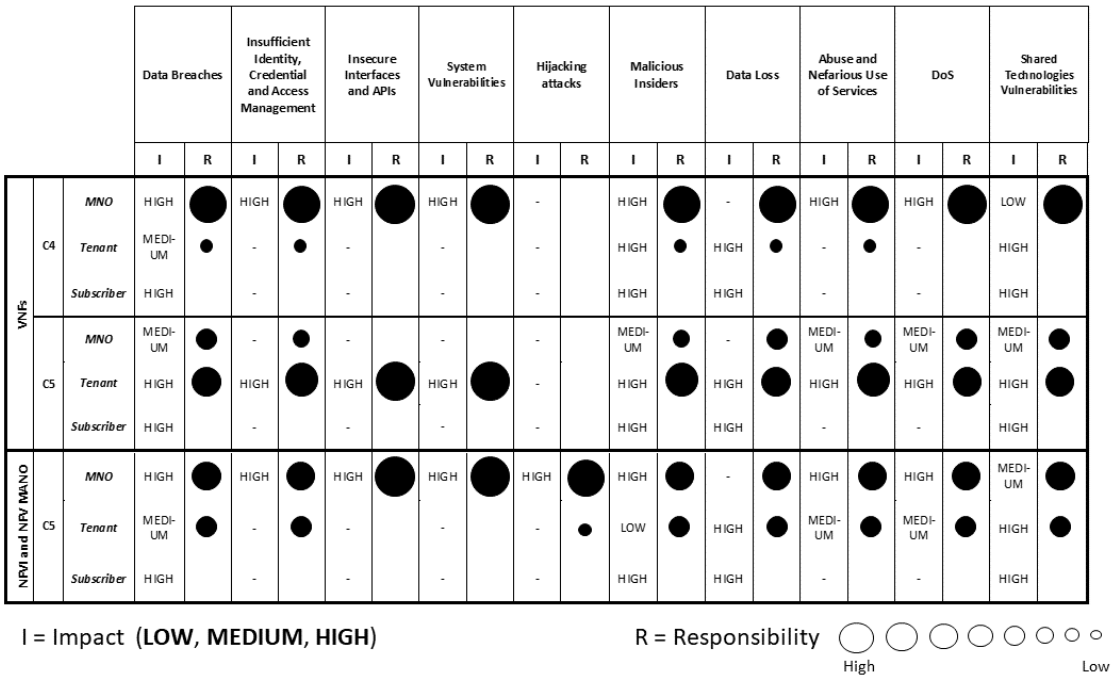


Figure 2-5: Stakeholder-based classification of NFV risks for different domains. I=Impact; R=Responsibility for attacked assets; Ci=Case i

VNFs

When a VNF is attacked, its provider is the most affected stakeholder. This role can be played by: the *MNO*, a *Tenant* or a third party developer, which could deploy its own VNF by using the NFVIaaS offered by an MNO [59]. Attacks on VNFs introduced in survey [50] belong to some of the groups we listed in Section 2.3.1.

Considering that NFV transforms network functions into software, Software Flaws can cause major threats. For example, through a Buffer Overflow, an attacker might be able to insert malicious code into areas of memory that users should not access, thus jeopardizing system behavior. The event of a badly configured VNF is described in [52] as another possible system vulnerability. It can be caused by the soaring demands for VNFs which contributes to increase the complexity of virtualized systems. The grown system complexity can pave the way also to unauthorized data access (Insufficient Identity, Credential and Access Management and Insecure Interfaces and APIs), traffic Eavesdropping (Data Breaches), and DoS attacks. Finally, the dynamicity of the VNFs, whose life cycle is influenced by consumers' demands, can also yield configuration errors that would make the system vulnerable.

NFVI and NFV MANO

Attacks on NFVI and NFV MANO belong to the same group because it is very likely that the same stakeholder builds the NFVI and manages it [56]. A risky situation for these domains arises when the NFVI is offered as a service by the MNO to external entities which want to develop their VNFs. Possible threats the *MNO* can incur are: Hijacking Attacks to the hypervisor (by malicious applications that can reach it, e.g., through VM Escape and VNF Manipulation attacks) and to the VIM (reached and manipulated through Privilege Escalation); Physical Host attack to the resources offered by the MNO through malicious code execution on the VM; DoS attacks to the storage and computing resources (used by the VMs on which the VNFs run (referred to as Resource Interference attacks in [50])) and to the hypervisor (that can be exhausted via Flooding Attacks).

The risks associated with the listed attacks on individual elements of the NFV system can become even more serious because of Shared Technologies Vulnerabilities. As an example, NFV allows the co-existence of different VNFs providers on the same NFVI. Each provider could implement its own security protocols on its VNF, resulting in diverse security levels among the various VNFs. This condition represents an important risk for the whole system, as it involves the presence of vulnerable VNFs which could be an easy target for attackers. Side Channel and VNF Location Shift attacks are other risks belonging to this category. Resource Theft [51] is a further example of an attack based on this type of vulnerability, as a malicious Tenant could access resources belonging to other consumers by exploiting a failure in isolation.

2.3.5 Network Slicing

The technology

The network slicing paradigm has the main goal of making the 5G network flexible and scalable, so as to be able to guarantee a satisfactory supply of heterogeneous services [61] over a single physical network infrastructure [62]. SDN and NFV are the technologies that fostered the birth of network slicing, since they enable the creation of different end-to-end virtual networks (i.e., slices) over the same physical infrastructure. The design of each slice is service-based, as it is steered by the requirements of a particular service [63]. As an example, an end-to-end network slicing framework to support the diverse IoT services on a 5G networks is proposed in [64], where its benefits are highlighted; in the same paper, the authors carry out an interesting review of existing research works on IoT network slicing.

The risks

The risk analysis for the network slicing paradigm is represented in Figure 2-6.

Network slicing is typical of multi-tenant environments, since an MNO can offer its network as a service [65] by allocating its partitioned resources to different services and even to different Tenants. Being this done by leveraging SDN and

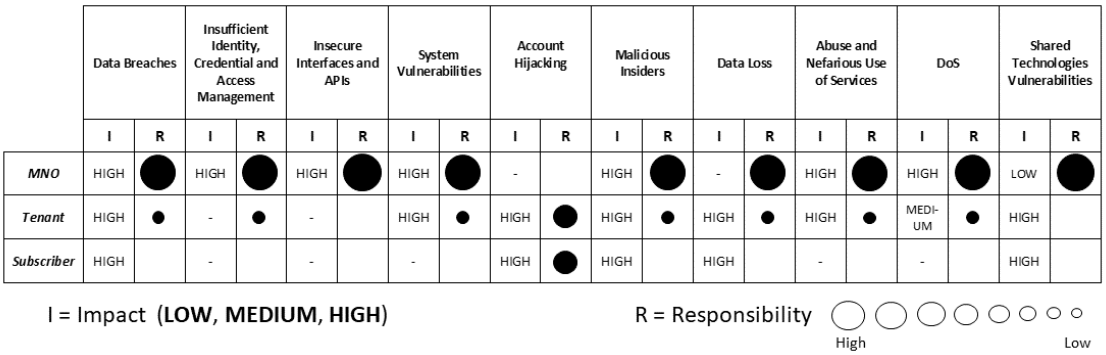


Figure 2-6: Stakeholder-based classification of Network Slicing risks. I=Impact; R=Responsibility for attacked assets

NFV technologies, network slicing obviously inherits the risks already illustrated for them. As a consequence, this Section only addresses the most representative risk for the network slicing paradigm: Shared Technologies Vulnerabilities [26]. *MNO* can protect itself from Breaches to its data, Hijacking, and DoS attacks on the elements of the network by strongly isolating its network infrastructure from the virtual resources assigned to Tenants. In this context, Security Policy Mismatch is a common cause of threat to MNO and to the *Tenants* which slices are provided to. In fact, if different levels of security are implemented on each slice, based on the type of service provided, this might allow a malicious entity to attack the weaker slice, then penetrate the isolation with the other slices or even with the host machine belonging to the MNO.

With reference to the NSaaS business model defined in [14], the distribution of security responsibilities changes according to the relationship between service provider and consumers. With a B2B model, Tenants have the full control of the protection of their Subscribers. In the B2C case, Tenants rent the slice without worrying about which operator is providing it, thus having a greater risk of incurring malicious or compromised MNOs. Finally, in a B2B2C configuration, three actors are involved in the supply of services to users: the MNO offers network resources to a Broker, which in turn provides the slice to the Tenant. The involvement of a third party (i.e., the Broker) in providing the slice to the Tenant obviously increases the possibility of attacks against MNO and/or Tenant.

2.4 Defence mechanisms

A detailed investigation of the defence mechanisms that may be deployed to protect 5G virtualized networks would require an in-depth analysis of the many defence domains and measures. However, this Chapter would not be complete if we completely disregard this aspect. For this reason, we have included in this Section a very brief (high level) overview of the the main defence mechanisms implementable to meet the target security requirements in terms of confidentiality and integrity of data, resilience, and protection of privacy.

Table 2.1 summarizes the defense mechanisms analyzed, the stakeholders who benefit most from them, and the reference literature.

Table 2.1: The major countermeasures to protect virtualized 5G networks

Countermeasure	**Benefits for Stakeholders**	**References**
Authentication and Access Control	The service providers (i.e., InP, MSP/MNO, Tenant) can protect access to their assets. Consumers (i.e., MSP, Tenant, Subscriber) can benefit from mutual authentication mechanisms to identify their legitimate providers.	[66] [67] [68] [69] [70] [71] [72] [73] [74]
Cryptography	Consumers (i.e., MSP, Tenant and Subscriber) can protect their data that are the main targets of attackers.	[75] [76] [77] [78] [79]
Secure Virtualization	The MNO can protect its network from penetration attacks. Data of Tenants and Subscribers can be securely isolated.	[40] [80] [81] [82] [83] [84] [85]
Resilience Assurance	Consumers (i.e., MSP, Tenant, and Subscriber) can receive a minimum level of service even in case of anomalies in the network.	[86] [87] [88] [90] [91] [92]
Intrusion Detection Mechanisms	Service providers (i.e., InP and MSP/MNO) can discover any attacks or anomalies in the network and collect information on the perpetrators.	[93] [94] [95] [96] [97] [98] [99] [100] [101] [102] [103]

2.4.1 Authentication and Access Control

The management of authentication and access control can help to avoid most security threats in environments rich in actors, services, and resources like a virtualized

5G cellular system. Thanks to the implementation of authentication mechanisms, each entity becomes identifiable. Thanks to access control, entities that can access services and resources can be selected by each provider for the protection of its assets. This countermeasure has the potential to mainly protects the service provider, therefore the *InP*, *MSP/MNO* or *Tenant*, based on the cases analyzed. Consumers, such as *MSP*, *Tenant* and *Subscriber*, can also benefit from mutual authentication mechanisms as they allow to discover malicious providers.

In [66], authors present a distributed reputation management system that optimizes the resource allocation in computation offloading to the Edges, by relying on reputation. This can be considered as a sort of access control measure, since only reliable users can access the service offered through edge computing servers, thus offering benefit to service providers. The use of a two-factor authentication mechanism is suggested in [67] to strengthen security in edge-of-things systems. As stated in [68], two-factor authentication can bridge the gap of text-password authentication, that is the most simple and used authentication mechanism. Security enhancement is assured by combining what the user has with what it remembers. In fact, one step of authentication usually consists in using a token that the user has (e.g., a smart card or a cell phone) and another step requires something that needs to be remembered (e.g., a password or a Personal Identification Number (PIN)). In order to cope with security and availability issues in a smart home, in [69] an edge-of-things solution is proposed, which relies on the implementation of two-factor authentication mechanism to make the procedure as safe as possible for the user.

In [70], authors propose the SDN-based AuthFlow architecture to aggregate mechanisms of authentication and access control with the SDN technology. The need for implementing authentication in SDN environments is also faced by authors in [71], wherein they implement a mutual authentication procedure aimed at protecting both the Controller provider and the network application developers.

A security-oriented MANO framework is proposed in [72], which provides Identity and Access Management security functions. Besides, a Trust Insurance Mechanism is presented in [73] to achieve collaboration among trusted VNFs running on different platforms through the implementation of a trust authentication mechanism.

As for network slicing, an efficient and secure service-oriented authentication framework is introduced in [74] to support privacy-preserving slice selection and anonymous authenticated key agreement for 5G-enabled IoT; the protection of the users is the primary goal of the proposal.

2.4.2 Cryptography

The main security mechanism to implement to protect integrity and confidentiality of data is cryptography coupled with a secure key management. By encrypting the transmitted or stored data, many actors can be protected from Data Breaches attacks. The major beneficiaries of this security measure are undoubtedly consumers (i.e., *MSP*, *Tenant* and *Subscriber*), whose data are mainly targeted by attackers.

In [75], authors present a privacy preserving scheme based on the use of encryption on data transmitted by terminal devices towards the edge server. Plaintext data is revealed only in the public Cloud center.

In [76], the symmetric and asymmetric cryptographic techniques implementable in a Software-Defined Wireless Sensor Network (SDWSN) are described, because considered suitable to resource-constrained devices that compose WSNs. SDN together with encryption mechanism is exploited in [77] to protect vehicles in a Vehicular Cloud Computing. In particular, encryption is implemented to conceal the real identity of each vehicles registered to the system and to secure inter-vehicle communications.

The Long Term Evolution (LTE) NFV vulnerabilities are faced in [78], where authors propose the vEPC-sec architecture, which entails that VNFs share private keys to encrypt exchanged control-plane messages.

Encryption mechanisms are implemented in [79] as part of a security solution for the protection of intra-slice domain in a 5G network.

2.4.3 Secure virtualization

Different solutions can be implemented to abstract physical resources of a network infrastructure into software entities to be offered to consumers.

In [40], a comparison between VMs and Containers approaches is analyzed. VMs represent the virtualization method most used in Cloud Computing. This technology is based on the use of a central hypervisor that is responsible for mapping between the physical and virtual resources assigned to each VM implemented in the physical host. The abstraction provided by a VM affects the entire Operating System (OS); this causes a slowdown in the boot process of the machine but, on the other hand, guarantees a robust isolation between virtual environments. Containers technology is newer and much lighter than the VM [80]. The typical lightness of the container is given by the fact that the same OS kernel is shared by the different application processes; therefore, a container must not activate its own dedicated OS thus ensuring simplified deployment and faster availability than the VM. Despite all these advantages, with containers the assets of the different Tenants should share the same OS, thus, they would be more exposed to attacks on the shared technologies.

A similar comparison between security in VM and Containers is carried out in [81], where also the Unikernel virtualization technique is considered. This is seen as a valid solution to the lack of isolation that affects containers. With Unikernel, lightweight VMs are realized allowing the allocation of OS and userspace layers on a single VM layer. However, the authors point out that some security vulnerabilities could arise due to the management of privileges for an excessive number of Unikernels.

Authors of [82] conduct an interesting analysis on the impact of virtualization technologies on Edge and Fog computing. Three supporting technologies are described as suited to be implemented within the Edge architecture, that are Containers, Real-Time Operating Systems (RTOS), appropriate for services that have strict requirements for the response times, and Unikernels, which revolutionize the idea of VM. Security issues that arise from each technologies are surveyed and discussed.

Also in [83], authors demonstrate the ability of a Unikernel-based solution to effectively deal with Cloud security and privacy concerns, while, in [84], strengths and weaknesses of the Unikernel virtualization solution are highlighted.

A recent work which provides a comprehensive overview of all the main virtualization models is [85], where authors also conduct a security analysis on each of

them. To this aim, the authors define a reference virtualization architecture, identify some vulnerabilities that could affect the different components of this architecture, and assess the impact of these vulnerabilities on the diverse considered virtualization models. In the following are some interesting conclusions inferred from this work:

- Virtualization based on type-I and type-II hypervisors is a popular model. The main difference between the two types is that the type-I (also referred as bare-metal hypervisor) runs on the host machine's physical hardware resources, thus having direct control on them, while the type-II (also referred as hosted hypervisor) is executed on top of the host OS as any software application. From the security analysis viewpoint, the two types are similar, except for the vulnerabilities of the execution environment of the hypervisor, since the type-II are the most affected.

- OS-level virtualization represents the containerization model, which envisages that only the applications and their dependencies are integrated into a Container. Many of the vulnerabilities identified by the authors have only a medium impact on Containers, except for those of the execution environment of the hypervisor and the VM-Hypervisor Crosstalks, which can cause DoS attacks on the hypervisor and attacks on shared technologies, such as VM Escape.

- The Unikernel solution emerges as the most effective and secure. A Unikernel can embed only one application and a limited set of its dependencies that, differently from Containers, also includes the libraries for hardware resource management. Almost all the vulnerabilities identified by the authors have a medium or low impact on Unikernels, excluding those concerning the OS Kernel Oversight category, since the isolation of the OS kernel from the application is more at risk than type-I and type-II virtualization models.

Choosing the proper virtualization implementation technique can help address many vulnerabilities, thus protecting the *MNO*, against penetration of its network by malicious entities, and *Tenants* and *Subscribers*, which do not risk their data being violated.

2.4.4 Resilience assurance

Resilience assurance has been investigated in the literature as a security measure for virtualized environments. As stated in [86], Cloud is vulnerable to many security threats, thus it is important that the Cloud service provider guarantees a sufficient level of service even after an anomaly occurs: this is a definition of resilience that well suited to all virtualized environments. Resilience assurance is a benefit especially for consumers, that could be *MSP*, *Tenant*, and *Subscriber*, that, despite everything, can receive a minimum level of service.

In [87], edge system availability is ensured by the deployment of some Mobile Agents (MAs), that are special-purpose software running in edge machines to handle possible faults. A proactive failover mechanism for the resilience of NFV-enabled edge computing is proposed in [88]. In [89], NFV and MEC paradigms are combined to improve network performance in terms of flexibility, latency, and capacity, in the face of the 5G systems requirements. Faults forecasting is carried out through a proactive failure-recovery management layer, which contains a module charged with running machine-learning-based prediction algorithms. The improvement in latency, ensured by the proactive mechanism compared to the reactive one, is demonstrated in the performance evaluation.

The resilience assurance in SDN is stated as an important issue in many works in the literature, such as [90] [91] [92], that elaborate different solutions to the urgent resilient Controller placement problem.

2.4.5 Intrusion detection mechanisms

Further valid solution to face security threats in the virtualized 5G environment consists in the use of intrusion detection mechanisms. Usually, the service provider, like MNO, is the entity responsible for detecting anomalies in the system. Once the problem has been identified, fault recovery techniques can be implemented to ensure a continuous service to consumers. The application of intrusion detection mechanisms is an advantage primarily for *InP* and *MSP/MNO*, which usually deal with the provision of services, therefore have a greater interest in finding any attacks

or anomalies in the network and collect information on the perpetrators.

Honeypots are an example of intrusion detection mechanism. The goal of a honeypot is to catch attacks or anomalies and gather information about them. In [93], honeypots are defined as unique security resources, as they are different from other security protection techniques. The main difference is that the value of a honeypot is defined by the amount of attacks it lures, differently from other security mechanisms which have to repel malicious behaviors. Everything could be a honeypot, not only computer but also password, application, network of computers, etc.. For example, in [94], some flexible honeynets are efficiently managed through the use of NFV and SDN and deployed for the security of IoT networks. The implementation of honeypots as intrusion detection tools in Cloud Computing is common in the literature [95][96][97]. Some works also deal with the deployment of honeypots in edge computing environments. In [98], the HoneyBot technique is proposed to detect, track, and isolate malicious nodes acting inside a corporate network in which D2D communications are established to allow computational offloading among collaborative mobile devices. HoneyBots are honeypots positioned in the network in order to lure attacks from malicious nodes. Therefore, the incoming and outgoing flows from HoneyBots are constantly monitored. Authors in [98] also show the impact of honeypots positioning within a MEC system. In [99], a Virtual Honeypot Device is used in order to make the system adaptive to security breaches by malicious edge devices; it is a device with dummy data that has to generate log files about ongoing attacks to send to an Attack Database Repository for predicting similar future attacks.

In [100], an intrusion detection mechanism based on machine-learning is implemented in a virtual SDN environment testbed to identify DDoS attacks. Authors in [101] propose a security solution for SDWSNs which includes intrusion prevention and collaborative anomaly detection systems.

A real-time attack detection and mitigation mechanism for 5G network slicing scenarios is presented in [102] which is based on the P4 data plane programming technology. In [103], authors introduce a framework to strengthen security protection in 5G slices that exploits two open source intrusion detection systems, that are

Snort [104] and Suricata [105], while Ntopng [106] is used for deep packet inspection, useful to prevent complex attacks.

2.5 The three stakeholder model - discussion

Throughout this Chapter, the risk analysis has been grounded on what has been referred to as *the three stakeholder model*. This model focuses on the security responsibilities shared across three main players, namely MNO, Tenant, and Subscriber, which are illustrated in Figure 2-1 together with other 5G stakeholders. This model is simple to handle and lies at the basis of practically any cellular/5G deployment. However, it is fair to remark that this model is just a starting baseline; indeed, the virtualization levels that can be nested on 5G infrastructures may be definitely more complex than such a three-layer model. On one side, it may involve certainly more than three "layered" stakeholders, with a Tenant of a bearer service being in turns provider for a value added service and hierarchically hosting its own (higher layer) Tenants; on the other side, the nature of such players can be extremely different, from virtual operators to content distribution providers, to vertical service providers or application providers, and so on.

It follows that a detailed analysis of *all* such possible scenarios appears cumbersome and would take quite far away from the goals of this Chapter. Moreover even if the specific roles and responsibilities do clearly differ in tailored scenarios (for instance, the stakeholders and roles that come into play in a vertical business in a Smart City domain are arguably very different from those in the Media & Entertainment sector), the dynamics of the relationships between additional stakeholders, with a view to security, can be inferred by applying the principles illustrated in this Chapter in a sort of "recursive", layered manner.

The main argument at the basis of this discussion stems from the observation of what has been done so far as best practice in classical Cloud settings. Here, as for instance discussed in [107], security responsibilities and obligations in real world Cloud deployments are typically contracted by means of pragmatic *shared security models* which focus on the careful analysis and attribution of responsibilities between

the Cloud service provider and the enterprise. The point is that, apart from the specific (and often non trivial, see e.g., [108]) details which clearly depend on the type and nature of the contracted cloud service, the model itself is conceptually simple, as it pragmatically focuses just on the two contracting parties (the Cloud provider and the contracting enterprise), and focuses on the distinction between:

- the responsibility of the Cloud service provider to maintain a secure and continuously available service (in essence, guarantee security of the service itself), and
- the responsibility of the enterprise to ensure secure use of the service

Such a distribution of responsibilities can be found also in network service scenarios. Among many others, a well known real-world example is the case of AWS IoT Greengrass, through which Amazon offers different functionalities to edge devices for various customers, among which many large companies - such as Bayer, LG, Philips, and so on [109] - which may in turn provide services to their customers.

Indeed, and in more generality, unlike the classical Cloud scenario where a stakeholder (e.g., an enterprise or a public Institution) contracting a Cloud service often is also the end user, the typical model of "verticals" in the 5G fosters the emergence of stakeholders which, on the lower layer, rely on Cloud networked services, and in turns sell value added services to their own customers, and hence share security responsibilities with them with the same paradigm introduced above.

The focus on a three-layer model was primarily motivated by this "layered" relation among stakeholders which naturally emerges when considering 5G Tenants, offering their services to the Subscribers, and, at the same time, leveraging network services from the MNO. It is obviously true that the pile of stakeholders can be much larger than just three, but, at least in most contexts, the sharing of security responsibilities can be reduced to the analysis of the relation between each stakeholder and the "adjacent" ones, i.e., the lower and higher ones in the hierarchy.

Going back to the previous example of AWS IoT Greengrass, a company that contracts IoT services from AWS will share security responsibilities only with AWS,

and not with the "layer" underlying AWS itself, for instance Intel as Cloud technology provider. Obviously, the possibility of envisioning scenarios in which roles and responsibilities are specified and detailed across the entire stack of potentially multiple players cannot be ruled out a-priori, but most of the scenarios may be captured and analyzed by the presented pragmatic three-layer model.

For instance, the following real-world four-player exemplary business model, closer to the 5G domain, can be considered. An Over-The-Top (OTT) (layer three) distributes its contents through a pay-TV platform (layer two) that uses the mobile network of the MNO (layer one) to provide the contents through its application to its customers (layer four). Here as well, the model for sharing security responsibility among the three players at the highest layers can be shifted down and applied to those at the lowest ones thanks to the principle that each layer makes the lowest layer transparent to the one above it. It is, obviously, assumed that trustworthiness relationships are established between a stakeholder operating at a level of virtualization and that or those of the lowest level that offer him a service/infrastructure. Since the manager of the pay-TV platform must meet the OTT's needs, it may be up to it to perform some security functions on behalf of the OTT. Referring to Figure 2-6, it could represent the distribution of responsibilities among the stakeholders involved in this real-world four-player exemplary, considering the manager of the pay-TV platform in place of the Tenant and the OTT in place of the Subscriber, being the OTT a consumer of the services offered by the pay-TV platform. Therefore, practically most of the responsibility for the network's assets lies with the MNO, while the remainder is managed by the manager of the pay-TV platform, in charge of ensuring the level of security required to the OTT. Another level of distribution of the security is added if the consumers of the services provided by the OTT are considered. In fact, they too could incur, for example, into risks of Data Breaches, even if they have not security responsibilities on provided services. In this case, what is illustrated in Figure 2-6 remains mostly valid considering the manager of the pay-TV platform instead of the MNO, the OTT instead of the Tenant and the consumers instead of the Subscriber.

A further degree of complexity not considered in the three-layer basic model

is related to the horizontal dimension, i.e., to any multi-domain situations. For example, two MNOs could provide their own infrastructure and collaborate, through the intervention of a Broker, to build a network slice for an Online Service Provider (OSP). In this case, both the impact and the security responsibility are differently distributed among the various stakeholders. The data relating to the OSP and the consumers of its services are distributed over the networks of two different MNOs and could be managed by the Broker, in charge of mediating the collaboration between the MNOs and guarantee an optimal service to the OSP, thus also protecting the OSP's assets. Obviously, the protection of the assets of the MNO is also a partial responsibility of the Broker, so the network of each MNO must be well isolated from that of the other and from the consumers of the services. Regarding the distribution of the impact, all the involved actors are potential victims of the threats described in Section 2.3.1, especially those of Data Breaches. Only for the Broker a low impact can be estimated for most of the described attacks.

2.6 Conclusions of Chapter

This Chapter has illustrated the results of a security risk analysis in virtualized 5G cellular environments, conducted from an innovative perspective: the one of the emerging new stakeholders. 5G key virtualization technologies (i.e., MEC, SDN, NFV, and Network Slicing) have been analyzed from the viewpoint of security and, for each of them, a stakeholder-based risk classification has been provided, distinguishing the possible different roles played by each actor depending on the business model implemented. Furthermore, an overview of the most common and effective defense measures that can be implemented to face and mitigate the effects of the analyzed risks is provided. The aspects of interest in this kind of analysis are manifold. Security is a key requirement of next generation cellular networks, even more when virtualization technologies are implemented. The greater number of actors involved in 5G environments makes a proper distribution of security responsibilities crucial. Therefore, a stakeholder-based risk analysis helps identifying the most vulnerable circumstances and actors. Finally, it is worth to repeat that not *all* possible scenarios

may be modeled using a three-layer approach. There may be, in fact, cases where it might be appropriate to introduce more complex relationships across multiple stakeholders down in the stack. Still, the pragmatic three-layer model introduced in this Chapter captures the majority of scenarios and is capable of representing many real business cases in the emerging 5G market.

Chapter 3

D2D to secure 5G multicast transmissions

D2D communication is considered as one of the key enabling technologies for 5G networks as it allows offloading of data generated by the huge number of connected devices. In this respect, group-oriented services are among the most interesting usage scenarios. Indeed, D2D can improve the performance of Conventional Multicast Scheme (CMS) in cellular networks which is known to suffer from low spectral efficiency. Security is a further key field of investigation for 5G system as any threat to privacy and security may lead to both deteriorated user experience and inefficient network resources utilization. Security issues are even more in focus for D2D connections between devices that are in mutual proximity. To improve the CMS performance and also sustain security requirements of the 5G networks, this Chapter introduces a secure D2D data transmission algorithm. Making use of mechanisms such as encryption and signature, this algorithm aims to protect the exchanged data and the privacy of the devices involved in the communication. A simulation campaign conducted using MATLAB shows the ability of the proposed solution to take advantage from the establishment of secure D2D communications and efficiently utilize network resources.

3.1 Introduction to Chapter

5G networks have to support a huge number of heterogeneous connected devices in manifold usage scenarios. Autonomous driving, tactile Internet, personal Cloud, disaster alert, video streaming and downloading are among the most challenging 5G use cases. Some technologies can play a key role in helping to satisfy the demanding requirements of the foreseen use cases. D2D communications and multicasting are certainly among these. The former because of its capability to offload cellular data traffic, enhance spectrum efficiency, and extend cell coverage [110]. The latter because of its capability to answer to the increasing user demand for multicast/broadcast multimedia services (mobile TV, IP radio broadcasting, and video streaming) [111].

Regarding 5G in general, in 3rd Generation Partnership Project (3GPP) the 5G radio access roadmap foresees two tracks: one is based on the evolution of Long Term Evolution (eLTE), and the other on the design of the New Radio (NR) access. Thus, the core enhancements/changes of the 5G paradigm are *(i)* the standardization of a new radio interface (i.e., called New Radio – NR – in 3GPP and other standardization bodies) and *(ii)* the empowering of the existing LTE systems in order to handle use cases (e.g., mMTC, Vehicle to Everything (V2X), Sidelink) for which NR is still not mature yet (i.e., the full specification of NR it was agreed just on the 15th of June during the 3GPP RAN#80 plenary). Consequently, in relation to the former case, it is good to point out that LTE constitutes an essential piece of the 5G puzzle and can be considered as a 5G-ready technology due to the variety of enhancements and new features already introduced in Rel-14 and Rel-15 timeframes in 3GPP. Therefore, even if the research efforts on D2D (i.e., later called Sidelink) and multicast/broadcast services started way before the concept of "5G" gained momentum, it is fairly evident that these technologies have evolved over the years to meet requirements more and more challenging.

Multicast transmission is an effective means for delivering group-oriented services since users can be fed through a single Point-to-Multipoint (PtM) transmission by exploiting the broadcast nature of the radio channel. In order to handle multi-

cast and broadcast services over cellular networks, the 3GPP has standardized the evolved Multimedia Broadcast Multicast Service (eMBMS) [112]. The approach for delivering multicast traffic in cellular networks, the so-called CMS [113], is known to suffer from poor spectral efficiency. According to it, all users belonging to the multicast group are served with the same data rate imposed by the user with the worst channel conditions. Despite this approach guarantees fairness because all users are always served and receive the same treatment, it suffers from poor performances because users with good channel conditions are constrained to the low data rates that cell-edge users can sustain.

In [114] a D2D-aided radio resource management policy is proposed for eMBMS, named D2D-enhanced CMS with Single Frequency (D2D-SF), with the aim to increase the aggregate data rate of CMS while maintaining the CMS short-term fairness. This protocol includes a first step, in which users with the best channel conditions are served via CMS directly by the eNodeB (eNB). Then, the served nodes forward the received data to the excluded users over D2D links. The peculiarity of this approach is that the forwarding devices send data simultaneously on the same frequency to their D2D receivers. Even though the good results of the protocol D2D-SF have been widely demonstrated, security in communications is not taken into account.

The need to look at aspects related to security stems from the fact that the 5G system is designed with security requirements in mind. In particular, the following properties make 5G a trustworthy multi-service platform: resilience, communication security, identity management, privacy and security assurance [115]. In addition to the magnified risk of security threats due to the huge number of 5G connected devices, D2D communications cause further problems due to connections happening directly between devices in proximity [116].

Several works in the literature deal with security in D2D communications. A classification and discussion of solutions to secure D2D communication can be found in [117][118], wherein also a comparison of the different approaches is performed in terms of their ability to satisfy D2D security requirements, such as confidentiality and integrity, authentication, privacy, non-repudiation, and so on. Among these

compared approaches, the work in [119] is identified as the more effective, since it is able to satisfy most of the security requirements posed by 5G networks [117][118].

This Chapter presents an algorithm that improves the CMS performance by exploiting secure D2D communications. The proposed enhanced CMS with secure D2D communications (eCMS-sD2D) can efficiently and securely deliver multicast traffic in 5G networks. As in the cited [114], D2D clusters are formed in order to forward data towards users with worst channel conditions, which are excluded from a first multicast transmission by the eNB. The algorithm introduced in this Chapter enhances the work in [114] by selecting the Relay Node (RN) (which is in charge to forward data sent by the eNB towards users unable to directly receive the multicast transmission) in each D2D cluster on the basis of its trustworthiness measured, by means of security mechanisms, as their capability of reliably acting as data forwarders. Thus, the proposed scheme can be seen as a clear security enhancement with respect to [114] since it takes into account the D2D communications security aspects previously not considered at all. In particular, security procedures inspired from [119] are implemented in order to guarantee confidentiality and integrity of data transmitted in D2D communications, and D2D users' privacy protection. Security mechanisms as encryption, Hashed Message Authentication Code (HMAC), and signature, are used to manage the message exchange between the peers. Data encryption is realized through a symmetric encryption algorithm, with the same private key used to encrypt and decrypt data. The private key is generated through an enhanced version of the Diffie-Hellman Key Exchange (DHKE) protocol, in which the public key exchange is intermediated by the eNB, representing the trusted third party. In addition, message authentication helps to avoid the Man-in-the-Middle attack, which represents the primary vulnerability of the DHKE algorithm. Thanks to the designed security mechanisms, many typical D2D attacks can be avoided. Among these, Eavesdropping, Impersonation and Masquerading, besides the already cited Man-in-the-Middle. The detection of any security attack performed by a networked node reduces the reliability of the node and, consequently, the probability of being selected as data forwarder.

The remainder of the Chapter is organized as follows. Section 3.2 and 3.3 present,

respectively, the related works in this field and the basics of the proposed eCMS-sD2D. Section 3.4 describes the designed algorithm in details. Results from the simulative analysis are shown in Section 3.5. Conclusive remarks are given in the last Section.

3.2 Related work

In the literature, many works deal with the candidate supporting technologies for enabling 5G networks [120], [57]. D2D communications is considered among these because of its capability to improve network performance in terms of delay, throughput, energy efficiency, and spectral efficiency.

The D2D taxonomy presented in [121] distinguishes between inband and outband D2D. Inband D2D communications use the cellular (i.e., licensed) spectrum and can be further categorized as underlay or overlay when the radio resources are shared with cellular users or are dedicated to D2D links. Differently, outband D2D exploits unlicensed spectrum. To this aim, an extra interface must be used and controlled by the cellular network (i.e., controlled mode) or by the users (i.e., autonomous mode). Usually, the underlay inband D2D is preferred to the other modes, because it better utilizes the spectrum and is suitable for all types of devices. As concerns the resource allocation in D2D communications several solutions can be found in the literature related to D2D [122] or in closely related fields [123].

An interesting usage scenario for the D2D technology is *multicasting*. Multicast and broadcast services are enabled in 3GPP Release 8 through the eMBMS architecture. According to [124], the group-oriented services are protagonists in 5G networks, and multicasting is an effective means to offer these services. Establishing direct communications between devices in proximity has shown to improve the multicasting performance. In [114], the D2D-SF approach has been designed to improve the performance of the CMS, counting on D2D communications occurring simultaneously at the *same frequency*. This paradigm has shown encouraging results in Long Term Evolution-Advanced (LTE-A) systems.

A further work focusing on content sharing by exploiting both D2D and mul-

ticasting technologies can be found in [125]. In this article, the authors present a Device-To-Device Multicast (D2MD) scheme for content sharing in cellular networks by taking into account social and physical attributes in D2MD cluster formation, and jointly optimizing power and channel allocation among D2MD clusters. However, trust and security aspects are still overlooked even if they play a fundamental role when involving social and physical relationship. Another work that address a similar topic is presented in [126]. Here, the authors consider a scenario where D2D users may demand multicast data at various rates and, in return, they offer different profits (revenue) to the telecom operator. However, it is shown that satisfying the user requests to maximize the profit is an NP-hard when the resource blocks are limited, and thus they propose a greedy heuristic algorithm to solve this problem. An interesting analysis of content dissemination scenarios is presented in [127], where two game theoretic medium access strategies, based on energy-aware utility functions, are proposed. The impact of cellular network characteristics on D2D communication is analyzed in [128], where the authors also exploit the benefits of Network Coding (NC) in the design of an adaptive cooperative protocol for the D2D data exchange.

No attention has been given so far to security which represents an important aspect for 5G networks; this is the focus of this Chapter. According to [129], privacy and security issues must be faced in order to definitely make D2D a successful technology. In [117], a thorough analysis on these problems is conducted. First, the difference between security and privacy concepts is defined. Then, the requirements to be satisfied in order to guarantee both security and privacy in D2D communications are listed, and the possible attacks are identified. Finally, related works and proposed solutions are described. Among these, Zhang *et al.* describe in [119] a secure data sharing strategy able to guarantee D2D privacy and security in LTE-A networks. The basic idea is to encrypt data transmitted in the D2D link using a symmetric encryption algorithm and generating the private key, for data encryption and decryption, following the DHKE. The strength of this strategy lies in the intervention of the eNB that represents a trusted third party and protects against malicious behaviors such as the Man-in-the-Middle attack. In [118], security solutions pro-

posed to improve D2D in 5G networks are analyzed. In addition to reporting D2D security requirements, threats and solutions, this work hints the role that the social relationships could play in improving the D2D security. This is an interesting starting point for future research aimed at exploiting concepts, such as social trust, to evaluate how much a network node can be reliable. In the algorithm presented in this Chapter, the security dimension is added to the D2D-SF solution proposed in [114] in order to make it suitable to 5G network and to cope with typical D2D vulnerability attacks.

3.3 Background

LTE-A is the solution proposed by 3GPP to bring broadband on mobile radio systems [130]. It offers a bandwidth of up to 100 MHz by exploiting the following additional bands compared to LTE: 450-470 MHz, 698-862 MHz, 790-862 MHz, 2.3-2.4 GHz, 3.4-4.2 GHz, and 4.4-4.99 GHz. At the physical layer, Orthogonal Frequency Division Multiple Access (OFDMA) and Single Carrier Frequency Division Multiple Access (SC-FDMA) are used, respectively for the downlink and the uplink directions. In OFDMA, the Resource Block (RB) is the smallest unit of resources that can be allocated to a user. The RB is 180 kHz wide in frequency and 1 slot long in time. In frequency, RBs are either 12 x 15 kHz subcarriers or 24 x 7.5 kHz subcarriers wide. The number of subcarriers used per RB for most channels and signals is 12 subcarriers. The number of RBs to allocate to each user varies depending on the available bandwidth. For example, if a bandwidth of 20 MHz is available, 100 RBs can be allocated. Every millisecond, the eNB decides how many RBs to assign to each user based on the Channel Quality Indicator (CQI) that has been communicated to it. CQI also determines which Modulation and Coding Scheme (MCS) the user can support. The CQI to MCS mapping foreseen in LTE-A networks is reported in Table 3.1 [114].

The eMBMS architecture, depicted in Figure 3-1, has been standardized to support multicast and broadcast services over LTE-A networks [112].

As explained in [124], the eMBMS architecture defines nodes belonging both

Table 3.1: CQI-MCS mapping in LTE-A

CQI index	Modulation Scheme	Efficiency D2D [bit/s/Hz]	Minimum Rate D2D [kbps]	Efficiency Cellular [bit/s/Hz]	Minimum Rate Cellular [kbps]
1	QPSK	0.1667	28.00	0.1523	25.59
2	QPSK	0.2222	37.33	0.2344	39.38
3	QPSK	0.3333	56.00	0.3770	63.34
4	QPSK	0.6667	112.00	0.6016	101.07
5	QPSK	1.0000	168.00	0.8770	147.34
6	QPSK	1.2000	201.60	1.1758	197.53
7	16-QAM	1.3333	224.00	1.4766	248.07
8	16-QAM	2.0000	336.00	1.9141	321.57
9	16-QAM	2.4000	403.20	2.4063	404.26
10	64-QAM	3.0000	504.00	2.7305	458.72
11	64-QAM	3.0000	504.00	3.3223	558.72
12	64-QAM	3.6000	604.80	3.9023	655.59
13	64-QAM	4.5000	756.00	4.5234	759.93
14	64-QAM	5.0000	840.00	5.1152	859.35
15	64-QAM	5.5000	924.00	5.5547	933.19

to the radio access network (E-UTRAN) and to the EPC. The *eNB* and the *multicell/multicast coordination entity (MCE)* belong to the E-UTRAN. The former is the evolved network node responsible for the direct interaction with users, the latter has to manage the coordination of the various eNBs (it allocates resources to each eNB and coordinates admission control). The EPC is composed by the *Broadcast Multicast-Service Center (BM-SC)* and the *Multimedia Broadcast Multicast Service-gateway (MBMS-GW)*. The first is responsible for the initialization of the Multimedia Broadcast Multicast Service (MBMS) session and for the management of some security functions (e.g., the authorizations for the MBMS subscribers), the second is in charge of forwarding the MBMS packets to the eNBs involved in the delivery service. These nodes need to be enhanced in order to support multicasting over 5G networks.

In order to efficiently manage the multicast and broadcast services over the 5G network, two main issues have to be faced: designing efficient radio resource allocation algorithms and providing trustworthy communications. With respect to the resource allocation problem, as previously discussed, the CMS approach [113] has been traditionally utilized for delivering multicast content because of its native short-term fairness capability. The possibility to improve the performance of CMS

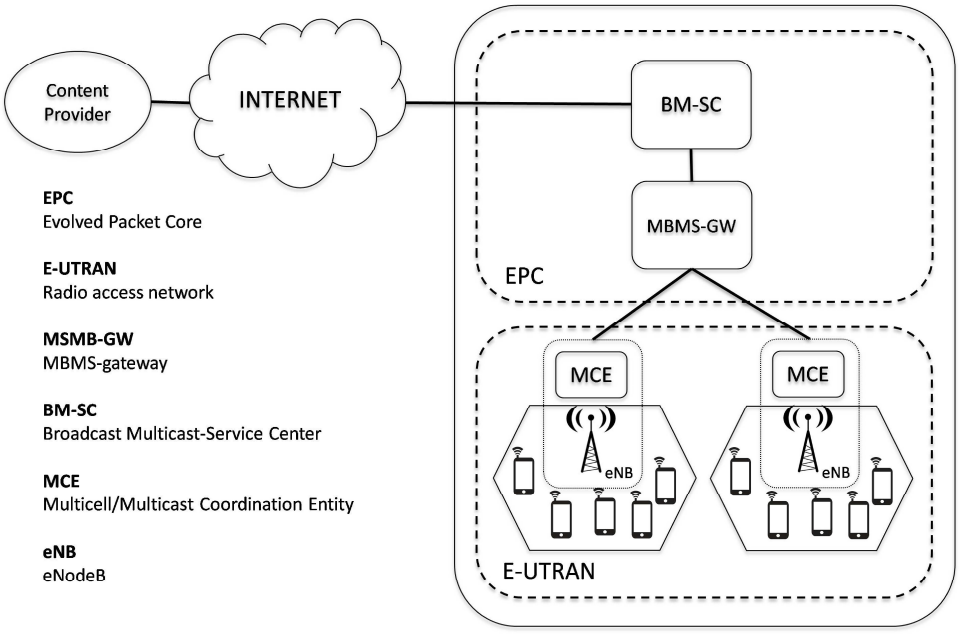


Figure 3-1: eMBMS architecture

by exploiting D2D communication has been proposed in [114]. But, since D2D communications are managed directly by the users, serious security problems arise.

3.3.1 Diffie-Hellman solution for security

A direct communication between devices over the wireless insecure channel is vulnerable to various types of attacks. Some basic security requirements have to be met in order to protect transmitted data and users' privacy. Among these, there are data confidentiality and integrity, authentication, non-repudiation, and reliability. According to Diffie and Hellman, cryptography is the best way to satisfy most of these requirements. In [131], they have proposed a *public key distribution system* suited to the scenario of two peers which have to exchange data in a secure way. Starting from the knowledge of two public keys, they can generate the same secret key to be used for both encrypting and decrypting data. The strength of the proposed technique is due to the difficulty of computing logarithms over a finite field (Galois Field) *GF(q)* with a prime number q of elements. Let:

$$Y = \alpha^X \bmod q, \qquad \text{for } 1 \leq X \leq q-1, \tag{3.1}$$

where α is a fixed primitive element of $GF(q)$ known to both users involved in the D2D communication, and X is the logarithm of Y to the base α, mod q, so that it can be computed as:

$$X = \log_\alpha Y \bmod q, \qquad \text{for } 1 \leq Y \leq q-1. \tag{3.2}$$

While computing Y from X is easy, the calculation of X from Y can be much more difficult. It is necessary to choose a number q consisting of many digits in order to make the system more robust. The security of the technique crucially depends on the difficulty of computing logarithms mod q. When users i and j want to communicate privately, first of all they must agree on the values of q and α. Then, each user generates an independent random number X_i, uniformly chosen from the set of integers $\{1, 2, 3, ..., q-1\}$, and keeps it secret. X_i is the logarithm of Y_i to the base α, mod q, where Y_i is the public key that user i must compute and send to j, computed as:

$$Y_i = \alpha^{X_i} \bmod q \tag{3.3}$$

The key used for both enciphering and deciphering by the two users is:

$$K_{ij} = \alpha^{X_i X_j} \bmod q \tag{3.4}$$

User i obtains K_{ij} by obtaining Y_j from user j and letting:

$$K_{ij} = Y_j^{Xi} \bmod q = (\alpha^{X_j})^{Xi} \bmod q = \alpha^{X_i X_j} \bmod q \tag{3.5}$$

Similarly, user j obtains K_{ij} as:

$$K_{ij} = Y_i^{X_j} \bmod q \tag{3.6}$$

For an untrusted third party it is impossible to generate the same key K_{ij}, since

it can not know X_i and X_j in any way because they are kept secret by users [131]. In addition to the DHKE algorithm, the use of message authentication can help to avoid the Man-in-the-Middle attack, which represents the main vulnerability of the DHKE algorithm.

3.4 The proposed eCMS-sD2D protocol

The reference scenario for the formulation of the introduced algorithm is composed by a set of devices interested in downloading data over the 5G network. This generic scenario is suitable to several types of applications, from software update to video downloading, and to both human-oriented and machine-oriented communications. Data transmission is accomplished over a multicast transmission by the eNB. The considered architecture is composed by all the nodes foreseen in the eMBMS standard architecture, but procedures must be improved to make multicast transmission more suitable for 5G networks. The proposed solution, called eCMS-sD2D, aims to enhance performance and security of a multicast CMS transmission. All steps of the proposed eCMS-sD2D solution are depicted in Figure 3-2.

Step 1 - Multicast service delivery notification

Through this first step, the eNB invites users interested in the service to form the Multicast Group (MG) by registering with the network.

Step 2 - CQI collection

Users belonging to the MG send their CQI values to the eNB. Each User Equipment (UE) has to communicate not only the cellular CQI value for its link towards the eNB, but also those for the D2D links to its neighbors. The eNB stores the received D2D CQI values in a matrix.

Step 3 - Multicast and D2D configuration selection

Thanks to the collected information, the eNB can establish: (i) the set of registered UEs to serve through the multicast transmission, (ii) the MCS to use for the

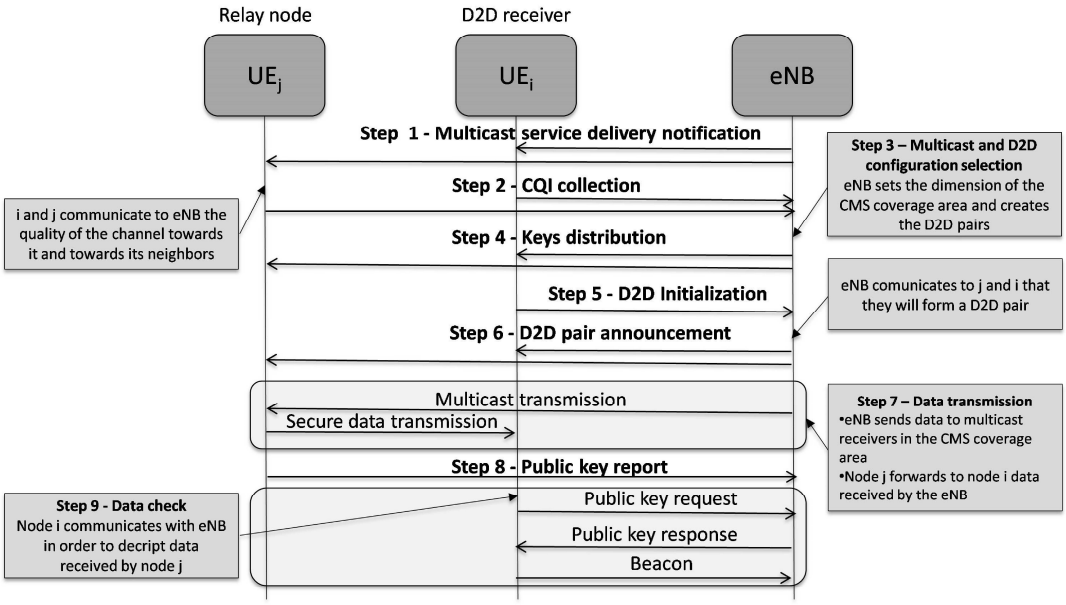


Figure 3-2: eCMS-sD2D procedures

multicast transmission in the CMS coverage area, (iii) the users served in multicast which can act as relay nodes by forwarding data received directly by the eNB towards the cell-edge users, (iv) the D2D pair to establish, and (v) the MCSs to use in each D2D communication.

The eCMS-sD2D approach envisages the formation of some D2D clusters composed by the selected RN and the associated users that it has to serve through D2D communications. Users inside the cluster receive the multicast content by the RN through unicast D2D communications, i.e., the RN will transmit the same content to each D2D receiver belonging to its cluster by setting the appropriate MCS to each D2D link.

The multicast and D2D configuration selection is accomplished through an iterative procedure. First of all, the eNB orders the received cellular CQI values from the lowest to the highest. For every CQI value, it determines the subset of UEs which can decode data transmitted with the correspondent MCS and the subset of UEs which, differently, are in worst channel conditions and must be served through D2D communications. Among all the eligible configurations (i.e., those in which

all UEs, belonging to the MG, receive all data), the eNB finally selects the one that guarantees the *maximization of system data rate*. Please refer to the *D2D-enhanced CMS with single frequency* solution presented in [114] for more details on the implementation of this step.

Once the multicast and D2D configuration is defined, the operations aimed at securing D2D communications are carried out. Security mechanisms described in the following are inspired by [119].

Step 4 - Keys distribution

In order to protect privacy of registered UEs, the eNB computes a pseudoidentity (PID) for each of them. For each UE_k that registered with the network using its real ID (RID_k) the eNB computes a pseudoidentity as: $PID_k = H_0(RID_k)$, where H_0 is a secure hash function, chosen and published by the eNB. In order to protect the privacy of the users and not increase the total overhead, the eNB never distributes the PIDs to the users, but each of them has to compute its PID autonomously, using the same function of the eNB (i.e., H_0). Then, through a secure control channel, the eNB sends to the D2D users their private and public keys. It obtains the first key by choosing $x_i \in Z_q^*$ (i.e., a set of integers with a prime number q of elements) and computes the second key as $X_i = g^{x_i}$, where g is the fixed primitive element of Z_q^* used as generator/base. Note that H_0, q, g, H_1, and the symmetric encryption algorithm $Enc_{key}()$ (the last two will be mentioned in the future steps) are all security parameters chosen and published by the eNB.

Step 5 - D2D initialization

After receiving the keys, the D2D receiver (in the following indicated by UE_i) sends an initialization message to the eNB. This message is composed by:

$$PID_i||P_i||z||h[(x_i^+ \oplus \text{opad})||h[(x_i^+ \oplus \text{ipad})||PID_i||P_i||z]] \tag{3.7}$$

where:

- P_i is the index of the portion of data that the user requires to receive. Indeed,

too large data can be divided into multiple portions, each identified by a specific index. The eNB keeps track of the portions of data sent to each user to avoid data retransmissions.

- $||$ is the operator used to concatenate strings;
- z is the first public key for generating the secret key k_c that will be used for data encryption and decryption. It is computed as $z = g^c$, where $c \in Z_q^*$ is randomly chosen by UE_i;
- $h[(x_i^+ \oplus \text{opad})||h[(x_i^+ \oplus \text{ipad})||PID_i||P_i||z]]$ is the $HMAC_{x_i}(PID_i||P_i||z)$. Generally, the $HMAC_k(m)$ is used to guarantee the integrity and authentication of the message m. It is based on the use of any cryptographic hash function h applied to a combination of the original message m and the secret key k. In Equation (3.7), x_i^+ is the key padded out to size, *opad* and *ipad* are specified padding constants. In the remainder of the Chapter, $h[(k^+ \oplus \text{opad})||h[(k^+ \oplus \text{ipad})||m]]$ will be expressed as $h(\bullet, k)$, where $\bullet$ denotes the message attached by the HMAC and k is the secret key hashed together with the message. Note that x_i is only known by the sender UE_i and the receiver eNB. In all future steps, the verification of the HMAC will always be performed by the recipients of the messages to verify message integrity and authentication, hence from here on this procedure will be omitted.

Step 6 - D2D pair announcement

After receiving the initialization message, the eNB authenticates the requesting user in the normal cellular communication mode, obtaining its RID and checking if it is registered. In positive case, the eNB has to inform both D2D devices involved in the direct communication of their imminent communication. So, it randomly selects $a \in Z_q^*$ and computes $u = g^a$ as the first public key for generating the secret key k_s to use in the exchange of private messages with the selected D2D transmitter (i.e., the RN). To communicate to UE_j that has been chosen as RN of the D2D communication, the eNB sends to it the following message:

$$PID_j||PID_i||z||u||P_i||h(\bullet, x_j) \tag{3.8}$$

Simultaneously, to acknowledge the reception of the initialization message, the eNB sends to UE_i a response message with PID and public key of the selected RN:

$$PID_i||PID_j||X_j||P_i||h(\bullet, x_i). \tag{3.9}$$

Step 7 - Data transmission

First of all, the eNB must sign with σ_1 data to send to devices:

$$\sigma_1 = H_1(P_i||M)^{x_0} \tag{3.10}$$

where H_1 is a secure hash function, x_0 is the private key of the eNB, M is data to be transmitted. After that, it performs multicast transmission to users with the best channel conditions, using a CMS.

UE_j, which has received data sent by the eNB, has to forward them to the previously notified D2D receiver. Then, it carries out all the operations aimed at securing D2D communication. First of all, to allow the receiver to generate the secret key k_c, it randomly selects $b \in Z_q^*$ and computes $y = g^b$ as the second public key for k_c. It does not send y directly to the UE_i but it sends it to the eNB, randomly choosing $f \in Z_q^*$, generating the secret key $k_s = u^f = g^{af}$ and using it to encrypt the public key y. Then, UE_j must encrypt data, so it generates the communication key $k_c = z^b = g^{cb}$ and uses it to encrypt the data M. After computing $M' = Enc_{k_c}(M)$, UE_j signs the message by calculating:

$$\sigma_2 = H_1(PID_j||P_i||M'||T_s||\sigma_1)^{x_j} \tag{3.11}$$

where T_s is the timestamp used against the replay attack. Thus, the secure D2D communication takes place when the RN sends the following message to the receiver:

$$PID_i||PID_j||P_i||M'||T_s||\sigma_1||\sigma_2 \tag{3.12}$$

Step 8 - Public key report

In order to allow the eNB to generate the secret key k_s used to encrypt the public key y, UE_j computes $v = g^f$ as the second public key for k_s, using $f \in Z_q^*$ chosen in the previous Step. So, it sends to the eNB a report:

$$PID_i||PID_j||P_i||Enc_{k_s}(y)||v||T_s||h(\bullet, x_j) \tag{3.13}$$

Step 9 - Data check

After receiving data, UE_i first has to verify the identity of the transmitter. To this aim, it compares the PID_j reported on the message received by UE_j with that communicated by the eNB and, if the two do not match, the packet is dropped, otherwise it proceeds with the next steps. So, it checks the signature of the transmitter (i.e., σ_2) and, if it is valid, data are considered sent by the entity corresponding to PID_j. Once the identity of the sender is verified, UE_i needs to generate the decryption key k_c to obtain the plaintext. To do this, it sends a public key request message to the eNB:

$$PID_i||PID_j||P_i||T_s||h(\bullet, x_i) \tag{3.14}$$

After receiving this message, the eNB decrypts the $Enc_{k_s}(y)$, first generating the decryption key k_s, and sends the response message to UE_i:

$$PID_i||PID_j||P_i||y||T_s||T_i||h(\bullet, x_i) \tag{3.15}$$

where T_i is employed to record the feedback time.

It is important to underline that in the traditional DHKE algorithm, public keys are exchanged directly between the direct-communicating users. Instead, in eCMS-sD2D the public keys exchange is mediated by the eNB, which represents the trusted third party. This can help to avoid the Man-in-the-Middle attack.

Thanks to the reception of the public key y, UE_i can get the communication key by computing $k_c = y^c = g^{bc}$. So, it can decrypt the message M' to obtain the

original data M. To verify the origin of data, it also checks the signature σ_1 and, if it is valid, data are accepted, otherwise, it is possible that data may have corrupted. In this case, UE_i must send to eNB a *beacon* in order to report the fabrication of the original data and to allow it to identify the attacker:

$$\beta = PID_i||PID_j||P_i||M'||T_s||\sigma_1||\sigma_2||h(\bullet, x_i) \tag{3.16}$$

The beacon must be sent within the timestamp T_i', which satisfies the condition $T_i' < T_i + \Delta T$, where ΔT is the time interval, starting with T_i, where the eNB is willing to wait for feedback from UE_i.

Thanks to Equation (3.16), the eNB must keep track of any malicious behavior of users. If beacon arrives during the time interval ΔT, the eNB first checks the validity of σ_1 and, if it is invalid, it is judged that data are not the original ones and may be fabricated by the transmitter. So, the eNB also verifies the validity of σ_2 to ensure that the fake message comes from the entity corresponding to PID_j. A *malicious behavior amount (MBA) counter* is stored by the eNB for each user which does not transmit data correctly in the D2D communication. Thus, in case of a malicious behavior of UE_j, the eNB increments by one its MBA counter. When a user's counter exceeds a given threshold, named maliciousness threshold, the user is punished by the network, i.e., it is excluded from future communications. The maliciousness threshold belongs to the interval $[0, \infty)$. Its value is of utmost importance in the evaluation of the performance of the proposed protocol, as it determines its degree of selectivity. A user $UE_k \in N$ (where N is the set of registered users) can be chosen as RN only if its MBA value is less than or equal to the maliciousness threshold, i.e. the following condition must be verified:

$$MBA_k \leq THRESHOLD \tag{3.17}$$

This means that the value of the threshold represents the maximum number of malicious behaviors tolerated to allow a user playing the role of transmitter (i.e., RN) in a D2D communication. When it is set to zero, only users with a MBA value equal to zero can be selected as RN, which means that selecting a malicious user

is only possible if the user has never had a malicious behavior in the past. As the value of the threshold increases, the algorithm is always less selective, this means that more users which in the past have already behaved maliciously can be chosen as RN.

3.5 Performance evaluation

A simulative analysis in MATLAB has been performed to study the performance of the proposed eCMS-sD2D protocol. The considered scenario consists of a variable number of users uniformly distributed in a single LTE-A cell of dimension 100m x 100m, with available bandwidth of 20 MHz, which corresponds to 100 RBs. A Time Division Duplex (TDD) LTE frame type 2 configuration 3 is used. Each slot (or Transmission Time Interval (TTI)) in the frame lasts 1 ms, so the entire frame has a duration of 10 ms. The inband D2D mode is chosen, so uplink slots are reserved to D2D communications. In the downlink slots, a multicast transmission allows to send data to in-coverage devices.

The performance of the proposed eCMS-sD2D protocol is evaluated on the basis of the following metrics:

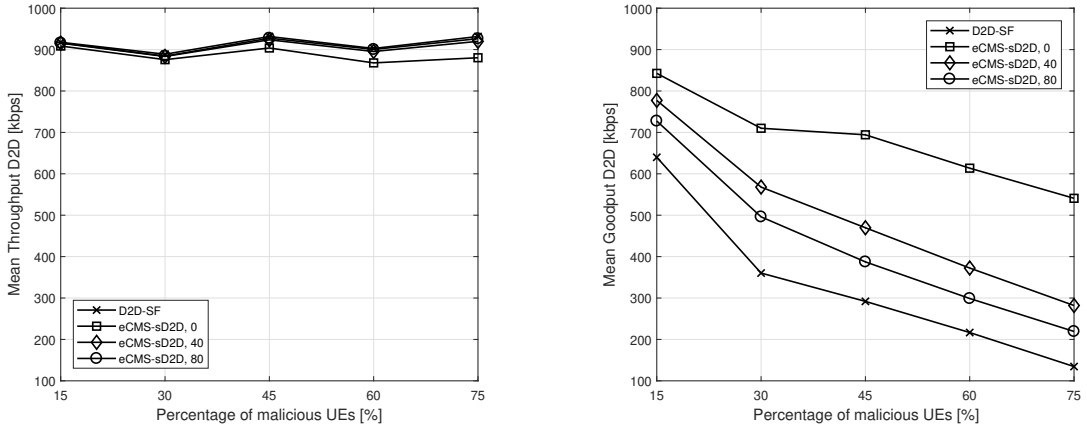
- *Data loss* in D2D communications because of an unreliable transmitter;
- *Mean Throughput*, measured as the mean data rate value experienced by the D2D receivers. It is independent of the nature of the communication transmitter (i.e., if it is malicious or not). In particular, even if the data transmitter is a malicious user, the amount of data it delivers is counted in the throughput computation;
- *Mean Goodput*, measured as the mean useful data rate value experienced by the D2D receivers (i.e., rate of data that has been forwarded by non malicious transmitters). This metric takes into account the reputation of the user. In fact, if a RN behaves maliciously, the amount of data that it delivers does not cause a goodput increase;

- *Aggregate Data Rate (ADR)*, computed as the sum of the data rates experienced by the D2D receivers;
- *Good ADR*, computed as the sum of the useful data rates experienced by the D2D receivers;
- *Mean number of malicious nodes* accounting for malicious D2D receivers that have been served and selected relay nodes;
- *Mean number of malicious relays* that have been selected to transmit data in D2D communications.

In the following simulation results, the proposed eCMS-sD2D is compared with the existing protocol presented in [114], in which the security of D2D communications is not guaranteed. The performance of eCMS-sD2D are analyzed by considering three different values of the maliciousness threshold (equal to 0, 40, and 80).

The results in terms of mean throughput and goodput are presented in Figure 3-3(a) and (b), respectively, under increasing percentage of malicious UEs. By looking at Figure 3-3(a), curves are almost overlapping, because throughput does not depend on security. Differently, the results in terms of goodput depicted in Figure 3-3(b) are substantially different. In fact, D2D-SF exhibits significantly lower performance with respect to eCMS-sD2D that achieves goodput values as close to the throughput as the maliciousness threshold is lower. In detail, as the threshold increases, eCMS-sD2D becomes less selective, therefore more similar to D2D-SF, in which no selection is applied in the choice of RNs. On the contrary, when the maliciousness threshold is set to zero, eCMS-sD2D shows the better results since also nodes that behaved maliciously just once are not selected as RN.

A similar reasoning holds for the ADR metric. In fact, looking at Figure 3-4, while the ADR is almost identical for eCMS-sD2D (under all maliciousness thresholds under analysis) and D2D-SF, the good ADR is significantly lower than ADR when no security mechanism is implemented (see the last pair of bars). Furthermore, the increment of the maliciousness threshold causes a performance degradation since security mechanisms are less stringent.



(a) (b)

Figure 3-3: Mean (a) throughput D2D and (b) goodput D2D for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, under increasing percentage of malicious nodes

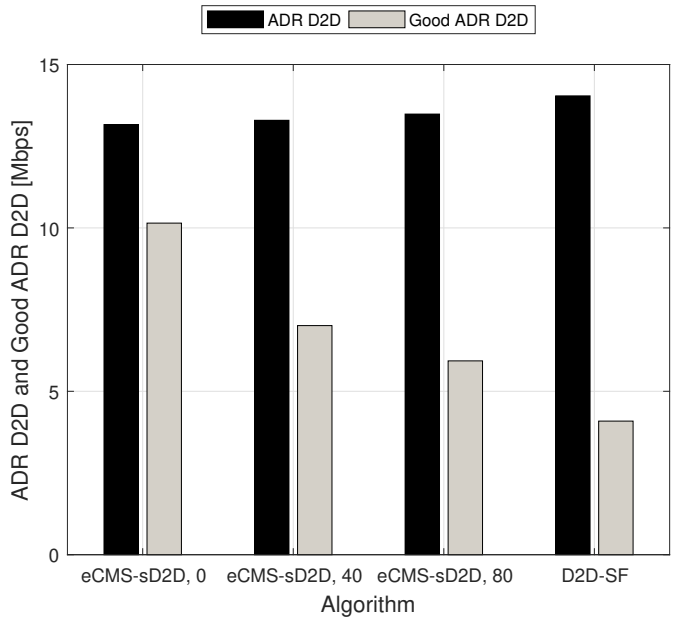


Figure 3-4: Comparison between ADR D2D and Good ADR D2D for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, with 75% of malicious nodes

This significant degradation of the goodput/good ADR is due to the high amount of data loss, as confirmed by Figure 3-5. Thanks to the implementation of the security mechanisms foreseen in eCMS-sD2D, data loss can be reduced of about 70%. In particular, when the maliciousness threshold is set to zero, thanks to the better selection of RNs, eCMS-sD2D shows the best results. Nevertheless, data loss is not zero, due to the fact malicious RN can be identified only after the eNB detects an incorrect behavior. As the threshold value increases, the efficiency of eCMS-sD2D in terms of selection of RNs is always lower, so the results are increasingly similar to D2D-SF.

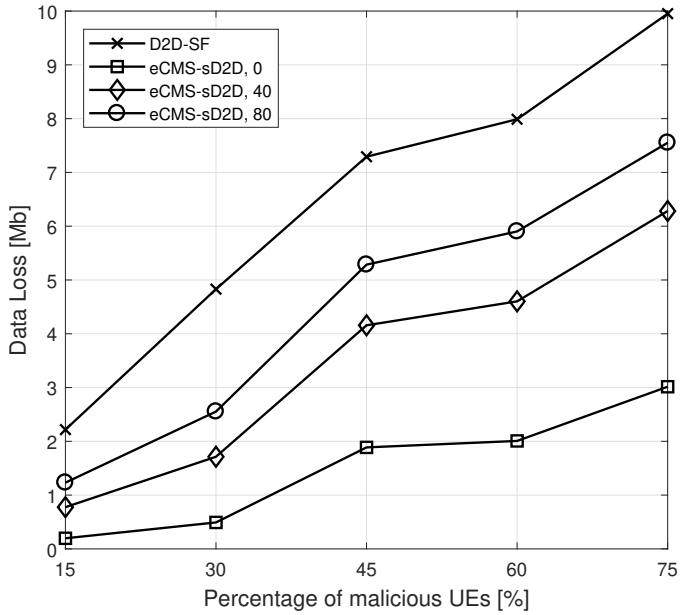


Figure 3-5: Data loss for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, under increasing percentage of malicious nodes

Because of security, as shown in Figure 3-6, the mean number of malicious D2D UEs that gain service is reduced (see the first bar with respect to the forth bar). However, despite this metric shows an improvement of about 10%, it takes into account both malicious users served by the CMS transmission (on which the security mechanisms do not have impact) and selected malicious RNs. This is the reason why the performance improvement of eCMS-sD2D with respect to D2D-SF is limited. Going more in depth in the analysis, Figure 3-7 show the mean number of selected malicious RNs under increasing percentage of malicious users. The reduction in the

number of selected malicious RNs is of more than the 50% also in case of a high number of malicious nodes (75% of malicious nodes).

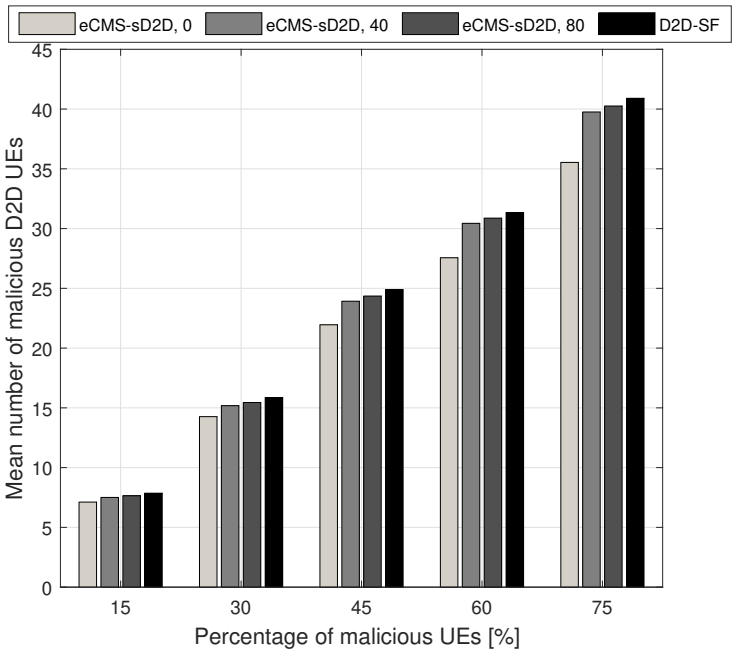


Figure 3-6: Mean number of malicious D2D nodes for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, under increasing percentage of malicious nodes

3.6 Conclusions of Chapter

In this Chapter an innovative protocol has been described, called eCMS-SD2D (enhanced CMS with secure D2D communications), which aims to ensure a secure management of a multicast service while also efficiently utilizing network resources of the a 5G network. In doing this, mechanisms as signature and encryption have been implemented in order to increase the data protection and the privacy when nearby devices aim of transmitting each other through proximity-based links (e.g., D2D). The outcome of the performance evaluation shows that, with the proposed approach, it is possible to decrease the data loss caused by malicious users (considered in the reference scenario) by guaranteeing, at the same time, reasonable data-rate to the users within the multicast group during a radio transmission.

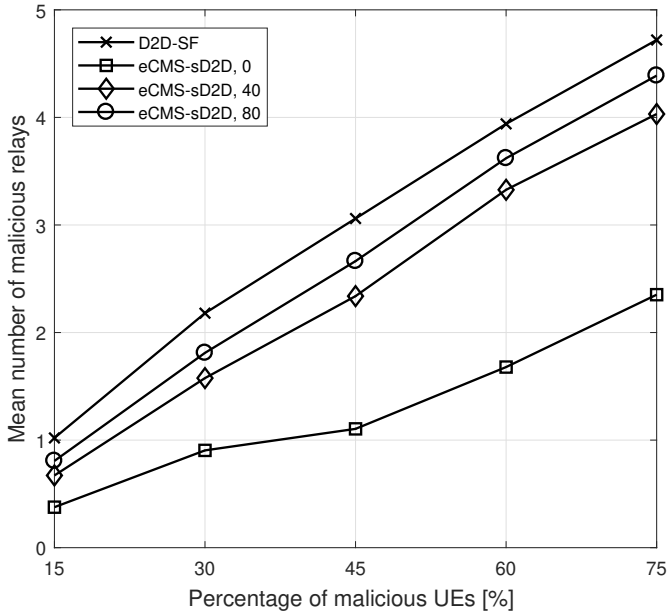


Figure 3-7: Mean number of malicious relays for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, under increasing percentage of malicious nodes

Chapter 4

A trustworthiness model for security in 5G networks

The design of the 5G systems has met the severe requirement of managing an always increasing amount of traffic generated by both humans and machines, while guaranteeing data security. Among the enabling technologies that can turn 5G into a reality, D2D and Multicasting certainly play a key role because of their capability to largely improve network resources utilization and to address emerging use cases requiring the delivery of the same content to a large number of devices. D2D communications can help to improve traditional point-to-multipoint transmissions by reducing the multicast coverage area and exploiting properly selected relay nodes as data forwarders towards users with worse channel conditions. However, security issues are even more challenging for D2D connections, as data exchange happens directly between nodes in proximity. To enhance performance and security of delivered traffic in 5G-oriented networks, in this Chapter the Secure and Trust D2D (SeT-D2D) protocol is introduced, according to which trustworthiness inferred from both direct interactions and social-awareness parameters is exploited to properly select relay nodes. Main contributions of this research product consist in the introduction of a model for the assessment of network nodes' trustworthiness and the implementation of security mechanisms to protect the data transmitted in D2D communications and the privacy of the involved users. The conducted simulation campaign testifies to the ability of the proposed solution to effectively select relay

nodes, which leads to an improved network performance.

4.1 Introduction to Chapter

Autonomous driving, tactile Internet, virtual and augmented reality, broadband and media everywhere, seamless connection of pervasive embedded sensors are just examples of the most attractive yet challenging use cases that the 5G network will turn into reality. D2D and Multicasting communications are expected to play a key role in helping to satisfy the demanding requirements of the foreseen use cases. The former, thanks to its capability to offload cellular data traffic, enhance spectrum efficiency, and extend cell coverage [121]; the latter, thanks to its capability to answer the increasing demand for multicast/broadcast multimedia services (such as, mobile TV, IP radio broadcasting, and video streaming and downloading) [111].

Multicast transmissions represent the top notch solution to deliver group-oriented services, since multiple users can be fed through a single PtM transmission by exploiting the broadcast nature of the radio channel. In order to handle multicast and broadcast services over cellular networks, the 3GPP has standardized the eMBMS [112].

The traditional approach to multicast traffic delivery in cellular networks is the so-called CMS [113], which guarantees perfect fairness, since all users are served and receive the same treatment, although it suffers from poor performance levels because users with good channel conditions are constrained to the lowest data rate that cell-edge users can sustain. This is why in several works in the literature, D2D communications are exploited to improve the performance of multicast service delivery [114, 125, 132, 133]. An interesting approach to select D2D transmitters, based on the channel conditions of the links between the D2D peers, for example, is proposed in [114].

The 5G system leveraging the mentioned solutions is, however, exposed to severe security threatens. Besides the magnified risk of security threats due to the huge number of 5G connected devices, D2D communications can raise further issues due to the direct connections between devices in proximity [118]. To make 5G a trustworthy

multi-service platform, resilience, communication security, identity management, privacy and security assurance must be provided [115].

In this Chapter, a mechanism to effectively deliver trustworthy multicast/broadcast traffic in 5G-oriented networks, named SeT-D2D, is presented, whose novelty is that two contributions are considered in computing node's trustworthiness: (i) the one derived from *direct interactions*, thus based on the actual behavior of the node following its selection as a relay node, (ii) and the other based on *social trustworthiness* parameters, thus able to give a first evaluation even in absence of previous interactions. The idea of using both contributions stems from the fact that, especially in its early stages, it is very likely that a requester node has not interacted directly with a service provider (i.e., the RN) in the past; therefore, the latter is unable to properly evaluate its maliciousness due to the unavailability of information on its trustworthiness. This issue is called *cold start problem* in the literature, and implies that several interactions have to take place before a node is able to understand if another node is malicious or benevolent. The trustworthiness model introduced in this Chapter considers both contributions to face this problem. Furthermore, security techniques are implemented in the presented SeT-D2D to protect the data transmitted via D2D communications and the privacy of users involved in the transmission. Namely, data transmitted in D2D are encrypted by using a symmetric encryption algorithm for which the two peers generate the secret key by leveraging the DHKE protocol. Another innovative factor compared to other existing works on D2D communications is that user identity privacy is preserved through the use of Subscription Concealed Identifier (SUCI) derived from the Subscription Permanent Identifier (SUPI) according to the 3GPP TS 33.501 [134].

The remainder of the Chapter is organized as follows. In Section 4.2 useful background information are provided. Section 4.3 and 4.4 are about, respectively, a brief overview of related works in the area of reference and a detailed description of the proposed SeT-D2D protocol, while Section 4.5 outlines the designed trustworthiness model. Results from the performance analysis are shown in Section 4.6. Conclusive remarks are given in the last Section.

4.2 Background

4.2.1 The 5G ecosystem

The 5G cellular network deployment involves a radical change compared to previous generations. A plethora of innovative technologies are expected to be utilized, thanks to which novel use-cases will be supported. Based on use cases' requirements, three different service categories have been defined: *(i) enhanced Mobile Broadband (eMBB)*, which includes services demanding very high peak data rates and improved QoE (e.g., ultra high definition TV); *(ii) mMTC*, which require connectivity for a massive number of energy-constrained IoT devices; *(iii) Ultra-Reliable and Low Latency Communication (URLLC)* supporting the most stringent requirements in terms of reliability and latency (e.g., V2X applications) [135, 61]. Thus, "flexibility" is the key design concept in 5G networks to meet the diverse requirements of each category. In this view, SDN, NFV, and D2D communications are among the more promising enabling technologies that the 5G system can exploit [57]. In particular, the D2D paradigm enables two devices to exchange data directly without going through the network. Countless benefits can be brought by D2D technology to cellular communications, among which high data rate, low latency, extension of the network capacity, energy saving, and network offloading stand out. While on the one hand the 5G enabling technologies will allow the network to offer a greater number of services at improved conditions, on the other hand several new challenges must be faced, especially regarding network architecture and security.

4.2.2 Security means

The DHKE algorithm is a well-known method for securely exchanging cryptographic keys, particularly suited to the generation of a secret between two peers since it requires only the exchange of information that, even if intercepted, does not allow an eavesdropper to obtain the secret. A critical vulnerability of DHKE is the Man-in-the-Middle attack, in which a malicious user impersonate a legitimate peer.

The concealment of the SUPI is another important security mechanism to ensure

the protection of user privacy. The 3GPP specifies that, in order to preserve the subscribers privacy, *the SUPI should not be transferred in clear text over NG-RAN (5G RAN) except routing information* [134]. Thus, following 3GPP guidelines, SUCI has to be transmitted during authentication procedures [134]. It is calculated by encrypting a part of the SUPI with the Home Network Public Key securely provisioned by the home network. Only UE and home network can de-conceal the SUCI to obtain SUPI; in the home network, the Subscription Identifier De-concealing Function (SIDF), located at the Authentication credential Repository and Processing Function / Unified Data Management (ARPF/UDM), is responsible for this functionality. The reference architecture for the protocol presented in this Chapter is that described by 3GPP in [136], from which Figure 6-1 is taken, with the addition of security features and procedures described in [134]. As reported in [134], only in three cases the protection of the SUPI may be missing: *(i)* unauthenticated emergency sessions, *(ii)* if the home network has set null-scheme to be used, *(iii)* if the home network has not provisioned the public key needed to generate a SUCI.

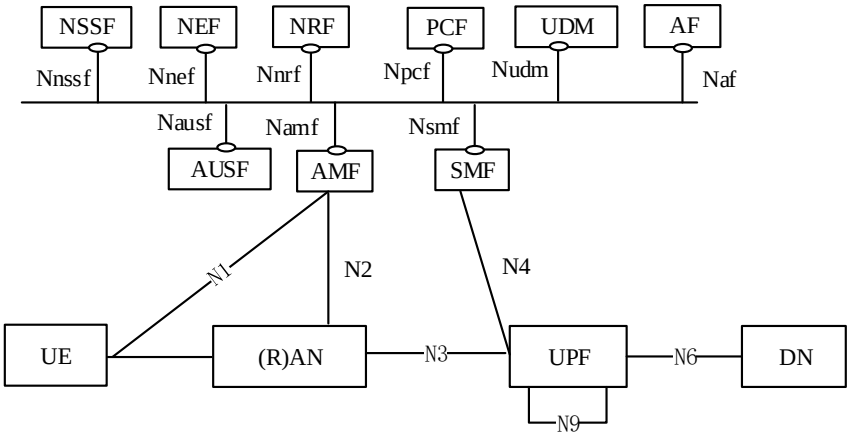


Figure 4-1: The reference 5G architecture [136]

4.2.3 Evaluating nodes' trustworthiness

In the research area addressing secure and trusted D2D communications, the social trustworthiness is considered a valuable means.

The literature uses the term *trustworthiness* (in brief, trust) with a variety of meanings. In this Chapter it is referred to by adopting one of its main interpre-

tations: the *reliability trust*. The reliability trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends. Two fundamental concepts of the theory of trustworthiness are: (1) *functional trust*, that is the trust in the ability of a node to provide services, and (2) *referral trust*, that is the trust in the ability of a node to provide recommendations. In the scenario examined in this Chapter, referral trust is not considered, since the centralized nature of the network architecture makes it lose meaning, and the functional trust, here denoted by the term *service trust*, is of primary importance. The service trust (st) is the trustworthiness parameter used to measure the trust in nodes' ability to provide services. Several trustworthiness models have been proposed for different technologies and architectures, ranging from Peer-to-Peer (P2P) to IoT and Social IoT (SIOT).

In the social-trustworthiness-related literature, a fundamental parameter is represented by the *service integrity belief* (in brief, integrity), that allows to predict the behavior in future interactions and to obtain a trustworthiness value closer to Ground truth. In this way, the calculation of trustworthiness is not based only on the degree to which a node has satisfied past interactions (i.e., the competence), but also on the deviation in the degree of satisfaction of the recent interactions with respect to the remote ones (i.e., the integrity).

The *decay (or decaying) factor* indicates the expiry of data related to a given transaction. For the computation of the decay factor, some trustworthiness models consider only a number of transactions occurred after the one considered (current validity of the interaction or cardinal contribution), while others consider the time elapsed from the considered transaction (recency of the interaction or temporal contribution). However, the joint use of both contributions would allow a better estimate.

In the proposed trustworthiness model, an *indirect contribution* is considered for assessing the trust of a node that, based on various parameters (i.e., relationship factor, centrality, and intelligence), allows to evaluate the trustworthiness of a node even in the absence of direct interactions. Considering both a direct and an indirect contribution in trust computation allows to mitigate the cold start problem, as ex-

plained in Section 4.1. More details about how the indirect contribution is measured are given in Section 4.5.

4.3 Related work

4.3.1 D2D for multicasting and related security issues

Considered as one of the most important technologies for 5G, D2D communication has been the subject of a vast scientific literature [121, 114, 133]. In [114], D2D technology is presented as the means to improve the performance of a *multicast* transmission via the establishment of direct communications between devices in proximity. Also in [125], D2D communications are considered highly valuable to improve content sharing in 5G cellular networks, since they can offload traffic from cellular base stations and guarantee an efficient management of radio resources. The problem of power and channel allocation to multicast D2D communications is tackled in [132] where two different solutions are proposed, both demonstrating the superiority of multicast D2D performance, especially in terms of throughput. In the mentioned research, not enough attention has been put on security, which is of paramount importance for 5G. As evidence, a security architecture for 5G networks is defined in [137], where network segments are logically divided into *Security Realms (SR)*. For each of them, security controls that could be implemented are classified in *Security Control Classes (SCC)*.

Privacy and security issues must be faced to definitely make D2D a successful technology for 5G systems. In [117], a thorough analysis on these problems is conducted. First, the difference between security and privacy concepts is defined. Then, the requirements to be satisfied in order to guarantee both security and privacy in D2D communications are listed, possible attacks identified, and solutions suggested. In [118], security solutions proposed to improve D2D in 5G networks are analyzed. In addition, when dealing with D2D security requirements, threats, and solutions, this work hints at the role that social relationships could play in this context.

A secure data sharing strategy able to guarantee D2D privacy and security in LTE-A networks is proposed in [119]. The SeT-D2D algorithm aims to overcome

the gaps of this interesting research, providing a twofold contribution. First, until a node is selected as a D2D transmitter, there is no information on its nature. Second, once a node is punished because of its malicious behavior, there is no way to redeem its reputation. The latter can be a problem when a node that usually performs efficiently and trustfully is actually itself a victim of attack and temporary performs some malicious behaviors. From this time on, it is considered not eligible any more for the role of D2D transmitter and there is no way to rehabilitate it; if this node has the potential to be more efficient than others, an avoidable degradation of communications performance is observed.

4.3.2 Social trustworthiness models

The benefits of proximity-based mobile social networking are discussed in [138]. In [139], devices' characteristics (such as brand, type of friendship with other nodes, and computational capabilities) are considered to compose the social trustworthiness of each node, to the purpose of setting up trustworthy D2D communications between nodes with a good reputation. In [140], a paradigm melting social trustworthiness and D2D communications is introduced to extend the coverage area of future 5G cells through the use of reliable relays. A framework that designs the caching based D2D communication scheme by taking social ties among users and common interests into consideration is proposed in [141].

The Self-ORganizing Trust (SORT) model for P2P scenarios is proposed in [142]. Each peer computes the trustworthiness of other peers based on past interactions and recommendations, by using only locally available information. In particular, they measure the trustworthiness in providing services and in giving recommendations. To evaluate interactions and recommendations, they use importance, recentness, and peer satisfaction parameters. The introduction of the concept of integrity, as "the level of confidence in predictability of future interactions", is one of the major contributions of [142]. A flaw of the model in [142] concerns the decay factor, which only considers the cardinal contribution.

In [143], the authors present an access service recommendation scheme in a SIoT scenario which considers the social relationships among things. An energy-aware

mechanism is also proposed to be utilized as a restrictive factor in trustworthiness evaluation. Even the recommendation is based not only on the past performance but also on the social relationship and on the energy status of nodes. Also in the model presented in [143], the decay factor is evaluated as a useful contribution to the computation of the trustworthiness of the network nodes. However, only the temporal contribution is considered, which leads to the previously discussed drawbacks.

Another well-known trust model in P2P systems is Peertrust [144]. It presents a transaction-based feedback system built on three basic parameters and two adaptive factors: the feedback that a peer receives from other peers, the total number of transactions that a peer performs, the credibility of the feedback sources, the transaction context factor, and the community context factor.

In [145], the authors propose to use reputation as a means to establish the reliability trustworthiness of resources in a P2P scenario. In addition, an approach to manage and exchange reputations, based on the use of fuzzy techniques, is presented.

A scalable, adaptive, and survivable trust management protocol in a dynamic IoT environment is designed and evaluated in [146]. Since entities in an IoT system are connected via the social networks of the entity owners, a social IoT based Community of Interest (CoI) is considered. The same authors, in [147], propose an adaptive trust management protocol for SIoT systems in which social relationships evolve dynamically among the owners of IoT devices. According to this approach, a social IoT application can adaptively choose the best trust parameter settings in response to changing IoT social conditions.

Two other noteworthy works are [148] and [149]. In [148], each node computes the trustworthiness of its friends on the basis of its own experience and on the opinion of the friends in common with the potential service provider. To evaluate the trust level, a feedback system is used and the credibility, the centrality, and the intelligence of the nodes are combined. Differently, in [149], information about each node is distributed and stored by making use of a distributed hash table structure so that any node can exploit the same information.

4.3.3 Main novelties introduced by the proposed trustworthiness model

The designed trustworthiness model has the main purpose to provide a *fine-grain detection of service supply profile changes*. To achieve this goal, the following features are leveraged:

- Both *direct* and *indirect* contributions are considered, which are clearly separated and properly weighted. This allows greater control over the weight that can be associated (even dynamically) to each contribution. This choice derives from the opinion, broadly shared in the literature [142, 143, 145, 146, 148, 149], that this approach enables an easy runtime tuning of these two main contributions. Furthermore, the indirect contribution has been designed with the aim to mitigate the cold start problem.

- Each parameter contributing to the trust computation is *properly weighted* to improve the adaptability to the considered scenario. This design principle has been used in [143, 148, 149] for the indirect contribution, and in [142] for the direct contribution. As an example, weighting the integrity parameter allows to set possible punishments. Depending on the reference scenario, the central controller (e.g., the Next Generation NodeB (gNB)) can decide the degree of harshness of the punishment given to a relay node providing a bad service. The simulative results that will be presented in the following of this Chapter demonstrate that, by correctly calibrating the integrity weight, the desired decrease of service trust is obtained. In this way, a service trust value closer to the Ground truth is reached.

- In the computation of the *integrity* parameter, the assessment of how the short-term service opinion deviates from the long-term service opinion is proposed. A different approach is followed in [142], where the deviation from the average behaviour is calculated based on the deviation of the last satisfaction value (associated to the last transaction) from the average value of satisfaction computed over past transactions. The motivation behind the choice made in

the proposal presented in this Chapter is that considering short-term service opinion and long-term service opinion allows to obtain the expected service integrity belief and a service trust very close to the Ground truth.

- Both the cardinal and the temporal contributions are considered in the computation of the *decaying factor* to its approximation to the Ground truth. In particular, the temporal decay can be better evaluated in scenarios where the considered interaction is occurred a long time before (long time interval), although it is among the last ones occurred (from a cardinal point of view). Also the cardinal decay can be better evaluated in scenarios in which many interactions occurred after the one considered (short time interval), although this latter is recent. In the literature, only the temporal contribution [143] or only the cardinal contribution [142] is considered.

4.4 Providing trusted D2D communications in 5G-oriented networks

In the reference scenario, devices located in the same coverage area are interested in downloading the same data. Main purpose of the proposed protocol is to optimize the data delivery from the provider to the network nodes, resorting to the establishment of *secure and trusted D2D communications*. *(1)* The *D2D* implementation is finalized to support the multicast communication and to avoid that a mere CMS transmission penalizes all the receiving devices, by imposing to all disadvantageous transmission conditions caused by the cell-edge nodes. *(2)* D2D communications are *trusted* because an innovative model is introduced to assess the trustworthiness of potential D2D transmitters, in order to select trustworthy relay nodes. *(3) Security* in D2D is fixed, since the privacy of communicating devices is preserved and data transmitted are protected through the implementation of a symmetric encryption algorithm, for which the secret key is generated according to the DHKE protocol.

In detail, according to the proposed SeT-D2D protocol, devices with the best channel conditions are served directly by the gNB through a CMS transmission.

Then, data are sent to cell-edge devices (i.e., those excluded from the multicast transmission because of their bad channel conditions) through secure D2D communications. Security is achieved by carefully selecting the D2D transmitters, referred to as relay nodes, and the implementation of some security mechanisms (such as DHKE, HMAC, and cryptography) aimed at guaranteeing confidentiality and integrity to data exchanged between devices in proximity. The selection parameters considered to choose the best RN for each D2D communication are: the channel quality indicator relative to D2D link (i.e., D2D CQI) and the trustworthiness of cell nodes.

According to the 5G security architecture presented in [137], Table 4.1 reports the SR-SCC mapping related to the use case analysed in this Chapter (i.e., secure D2D data transmission). In the *access network* domain, the gNB shall be responsible for managing the credentials of users and protecting their privacy; moreover, identity of users has to be verified. In the *application* realm, data destinations shall be controlled since only registered users shall be reached; furthermore, the true identity of users shall not be revealed to the applications, therefore, fake identities could be used to reach them. For an effective *management* of the overall network, some security mechanisms have to be implemented in order to provide information about the trustworthiness of the system. Finally, the *UE* realm includes the "other UE domains" that also cover D2D communications. Data transmitted during the direct communication between devices shall be confidential and their integrity be protected. To this aim, security keys could be used to allow data encryption. In addition, the privacy of users shall be protected and the identity of the devices involved in the direct communications be checked to track any possible malicious behavior. As regards *network* and *infrastructure & virtualisation*, i.e. the last two realms presented in [137], the security mechanisms proposed in this Chapter do not affect these network segments, thus no security control class is reported for them.

The proposed SeT-D2D protocol aims to implement the reported security controls for each security realm. In the following, all steps of SeT-D2D are described in detail.

Table 4.1: SR-SCC mapping for the reference use case of SeT-D2D

Security realms (SR)	**Security control classes (SCC)**	**Security control examples**
Access Network	Authentication, Identity and Access Management, Privacy	Credentials management, privacy protection, identities checks.
Application	Identity and Access Management, Privacy	Data destinations controls, use of fake identities for privacy protection.
Management	Trust and Assurance	Knowledge of system trustworthiness.
User Equipment	Confidentiality, Integrity, Authentication, Privacy, Non-Repudiation	Security keys management, data encryption, D2D users identities checks, D2D users privacy protection.
Network		
Infrastructure & Virtualisation		

4.4.1 Multicast service delivery notification

Initially, the gNB announces the multicast service. It invites interested users to form the MG by registering to the network.

4.4.2 Registration & Authentication

Users must register to enjoy the multicast service notified by the gNB. Mutual authentication between UE and network is a primary requirement to ensure the security of both. Thus, the authentication procedure described by 3GPP in [134] is implemented in the SeT-D2D algorithm. According to [134], Extensible Authentication Protocol for Authentication and Key Agreement (EAP-AKA') and 5G AKA are the protocols supported for the mutual authentication between UE and network. In particular, the ARPF/UDM node selects the proper authentication method for the user based on its SUPI and the subscription data. As already mentioned in the previous sections, the subscriber privacy is protected through the concealment of its permanent identifier to eavesdroppers on the air interface; the SUCI is transmitted in its place for this purpose. The likelihood of the occurrence of a SUPI catching attack is much lower than that of International Mobile Subscriber Identity (IMSI) catching [150], nonetheless 3GPP states that, in some cases, SUPI is at risk of being exposed to attackers (see Section 4.3). For the scope of the definition of the SeT-

D2D protocol, we assume that users are always identified by their SUCI in the air interface, so the privacy of their identity is protected.

4.4.3 CQI collection

The network needs information from users about the conditions of their channels to decide which devices to serve through the multicast transmission and which via D2D communications. During this step, each device belonging to the MG sends to gNB its CQI values, concerning both its connection with gNB and the D2D links to its neighbors.

4.4.4 Trustworthiness parameters collection

The proposed trustworthiness model envisages the setting of some parameters concerning the “social state" of network nodes. During this step, cell nodes send to the gNB the information necessary to assess their trustworthiness in absence of direct interactions with the other nodes. Details on the model will be provided later, while, during this step, each device i communicates the following trustworthiness parameters: its relationship factors (i.e., $F_{ij} \quad \forall j$ friend of i in the cell), information to compute its centrality (i.e., R_{ij}), and information on its intelligence (i.e., I_i). The last term mainly refers to the computation capabilities of the device and it is better discussed in Section 4.5.

4.4.5 Multicast and D2D configuration selection

Thanks to the collected information, the gNB can plan: *(i)* the set of registered UEs to serve through the multicast transmission via CMS; *(ii)* the MCS to use for the multicast transmission in the CMS coverage area; *(iii)* the set of registered UEs to serve via D2D communications because of their bad channel conditions; *(iv)* the served UEs which can act as RNs by forwarding data towards the cell-edge users, thus forming the D2D pairs.

Pseudocode shown in Table 4.2 illustrates the sequence of steps executed to select the best multicast and D2D configuration.

Table 4.2: Multicast and D2D configuration selection in SeT-D2D

Data: $U, CQI, CQI^c, CQI^d, SF, F, R, I, threshold$
Result: U^m, P^d, MDC
for all $c \in CQI$ **do**
  for all $u \in U$ **do**
    if $CQI_u^c \leq c$ **then**
      Insert u in U^m
    end if
  end for
  for all $r \in U \setminus U^m$ **do**
    Find $s \in U^m | CQI_{rs}^d \neq 0$
    Compute $st_{rs}(SF, F, R, I)$ ▷ According to Eq. 4.9
    if $st_{rs} \geq threshold$ **then**
      Insert s in PR^r
    else
      s is not a possible transmitter for r
    end if
    for all $p \in PR^r$ **do**
      Find max(CQI_{rp}^d)
      Update P^d
      Insert r in U^d
    end for
  end for
  if $U^m \cup U^d = U$ **then**
    Insert MDC_c in MDC ▷ MDC_c is related to CQI=c
  end if
end for
Find $m \in MDC | THR_m$ is max

Variables that are used are:

- U, the set of registered UEs;
- CQI, the set of all CQIs (i.e., $[1, 15]$);
- CQI^c, the set of cellular CQIs of registered UEs (e.g., CQI_u^c is the cellular CQI for UE u);
- CQI^d, the set of D2D CQIs between nearby UEs in the cell (e.g., CQI_{rs}^d is the D2D CQI between UEs r and s);
- SF, the set of satisfaction factors sf_{ij} related to the D2D pairs that interacted;
- F, the set of F_{ij} related to pairs of UEs for whom there is some kind of social relationship;

- R, the set of R_{ij} of registered UEs;
- I, the set of I_i of registered UEs;
- *threshold*, is established to assess the eligibility of possible D2D pairs;
- U^m, the set of registered UEs to serve in multicast;
- P^d, the set of D2D pairs;
- MDC, the set of eligible multicast and D2D configurations;
- $U \setminus U^m$, the set resulting from the difference between the sets U and U^m;
- st_{rs}, the service trust value between UEs r and s;
- PR^r, the set of possible D2D relays for user r;
- U^d, the set of users that can be served in D2D as a transmitter is found for them;
- THR, representing throughput (e.g., THR_m is the throughput related to configuration m).

The multicast and D2D configuration selection is accomplished through an iterative procedure. First, the gNB sorts the received cellular CQI values from the lowest to the highest. Then, it analyzes every possible CQI value and, for each, determines the subset of UEs which can decode the data transmitted with the correspondent MCS and the subset of UEs which, differently, are in worst channel conditions and must be served through D2D communications (lines 3-8). The selection of the most suitable D2D transmitters is the heart of the proposal. The gNB has stored information about the D2D CQIs of cell nodes; thus, it knows what the potential RNs for each D2D receiver could be. For each of them, it computes the value of *service trust* to have a measure of their trust in the ability in providing services (lines 9-11), as will be detailed in Section 4.5. At this point, it classifies as "not eligible" the devices for which the service trust is not at least equal to an established threshold (lines 12-16). Among the remaining ones, the gNB selects, for each D2D receiver,

the device with the highest D2D CQI towards it, i.e., the most efficient one (lines 17-21). As a consequence, D2D pairs are formed. This procedure is performed for each analyzed CQI value, in order to investigate all possible configurations. The term “configuration" indicates the set of nodes to be served in multicast and those to be served in D2D, which depends on the MCS selected for the CMS transmission. Among all the eligible configurations (i.e., those in which all UEs, belonging to the MG, are able to receive data), the gNB finally selects the one that guarantees the maximization of transmission performance (lines 23-27).

Once the selection of multicast and D2D configuration is accomplished, the operations aimed at securing D2D communications are carried out.

4.4.6 D2D initialization

The D2D receiver (in the following referred as UE_i), which wants to receive data, sends an initialization message to the gNB to communicate its identity (i.e., SUCI) and the key generated for the implementation of the DHKE algorithm. In this message and also in those to follow, the use of message authentication (i.e., HMAC) is envisioned for the integrity and authentication of transmitted data.

4.4.7 D2D pair announcement

After receiving the initialization message, the gNB verifies that the identity of the requesting UE is among those previously registered to the network. In positive case, the gNB communicates to each device of the D2D pair the identity of the other peer. Furthermore, it sends to the relay node, UE_j, the key previously received by UE_i, that it will need for the generation of the encryption key through the DHKE algorithm.

4.4.8 Data transmission

The gNB must sign data, before starting the multicast transmission to cell nodes, in order to attest their origin. The gNB computes the signature by applying a public hash function (H) to the data to be transmitted (D) and by encrypting the resulting

digest with its private key (pk): $\sigma_1 = H_{pk_1}(D)$. After that, it sends data to users with the best channel conditions, using CMS. UE_j, which has received data sent by the gNB, has to forward it to the previously notified D2D receiver; therefore, it carries out all the operations aimed at securing the D2D communication. It selects the key to be sent to the gNB so that UE_i can generate, via the DHKE algorithm, the secret key used to encrypt data. After that, the RN itself generates the secret key and encrypts data. Eventually, UE_j signs encrypted data and sends them to UE_i: $\sigma_j = H_{pk_j}(D')$, where pk_j is the private key of UE_j and D' is the encrypted data.

4.4.9 Data check

After data reception from the RN, UE_i must ensure that data comes from the transmitter previously announced by the gNB. If so, in order to accomplish the DHKE procedure and to obtain the plaintext, it requires to the gNB the key previously selected by UE_j. It is worth mentioning that, in the traditional DHKE algorithm, non-secret keys are exchanged directly between the communicating peers. Instead, in SeT-D2D the key exchange is mediated by the gNB, which represents a trusted third party. This helps in avoiding Man-in-the-Middle attacks that represent the main vulnerability of DHKE.

Data are accepted by UE_i if and only if their origin is verified through the gNB's signature check (if this signature is not valid, then data may have been tampered by UE_j). In any case, UE_i must send to the gNB a report in order to communicate some parameters on the quality of the transmission and, possibly, to report the fabrication of the original data, thus allowing the gNB to identify the attacker. The gNB waits for the report for an established waiting period. If it receives a report which announces a data security breach, then it checks by its own the information reported by UE_i. If the data breach is actually occurred and if the gNB ensures that data were sent by UE_j, then the gNB sets to 0 the *good transmission flag* (gtf_{ij}^l) related to the l transmission from UE_j to UE_i, in order to indicate that the D2D communication has not been successful. The same thing happens if the gNB does not receive any report by the end of the waiting period. On the contrary, if the

report received from UE_i indicates a well completed D2D transmission, the gNB sets to 1 the gtf_{ij}^{l}.

All steps of the proposed protocol are depicted in Fig. 4-2.

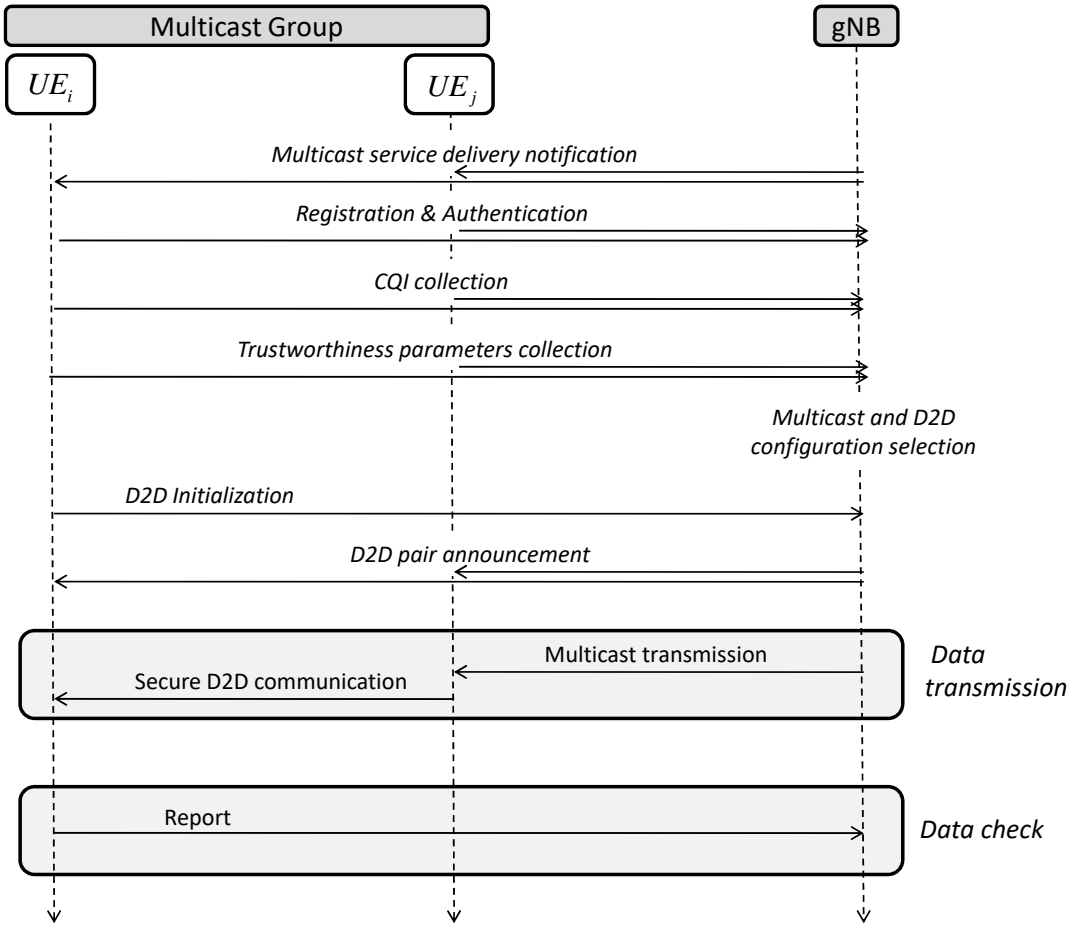


Figure 4-2: The SeT-D2D protocol

4.5 Trustworthiness model

In this Section, the trustworthiness model designed to allow the selection of trustworthy nodes acting as relays in secure D2D communications is described. In the scenario under analysis, the gNB operates as a central controller that is able to assess whether the RN has transmitted data correctly or not (i.e., if it exhibits a malicious behavior or not). The main problem in such a scenario is that, especially in the early stages, there is no information on the trustworthiness of the service provider (i.e., the RN). In fact, a requester node that never interacted directly with a RN is

not able to make a judgment on it. Moreover, before being able to understand the true nature of the RN (if it is a malicious or benevolent node), several interactions will have to take place. In short, the system is affected by the cold start problem, which we cope to by designing a *trustworthiness model* including not only a *direct contribution*, accounting for the direct interactions between nodes, but also an *indirect contribution*, accounting for structural and social properties independent of the transactions (interactions) between the nodes. For this reason, even in the absence of previous transactions, it is already possible to evaluate the maliciousness of the provider and, consequently, to reduce the cold start problem.

In the trustworthiness realm, with the term *functional trust* the ability of a node to provide services [151] is meant. In this Chapter, in adopting the nomenclature used in [142], the functional trust is referred to as *service trust* for a more immediate understanding of the concept that it implies. In turn, service trust can be divided into *direct service trust* and *indirect service trust* [151].

The direct service trust is measured through the opinion of the requester that directly interacted with the provider in the past and, thus, can judge its ability in providing the requested service. The indirect service trust results from the evaluation of the service that the RN has indirectly provided, i.e., through the opinions of the nodes that have already directly interacted with the service provider. Since in the considered scenario the gNB works as a trusted third party, the indirect service trust (and, more specifically, the service reputation) results from the real behaviour of the provider j in all the past transactions in which j has provided a service. In a general trustworthiness model, also the concept of referral trust (named recommendation trust in [142]), that is the trust in the ability of a node to provide recommendations, can be included. In the scenario under investigation, referral trust is not analyzed since the centralized nature of the network architecture makes it lose meaning.

In order to model the service trust, some factors must be introduced that are described by using concepts of graph theory. With i and j two nodes of the graph are represented and with l the interaction (transaction) that occurs between them.

The first step is to find a way to evaluate the interaction between the specific pair of nodes i, j. Generally, in the literature, there are three parameters necessary

to achieve this goal. The first factor is sf_{ij}^{l} that represents the *satisfaction* of i's l^{th} interaction with j. This contribution allows a node i to provide an evaluation of the service it has received by the provider j [142, 143, 144, 148, 149]. Since in the analysed case the gNB is a central entity able to assess whether the RN has transmitted data correctly or not, the following property can be considered as valid:

$$sf_{ij}^{l} = gtf_{ij}^{l} \tag{4.1}$$

where gtf_{ij}^{l} is the good transmission flag for the specific interaction l between node i and node j. It is worth mentioning that gtf_{ij}^{l} assumes a value of 1 if the interaction between i and j is successful, 0 otherwise.

Generally, the satisfaction sf_{ij}^{l} can also keep into account other factors in addition to the contribution of security, such as throughput TP_{ij}^{l} and delay D_{ij}^{l}. In such a case, the expression of sf_{ij}^{l} is the following:

$$sf_{ij}^{l} = \chi gtf_{ij}^{l} + \psi TP_{ij}^{l} + \sigma D_{ij}^{l} \tag{4.2}$$

Equation (4.1) is considered for computing the satisfaction of the interaction to specifically focus on security. In fact, by assigning the good transmission flag calculated by the gNB as the satisfaction value, we have a correct and objective evaluation of the occurred data transmission.

The second parameter needed to evaluate the transaction between the specific pair of nodes i and j is $s\omega_{ij}^{l}$, that represents the *importance* (or relevance) of i's l^{th} interaction with j. It is used to discriminate important transactions from irrelevant ones [142, 143, 144, 148, 149]

The last term to consider for evaluating the interaction is $s\delta_{ij}^{l}$, that represents the *decaying factor* of i's l^{th} interaction with j [142, 143] that is expressed as:

$$s\delta_{ij}^{l} = \begin{cases} \mu\frac{l}{sh_{ij}} + \nu\frac{1}{ln(|t-t^{I}|)}, & \text{if } ln(|t-t^{I}|) > 1 \\ \mu\frac{l}{sh_{ij}} + \nu, & \text{otherwise} \end{cases} \tag{4.3}$$

Looking at Equation (4.3), sh_{ij} indicates the size of i's service (interaction) history with j, that is the total number of interactions occurred between i and j

[142], while l represents the number of the current interaction between i and j, t is the actual time, and t^I is the occurrence time (generation time) of the current interaction. Also the existence condition of the logarithm is imposed, that is $|t - t^I| > 0$. Variable μ and ν represent the weights of the two contributes and must be set on the basis of the scenario under investigation. In particular, the first contribution of the decaying factor takes into account the number of interactions occurred after the one under analysis (current validity of the interaction), while the second contribution accounts for the time elapsed from the considered interaction (recency of the interaction). The first term is derived from [142], while the second from [143]. In particular, the first contribute is important in scenarios in which many interactions occur in a short time interval. In fact, even if an interaction took place recently, since other interactions occurred later, it may be not consistent with the current situation. The second contribution has been added because it can allow to account also for cases where not many interactions occur. In these scenarios, the interaction considered may be the last occurred between that specific pair of nodes, but the same can be no longer trustworthy if it happened a long time ago. By merging these two contributions, as explained above, a decaying factor that can more accurately consider both the decay phenomena is expected.

The competence belief and the integrity belief constitute the direct contribution of the service trust and are expressed as a function of the parameters introduced so far. The *service competence belief* measures how well an acquaintance satisfied the needs of past interactions [142].

$$scb_{ij} = \frac{\sum_{l=1}^{sh_{ij}} (sf_{ij}^l s\omega_{ij}^l s\delta_{ij}^l)}{\sum_{l=1}^{sh_{ij}} (s\omega_{ij}^l s\delta_{ij}^l)} \tag{4.4}$$

This term is fundamental because it stores the past history of the transactions occurred between each pair of nodes.

The *service integrity belief* is the level of confidence in the predictability of future interactions [142].

$$sib_{ij} = \sqrt{\frac{1}{sh_{ij}} \sum_{1}^{sh_{ij}} (SO_{ij}^{rec} - SO_{ij}^{lon})^2} \tag{4.5}$$

Small values of integrity translate into a more predictable behavior of j in future interactions. The idea is to consider not only the degree to which a node has satisfied past interactions, but also the deviation in the degree of satisfaction of the recent interactions with respect to the remote ones. The concept of predicting the degree of satisfaction of future interactions is found in the literature in Bayesian Systems and Belief Theory models (including Subjective Logic [151]). These models use the Probability Density Function (PDF) and the expected values of PDFs. A less complex way to try to calculate predictability of future interactions is by using the standard deviation [142]. The novelty introduced in this model is to use the standard deviation for calculating the predictability of future interactions and to consider the service opinion long as the mean value. The advantage is that this method is simple and allows greater control. Furthermore, it does not resort to complex formulas (like Bayesian Theory and Belief Theory), which also include other parameters such as uncertainty.

The two terms used to calculate service integrity belief are *service opinion long* and *service opinion recent* as in [148, 149]. They can be expressed as:

$$SO_{ij}^{lon} = \frac{\sum_{l=1}^{L^{lon}} (sf_{ij}^{l} s\omega_{ij}^{l} s\delta_{ij}^{l})}{\sum_{l=1}^{L^{lon}} (s\omega_{ij}^{l} s\delta_{ij}^{l})} \tag{4.6}$$

$$SO_{ij}^{rec} = \frac{\sum_{l=1}^{L^{rec}} (sf_{ij}^{l} s\omega_{ij}^{l} s\delta_{ij}^{l})}{\sum_{l=1}^{L^{rec}} (s\omega_{ij}^{l} s\delta_{ij}^{l})} \tag{4.7}$$

They represent the long-term and the short-term service opinion of i about j and are based on the satisfaction of i with respect to the services provided by j. L^{lon} represents the long-term opinion temporal window and L^{rec} the short-term opinion, with $L^{lon} > L^{rec}$ and l indexes from the latest to the oldest transaction.

So far the parameters that underlie the calculation of the direct contribution of service trust have been described.

The first term included in the indirect contribution of the service trust is F_{ij}, that is the *relationship factor* indicating the type of relation that connects i with j [148, 149]. It represents a unique characteristic of the SIoT. The types of existing social relationships are described in [152]: the Owner Object Relationship (OOR) is

established between two objects that belong to the same owner and rarely include a malicious node; the Co-Location Object Relationship (C-LOR) connects domestic objects; the Co-Working Object Relationship (C-WOR)) links objects belonging to the same workplace; the Social Object Relationship (SOR) is established between objects that meet occasionally; the Parental Object Relationship (POR) is created between objects of the same model. The process of establishment of these relationships precedes the interactions, as it is mainly based on the number and duration of previous contacts occurring between the devices. The SWIM simulator [153] has been used with the aim of generating traces of people's mobility. It has been properly modified to obtain traces of the mobility of devices owned by people. A trustworthiness value has been associated with each social relationship as shown in Table 4.3, according to [148].

Table 4.3: Possible numerical values of social trustworthiness relationships

Relationship	**Description**	**Trust**
OOR	Objects owned by the same person	0.9
C-LOR	Objects sharing experiences	0.8
C-WOR	Objects sharing public experiences	0.8
SOR	Objects in contact for owner's relations	0.6
POR	Objects with production relations	0.5
No relationship		0.1

The second term of the indirect contribution is also of a social nature and is $R_{ij} = \frac{|K_{ij}|}{|N_i|}$, that is the *centrality* of j in the life of i, where $|K_{ij}|$ represents the *common friends* between i and j, and $|N_i|$ is the *neighborhood* of node i [148, 149]. This term is very important because if a node has many relationships, it is expected to assume a central role in the network in terms of leadership, efficiency in problem solving, and personal satisfaction of participants. Furthermore, if two nodes have many friends in common, it is likely that they have similar evaluation parameters about building relationships.

The third parameter of the indirect contribution of the service trust is I_j, that is the *intelligence* of j, representing its computational capabilities [148, 149]. It is a static characteristic of the objects since it does not vary over the time, but depends only on the type of the object considered. A smart object is expected to

have more capabilities to cheat with respect to a "dummy" object, thus leading to riskier transactions.

As stated in Section 4.4, UE_i will send to the gNB the F_{ij} and R_{ij} values related to each of its neighbors. Furthermore, it sends its own I_i value.

The last term constituting the indirect contribution of the service trust is the service reputation sr_j. Generally, a node can get information about the ability in providing service of j by asking the opinion to other nodes that have already received a service from j. In particular, in distributed scenarios, service reputation can be calculated by considering only the subjective opinion of a specific subset of nodes to which j has already provided a service. Often, this subset is the neighborhood of the requester node i since there is no trusted third party. In the considered scenario, the gNB works as a central controller and computes the service reputation by considering the real behaviour of the provider j as:

$$sr_j = \frac{1}{n_j} \sum_{g=1}^{|N_j|} (sf_{gj}) \tag{4.8}$$

where $|N_j|$ is the set of nodes that have already interacted with j and n_j is the total number of transactions in which j has supplied a service.

Finally, the service trust between nodes i and j (st_{ij}) can be computed with the following formula:

$$\begin{aligned} st_{ij} = &\left(\frac{log(sh_{ij}+1)}{1+log(sh_{ij}+1)} \right) (\beta_1 scb_{ij} - \beta_2 sib_{ij}) + \\ &+ \left(\frac{1}{1+log(sh_{ij}+1)} \right) (\gamma sr_j + \epsilon F_{ij} + \zeta R_{ij} + \theta(1-I_j)) \end{aligned} \tag{4.9}$$

characterized by this structure:

$\alpha * DirectExperience + \beta * IndirectExperience$

where α grows and β decreases with the number of interactions. Values of α and β are taken from the literature [148].

Thanks to this structure, as the number of interactions increases, an increasing weight can be assigned to the direct experience contribution. A similar structure is used in [142, 143, 145, 146, 148, 149]. In the direct contribution, the first term

(service competence belief) corresponds to the direct functional trust; while, the first term of the indirect contribution (service reputation) corresponds to the indirect functional trust [151]. To ensure that st_{ij} assumes values between 0 and 1, the sum of the constants of both the direct and indirect contributions are equal to 1.

In the described model, the threshold is not considered to definitively exclude the nodes that did not behave trustworthy, for several reasons. First of all, in any case the model will tend to naturally assign low values of service trust to malicious nodes, thus excluding them (not definitively) even without using a threshold. A second reason is that, unlike threshold-based models, the presented model is able to recover the benevolent nodes which behaved badly for a few interactions (for example, because they have been temporarily infected by viruses). Obviously, the recovery process is not immediate and depends on the past history of the node. To conclude, Table 4.4 shows the weights of the parameters used to carry out the simulations. These values are relayed by existing works [142, 148, 149].

Table 4.4: Values of the weights of parameters used to test the trustworthiness model of SeT-D2D

Weight	**Parameter**	**Value**
β_1	Competence	1
β_2	Integrity	0.5
γ	Reputation	0.5
ϵ	Relationship Factor	0.175
ζ	Centrality	0.175
θ	Intelligence	0.15

4.6 Performance evaluation

The performance of the proposed protocol have been tested via the MATLAB tool.

The considered scenario consists of 100 devices uniformly distributed in a 100 m x 100 m cell. Inside the multicast group, including all terminals, a portion of devices is served according to a CMS approach, while those in worst channel conditions receive data via D2D connections. A NR frame with transmission numerology $\mu = 0$ is considered in the simulations, that is a frame with 15 KHz subcarrier spacing

composed by 10 slots, each lasting 1 ms. A bandwidth of 20 MHz with 100 RBs is available. The NR frame used in the simulations consists of six slots in format 0, three slots in format 1, and one slot in format 2, organized as in a TDD LTE frame type 2 configuration 3. The Inband D2D mode is chosen, therefore uplink slots are reserved to D2D communications. In downlink slots, the multicast transmission takes place.

The following metrics are used to assess the performance of the proposed protocol:

- *Percentage of wasted capacity* on the D2D link caused by the selection of untrustworthy transmitters.
- *Mean number of non-corrupted received kbits*, which indicates the amount of data correctly downloaded in D2D, as transmitted by non-malicious relays.
- *Percentage of malicious relay selection*, computed as the percentage of frames, over all simulation time, in which at least one malicious relay has been selected.

Below, before discussing the performance offered by the proposed protocol, it is demonstrated how some features introduced in the trustworthiness model can help overcome the drawbacks highlighted in Section 4.3. Then, the performance enhancement that the proposed SeT-D2D protocol can provide will be illustrated with respect to: *(i)* exploiting only information derived from past interactions, thus regarding security (Se-D2D), and *(ii)* a security- and trust-unaware algorithm (D2D). Note that the Se-D2D comparison protocol corresponds to those defined in [119], while the D2D protocol represents a legacy D2D communication. The work of SeT-D2D proposed approach is analysed under two different kinds of attack model. In case of *on-off attacks* (inspired by [154]), malicious nodes exhibit their malevolent nature only during on periods. Differently, *receiver-selective attacks* reflect the case of a node that behaves maliciously only toward specific receivers.

As stated in Section 4.5, only nodes with an *st* value higher than a predetermined threshold are considered as possible relay nodes. Figure 4-3 shows the results of an experimental analysis carried out with the aim to define the most appropriate value

of such a threshold. Since, under all analyzed percentages of malicious nodes (ranging from 15% to 60%), the mean number of non-corrupted received kbits reaches the highest value around the threshold value of 0.3, in all simulations results that will be shown in the following, the threshold is set to this value. As expected, Figure 4-3 also allows to appreciate that higher amount of non-corrupted data is delivered to receiver nodes under lower percentage of malicious nodes.

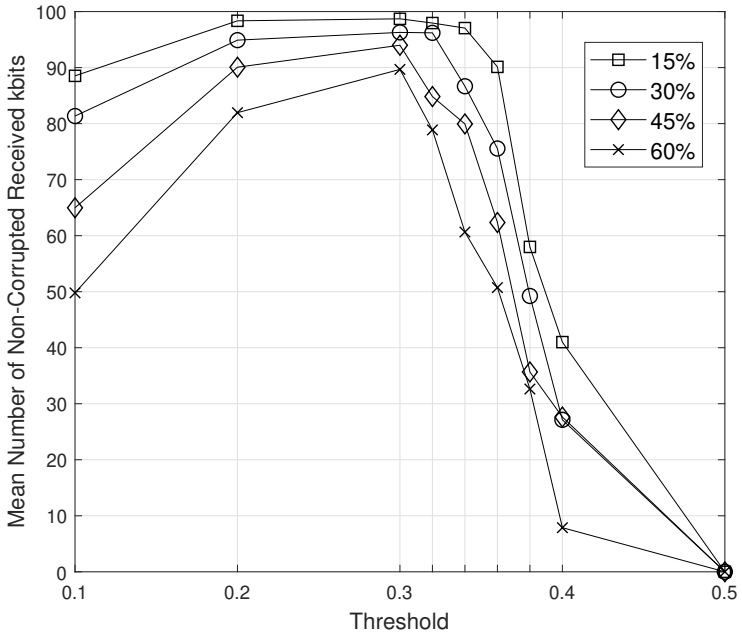


Figure 4-3: Mean number of non-corrupted received kbits under varying maliciousness threshold for SeT-D2D

4.6.1 Proof of concept of the trustworthiness model

First, the calculation of the service integrity belief sib_{ij} measured by node i by referring to the service received by provider j (see Equation 4.5) is considered. Similarly to [142], an approach based on the standard deviation has been followed since it is simpler than the Bayesian and Belief models and allows greater control. In Figure 4-4, the proposed approach in case service integrity belief is calculated according to Equation 4.5 is compared with the case in which it is computed with the SORT integrity formula proposed in [142]. The ideal case in which node j always provides an excellent service (i.e., sf is always equal to 1 and corresponds to the

Ground truth) is analysed. In such a condition, since the deviation in the degree of satisfaction of recent interactions with respect to the remote ones is null, node i expects that j exhibits the same behavior shown in the past. By looking at Figure 4-4, it can be noticed that, by using SORT, the service integrity belief tends to be overestimated, while the service trust is underestimated. Differently, the adoption of the presented model allows to obtain the expected service integrity belief (the curve is always equal to 0) and a service trust very close to the Ground truth. Similar conclusions can be drawn also in non-ideal scenarios (i.e., when node j does not always provide satisfactory services).

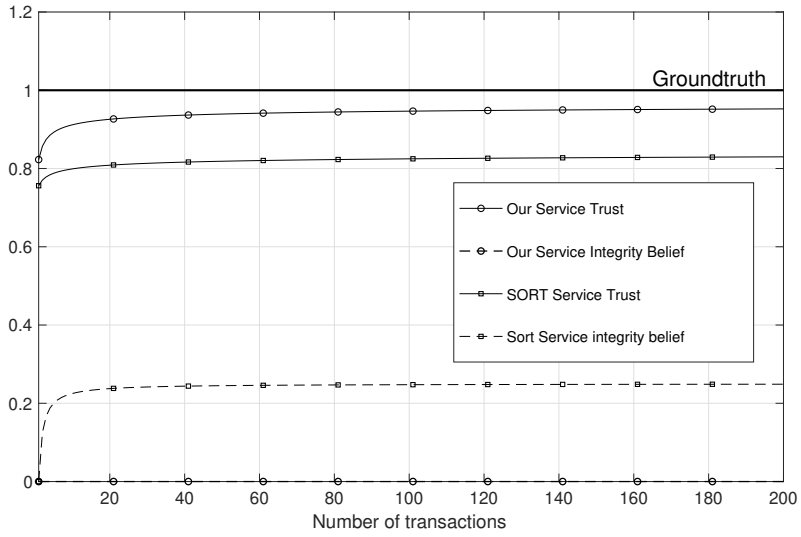
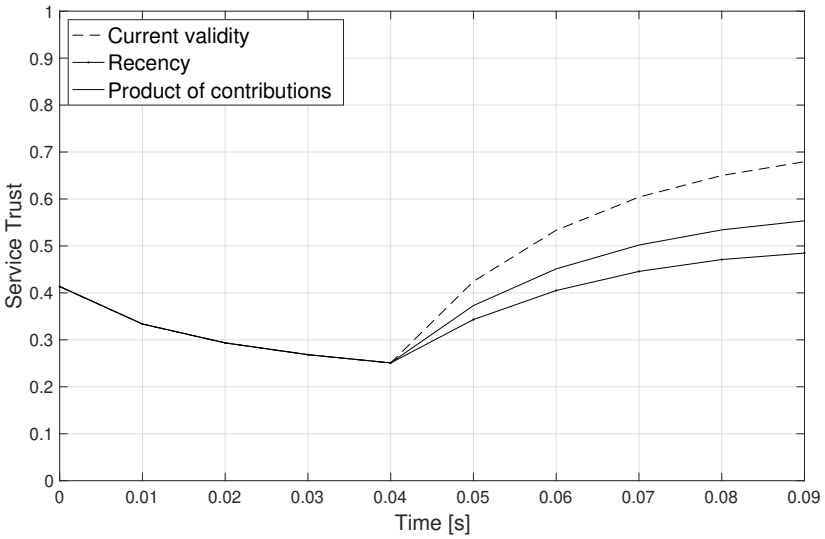


Figure 4-4: Performance comparison obtained by the model presented in SeT-D2D with different service integrity belief formulas, in a scenario with sf (service satisfaction) always equal to 1

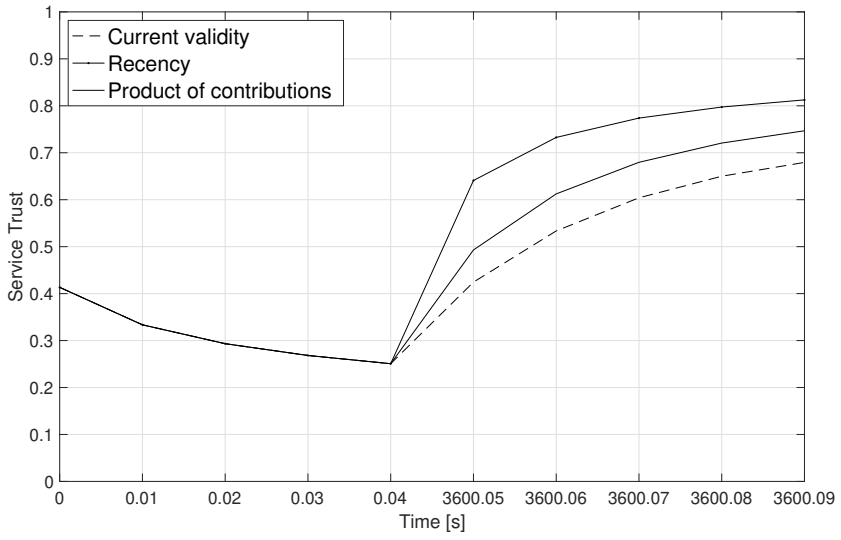
By focusing on the decaying factor $s\delta_{ij}^{l}$ of the $l-th$ transaction between node i and provider j (see Equation 4.3), in the literature, some models (such as [142]) consider only the *cardinal contribution* that keeps into account the number of transactions occurred after the considered one (current validity of the interaction), while other research works (such as [143]) focus only on the *temporal contribution* related to the time elapsed from the $l-th$ transaction (recency of the interaction). With the aim to provide a good approximation of the decaying factor, the presented model considers both contributions. Two scenarios are analysed in which ten transactions take place either in a short time interval (Fig. 4-5(a)) or in a long time interval

(Fig. 4-5(b)), respectively. In the "short time interval" scenario, a transaction takes place every 0.01 s. Differently, in the "long time interval" scenario there is a pause of 3600 s between the fifth and the sixth transaction. In both cases, only the last five transactions are assumed to have $sf = 1$ (i.e., node i evaluates as satisfactory the service received by j in the last five transactions). Figure 4-5(a) shows that, when considering only the *cardinal contribution* ($\mu = 1$, $\nu = 0$), the weight of last five transactions increases compared to the case in which only the *temporal contribution* is taken into account ($\mu = 0$, $\nu = 1$). The curve lying in the middle represents the case in which both contributions are considered and weights μ and ν are set, as an example, to 0.5. Differently, by looking at Figure 4-5(b), it can be inferred that the *temporal contribution* alone ($\mu = 0$, $\nu = 1$) makes the last five transactions more relevant. The straightforward reason for this behaviour is that, in scenarios wherein the considered transaction is recent in time, although followed by several further interactions (i.e. the situation represented by the "short time interval" scenario), models that keep into account only the *temporal contribution* could reduce the decay factor since they evaluate only the recency of the interaction. However, the likely high number of interactions occurred after the considered one might have led to changes that the temporal contribution alone is unable to catch. Indeed, in this case, accounting also for the *cardinal contribution* would make the presented model more effective. Differently, in scenarios in which the considered interaction is not recent, although it is among the last ones occurred (i.e. the situation represented by the "long time interval" scenario), a higher weight given to the *temporal contribution* could increase the effectiveness of the model. To conclude, both the decay contributions should be accounted for and, in doing so, the proposed solution becomes flexible enough to allow getting all intermediate performance levels that lie in between the two limit cases represented above. This is achieved by properly setting the weights μ and ν in the calculation of the decay factor.

As a final remark, it is worth stressing that the proposed trust model is explicitly designed for SIoT scenarios. Thanks to the presence of the intelligence, centrality, and relationship factor parameters, it allows the calculation of an indirect contribution even in the total absence of transactions (i.e., in the absence of



(a)



(b)

Figure 4-5: (a) Short time interval scenario, and (b) Long time interval scenario for SeT-D2D

service reputation), which makes it possible to mitigate the cold start problem. This will emerge in Figures 4-6, 4-7, from the comparison between Se-D2D and SeT-D2D. Besides, it gives weights to parameters so as to allow a greater adaptability to the considered scenarios. This last advantage emerges in Figure 4-11.

4.6.2 Proof of concept of the SeT-D2D protocol

Fig. 4-6 shows the benefits that the proposed SeT-D2D can bring with respect to Se-D2D and D2D in terms of mean number of non-corrupted received kbits (Figure 4-6(a)), percentage of wasted capacity (Figure 4-6(b)), and percentage of malicious relay selection (Figure 4-6(c)) for an increasing percentage of malicious nodes. Plots show that utilizing information deriving from security is of primary importance and that a further considerable performance enhancement can be achieved when social trustworthiness is also kept into account. In fact, SeT-D2D protocol is able to deliver the highest amount of non-corrupted kbits, thus leading to the lowest percentage of wasted capacity, thanks to the infrequent selection of malicious relay nodes.

To further prove the effectiveness of the proposed SeT-D2D protocol, Figures 4-7 show an analysis under increasing file dimension, representative of the performance that SeT-D2D could assure in different use cases, ranging from alert messaging to file downloading. Results testify that, for all considered file dimensions, SeT-D2D exhibits the best performance in terms of both mean number of non-corrupted received kbits (Fig. 4-7(a)) and percentage of wasted capacity (Fig. 4-7(b)). This last metric is insensitive to file dimension while the former shows an increasing trend.

4.6.3 Analysis of on-off attacks

A malicious D2D transmitter could follow different attack models. In the following analysis, the response of the trustworthiness model presented in this Chapter is shown under three different *attack rates* (i.e., 30%, 50%, and 80%), indicating the percentage of simulations over the total number of executed runs in which the relay acts maliciously against all its receivers. These are referred as *on-off attacks*. Attack simulations can be consecutive or have an irregular pattern.

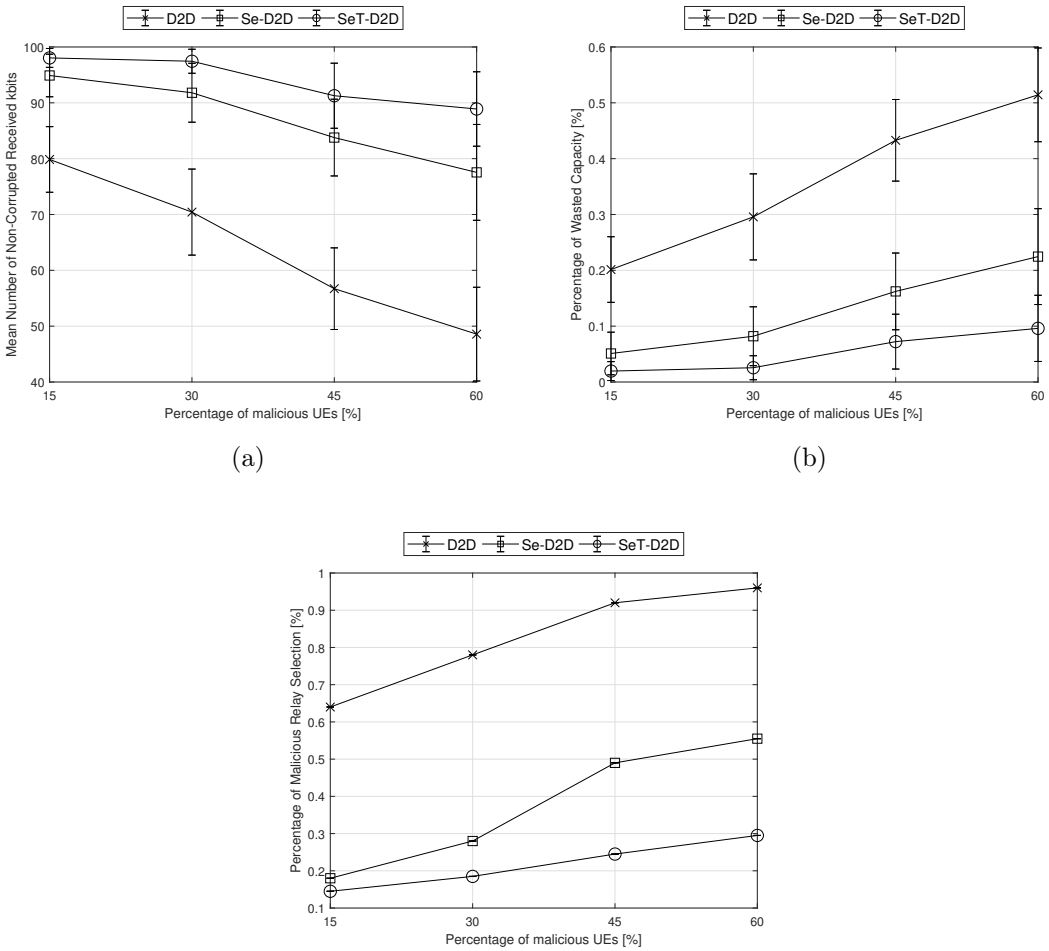
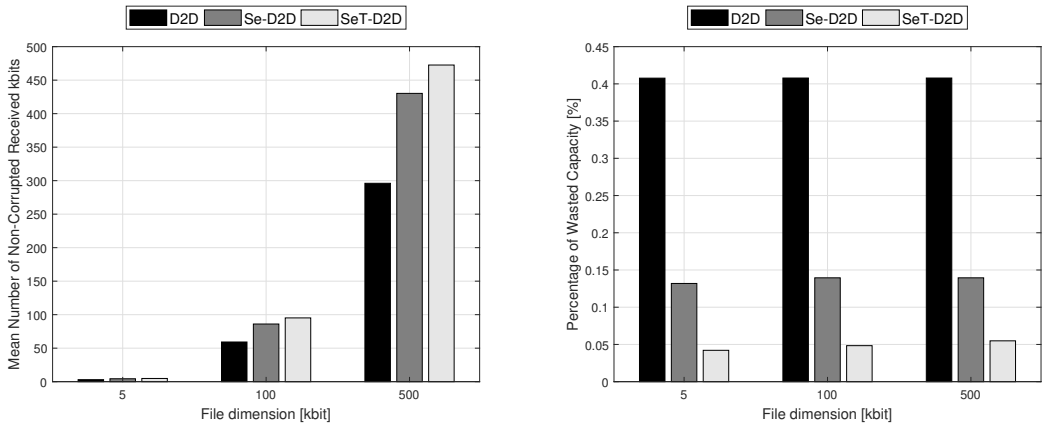


Figure 4-6: (a) Mean number of non-corrupted received kbits, (b) percentage of wasted capacity, and (c) percentage of malicious relay selection under varying percentage of malicious users per cell (for the evaluation of SeT-D2D protocol)



(a) (b)

Figure 4-7: (a) Mean number of non-corrupted received kbits, and (b) percentage of wasted capacity under increasing file dimension (for the evaluation of SeT-D2D protocol)

In case of *consecutive* attacks, the node could exhibit its malicious behavior after a period of time in which it hides its real nature by avoiding to carry out any attacks. Vice versa, it could behave maliciously initially, then moving to a good behavior. Figures 4-8 show how st_{ij} evolves over time for the D2D pair ij that interacted during all simulations. The relay node behaves correctly when the attack model profile is equal to 1. Contrarily, it performs a malicious behaviour when the profile is equal to 0. Two complementary attack models are analyzed. In the first one, the malicious transmitter initially performs a good behavior and then attacks all its receivers for a number of simulations related to each attack rate (Figures 4-8(a), 4-8(b), and 4-8(c)). The opposite attack profile is considered in Figures 4-8(d), 4-8(e), and 4-8(f)). All graphs show a trend in the value of the service trust that is consistent with the evolution of the attack model, as the value of st_{ij} grows as long as the relay transmits data correctly, and begins to decrease when it exhibits its malicious nature. This proves that the proposed trustworthiness model produces a service trust value that reflects the nature of the node, thus representing an effective estimate of node's trustworthiness.

Figure 4-9 shows the trend of st_{ij} under an *irregular* attack model characterized by a discontinuous behavior of the malicious relay due to frequent transition from correct to corrupted D2D transmission. Also this Figure demonstrates that the

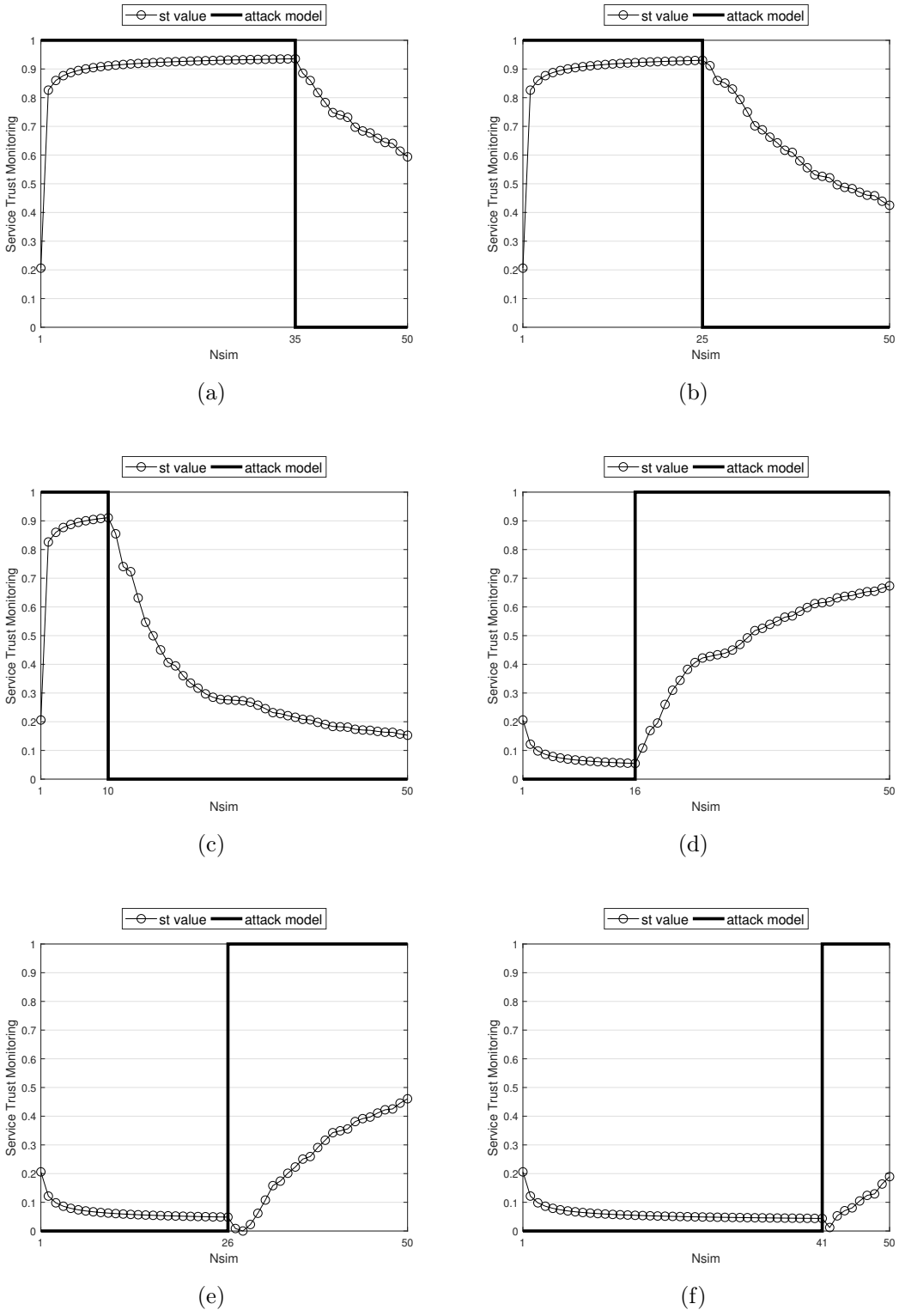


Figure 4-8: Service trust monitoring in SeT-D2D in case of on-off attack model with a final attacker activity equal to (a) 30%, (b) 50%, and (c) 80%; vice versa, with an initial attacker activity equal to (d) 30%, (e) 50%, and (f) 80%

proposed trustworthiness model is able to produce a service trust value that is coherent with the attack model profile.

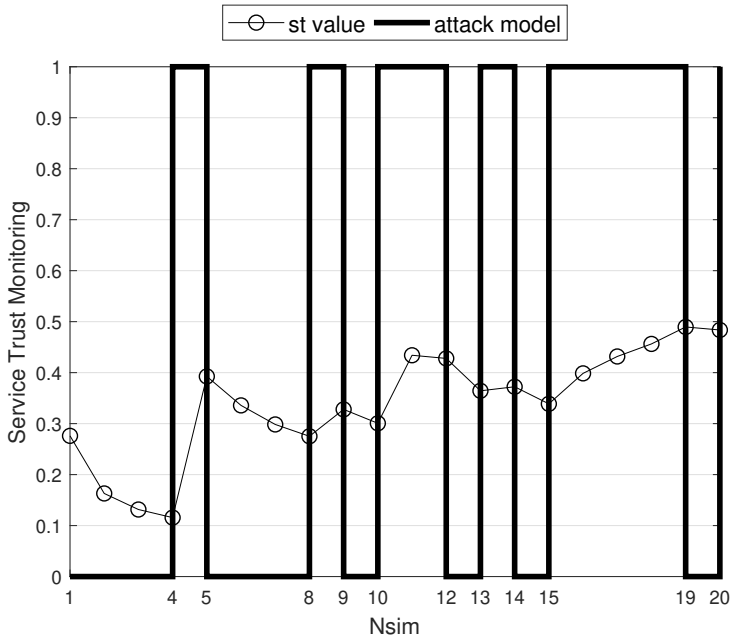


Figure 4-9: Service trust monitoring in SeT-D2D in case of irregular attack model

Figure 4-10 is a further proof that the trustworthiness model reacts well to both types of attack model (consecutive and irregular) since, by varying the attack rate, the amount of non-corrupted data delivered to the D2D receiver is similar in both cases.

A further test of the trustworthiness model responsiveness to on-off attacks is done by simulating a *periodic* attack model in which the malicious relay alternates a good and a bad behavior at regular intervals. Figure 4-11 depicts how st_{ij} evolves when different β_2 values are used to weigh the integrity of the D2D interacting couple. As discussed in Section 4.5, when evaluating the direct experience in the interaction between receiver i and malicious relay j, a proper decrease in the value of st_{ij} is guaranteed by an appropriate proportion between competence (i.e., scb_{ij}) and integrity (i.e., sib_{ij}) values of the D2D pair (Equation (4.9)). The higher the value of β_2, the greater the decrease in st_{ij}. This may not be an advantage when a node manifests a single malicious behavior, not necessarily intentional, as its trust value falls considerably, making its recovery very slow. This analysis proves that

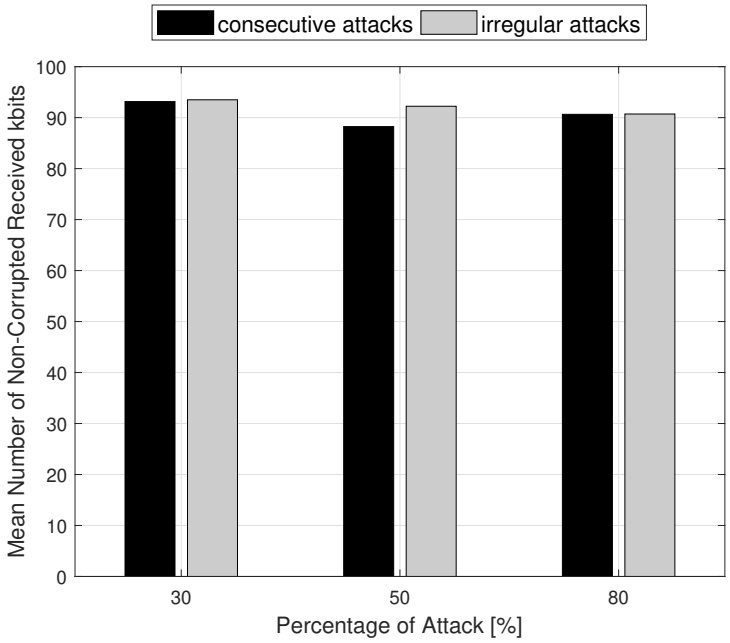


Figure 4-10: Mean number of non-corrupted received kbits under varying attack rate in SeT-D2D

the choice of the β_2 weight is very important and must be made based on the type of application and the severity to be attributed to incorrect behaviors. In all other simulations, β_2 is set to 0.5.

4.6.4 Analysis of receiver-selective attacks

Unlike on-off attacks, with *receiver-selective attacks*, a malicious relay exhibits its bad nature at any time but not with all data recipients. Purpose of this analysis is to observe the effect of these attacks on the reputation of the malicious node and, consequently, on the evaluation of its service trust.

The curves in Figures 4-12 represent the service trust value referred to the interacting pairs in all executed simulations. Figure 4-12(a) shows the trend of st_{ij} for the pair ij, where j is the malicious relay and i is its only victim receiver among the three receivers that it serves. Differently, in Figure 4-12(b), st_{wj} is computed between the malicious relay j and the non-victim receiver w.

By looking at Figures 4-12, st_{ij} has a trend which depends on the behavior that the relay exhibits with the peer. In fact, the gNB calculates for non-victim

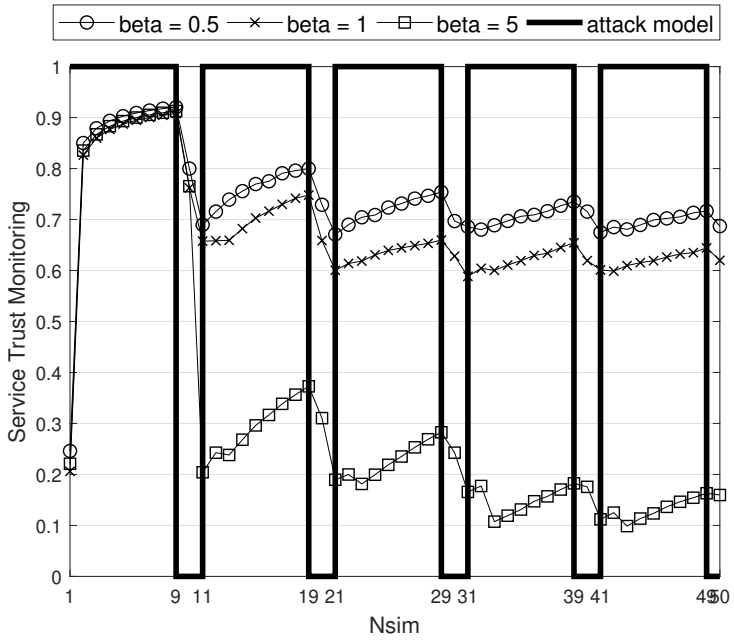
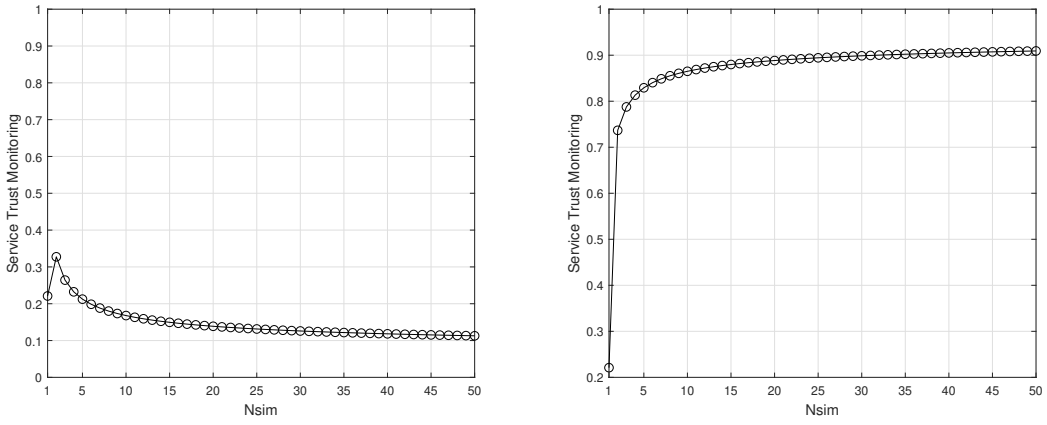


Figure 4-11: Service trust monitoring in SeT-D2D in case of periodic attack model under varying β_2 values



(a) (b)

Figure 4-12: Service trust monitoring in SeT-D2D between malicious relay and: (a) victim node, (b) non-victim node

node (see Figure 4-12(b)) a service trust value that is substantially higher than the one computed for the victim node (see Figure 4-12(a)), due to the different direct contribution values. This proves that the higher the information available regarding security, the lower the influence of reputation on service trust and that the SeT-D2D mechanism is able to quickly provide a differentiated estimation of the real malicious/non-malicious nature of the relay to victim and non-victim nodes, respectively.

4.6.5 Security analysis

This Section is aimed at highlighting the security assurances that the SeT-D2D protocol offers. Similar security analysis are also conducted in [119, 155, 156].

Thanks to the implementation of a symmetric encryption algorithm and a secure key agreement between the peers, *confidentiality and integrity* of data transmitted in D2D communications are ensured. Thus, data remain confidential (i.e., not understandable by unauthorized parties) and integral (i.e., not modifiable by those who do not have the key).

As previously explained, a secret key is generated by both the D2D transmitter and receiver through the DHKE protocol and is used for the encryption/decryption of data sent over D2D links. The DHKE algorithm allows *resistance to attacks by eavesdroppers*, since it ensures that the generated secret key is not intercepted by malicious users.

By employing the gNB as a trusted third party in the interactions between the D2D peers, the SeT-D2D protocol also ensures *resistance to Man-in-the-Middle attacks*, which represent the DHKE's main vulnerability.

The *authentication* of the nodes belonging to the multicast group is managed, in the SeT-D2D protocol, by using the procedures described by 3GPP in [134]. Furthermore, the application of the HMAC to the messages sent by the D2D peers to the gNB and vice versa guarantees the authentication and the integrity of the transmitted messages. HMAC envisages the implementation of a hash function to a particular combination of the message to be transmitted and the private key known only by the sender and recipient. In so doing, any modification to the transmitted

message would be easily detectable by the receiver, for which the verification process of the message authentication would fail.

Moreover, the SeT-D2D protocol requires that the *signature* is implemented by the message senders (i.e., gNB and relay nodes) in order to certify the origin of the data and guarantee the *non-repudiation* of the transmitted messages.

Finally, the assurance of the *privacy protection* of the users is obtained by transmitting their SUCI instead of the SUPI for their identification on the air interface.

4.7 Conclusions of Chapter

In this Chapter, the SeT-D2D protocol has been defined in order to foster a trusted multicast service delivery in 5G-oriented networks through an improved version of the CMS aided by secure D2D communications. The selection of trustworthy and efficient D2D transmitters is the heart of the proposal, since both channel conditions of D2D links and trust parameters affect the procedure carried out to choose the best relay node for each D2D receiver. Furthermore, data sent via D2D communications are protected thanks to the implementation of an encryption algorithm, for which the keys are generated through a trusted use of the DHKE protocol.

In order to evaluate the performance of the proposed SeT-D2D protocol, a simulation campaign has been conducted by using the MATLAB tool. The comparison with other protocols, which either do not use social trustworthiness to evaluate the trust of the nodes (i.e., Se-D2D) or do not take into consideration at all trustworthiness (i.e., D2D), shows that SeT-D2D allows a better management of network resources, ensuring more efficient data delivery. In fact, SeT-D2D effectively guarantees a proper selection of trustworthy D2D transmitters, thanks to the use of a trustworthiness model consistent with the actual nature of the network nodes.

Chapter 5

The value of security for 5G MTC traffic

To date, group-oriented communications have been mainly exploited for delivering multimedia services in human-oriented communications while, in 5G cellular networks, objects are the main target. IoT plays a key role in 5G networks, wherein mMTC feature a use case as crucial as challenging since cellular IoT connections are predicted to grow heavily in the next future. To boost capacity and energy efficiency, the 5G network can leverage D2D communications which are recognized as an effective offloading technique. This is achieved thanks to the fact that, in legacy D2D communications, data are directly sent from one device to another, avoiding the crossing of the network. Obviously, the distributed nature of such a communication paradigm and the inherent broadcast nature of the wireless channel make it necessary to think how to secure the so called “sidelink" transmissions. This Chapter proposes a protocol for the efficient and reliable management of multicast services in a 5G-oriented IoT scenario, in which security is a crucial requirement to be met. The proposed protocol is tailored to Narrowband IoT (NB-IoT) and makes use of D2D communications with the aim of improving network efficiency and optimizing network resource utilization. In addition, cyber security and social trustworthiness mechanisms are exploited to secure D2D communications.

5.1 Introduction to Chapter

5G cellular systems are hyper-connected networks mostly consisting of pervasive smart objects. If human communications have been the reference target in previous generations of mobile networks, they will be hugely overtaken by communications among objects in next-generation cellular networks. The 3GPP has specified a 5G system architecture aimed to support a wide set of use cases, typically grouped into three classes: eMBB, URLLC, and mMTC [57]. Focus of this Chapter are mMTC communications, given such soaring demands for smart objects connectivity.

The number of cellular connections among objects belonging to the diversified world of the IoT is expected to reach 4 billions by 2024 [157]. In fact, "smart-things networks" are going to be exploited in the more disparate fields spanning from healthcare to agriculture, intelligent transportation system, education, industry, gaming, and so on. It follows that IoT networks will be composed of even-more-intelligent heterogeneous objects which, being typically resource-constrained, have the common feature of requiring a low energy consumption. This is why 3GPP standardized the NB-IoT technology, optimized to guarantee longer battery life to resource-constrained cellular devices.

In the road towards 5G systems, the increase in the number of connected objects is complemented by the growth in demands for group-oriented communications. In fact, although several IoT applications primarily involve the Uplink (UL) direction, there are also many use cases, such as massive media distribution and software update, that require the same data to be sent from the network to groups of IoT devices, i.e., in the Downlink (DL) direction. To date, group-oriented communications have been mainly exploited for delivering multimedia services in human-oriented communications, while, in 5G networks, objects are the main target. Although typical traffic flows involving objects are related to sensing and automation activities, multimedia applications have a great potential in the IoT ecosystem. This is testified by the increasing interest towards the Internet of Multimedia Things, an innovative concept according to which heterogeneous multimedia things can interact and cooperate to achieve multimedia-based applications/services [158]. In fact, as

also stated in [159], the target of multimedia services is shifting from traditional TV to streaming on connected devices, such as mobile devices and monitoring devices. The feasibility of delivering less-demanding multimedia IoT applications over NB-IoT has been investigated in [160].

Actually, multicast transmissions could allow to largely weigh down latency and energy consumption of the receiving IoT devices. The traditional way of serving multicast traffic is the CMS, which assigns the group data rate based on the device that experiences the worst channel conditions. As stated in [161], guaranteeing all multicast receivers a similar performance experience is as necessary as challenging, since the instantaneous channel condition of each device in the multicast group varies independently. Despite using CMS all devices receive the same treatment, the transmission is heavily constrained by the cell-edge users. As a consequence, CMS fails to offer a high QoE, which is the quality focus of 5G networks [162]. This is the reason why it is necessary to design effective methods for delivering multicast services over 5G networks.

The Single Cell Point to Multipoint (SC-PTM) architecture and procedures have been standardized to deliver multicast traffic within a NB-IoT cell. Although NB-IoT and SC-PTM are the current standards for IoT, still several features need to be applied to further optimize the performance of IoT data delivery. In this regard, Machine-type Multicast Service (MtMS) is proposed in [163] to define the proper architecture and transmission procedures to manage the MTC multicast traffic. Although this architecture is well-suited to IoT traffic, it does not take into account any security problems, even though their undoubted importance in the 5G ecosystem.

Among the enabling technologies of 5G networks, D2D communications stand out for the advantages they can bring in terms of latency, data rate, spectral and energy efficiency, thanks to the proximity between the communicating devices [121]. As in [164], D2D communications are often established as an underlay to cellular networks with the aim to meet the increasing demand for mobile data services, achieve high data rates, and reduce the traffic load on the base station. On the other hand, a clear weakness in 5G-oriented D2D communications is undoubtedly the vulnerability to security attacks, during data exchanges. Security is one the

main requirements of the 5G mobile networks, mainly due to the fact that many actors are involved in the provision of services, therefore, sensitive data are exposed to different parties, some of which may not be trusted. Moreover, softwarization is a key technique in the development of the 5G, hence, technologies such as MEC, NFV, and SDN are considered enabling for the future generation networks. Despite the undoubted benefits brought by these technologies, they cause the network to be exposed to many new security threats, which must be managed efficiently. Many works in the literature deal with the vulnerabilities of 5G virtualization technologies and potential solutions [38] [165] [24].

In IoT scenarios, where devices are often called upon to transmit sensitive data through insecure wireless channels, this flaw pushes to look for highly effective mechanisms for both data confidentiality and integrity guarantee, user authentication and authorization, and device protection. This problem has been tackled in [166], where a protocol intended to secure D2D communications is defined in which D2D peers generate a private encryption key by using a trusted version of the DHKE protocol. The public keys exchange is then mediated by the base station that acts as a trusted third party. The main drawback of the presented protocol is that there is no way to disclose the bad nature of the nodes before they exhibit their malicious behavior. Furthermore, the proposed protocol is not properly tailored to the IoT domain, in which the presence of resource-constrained devices poses specific challenges.

In this vein, this Chapter proposes the *MtMS with secure and trust D2D (MtMS-stD2D)* protocol, specifically designed for the highly reliable delivery of multicast traffic to a set of machines in IoT scenarios. It leverages D2D communications over sidelinks, coupled to a secure mechanism based on the DHKE protocol. It is worth mentioning that sidelink is defined in [167] *as the interface between UEs for sidelink communications, which also include the D2Ds, thus it is the link over which the communication between devices in proximity occurs.*

The main contributions of this Chapter are the following:

- the architecture presented in [163] is enhanced by the inclusion of secure sidelinks, aimed at improving the performance of the multicast transmission, while ensuring protection of data transmitted in D2D;

- the security protocol described in [166] is strengthened by the possibility to estimate the reliability of nodes also before they perform a malicious behavior, thanks to information on the social relationships established among nodes in the network;

- an analysis of the protocol feasibility in terms of energy consumed to implement the proposed solution on resource-constrained nodes of a NB-IoT network, such as those that populate IoT scenarios, is carried out in order to determine which kind of use case could take advantage from the MtMS-stD2D architecture.

The remainder of the Chapter is organized as follows. In Section 5.2, the research background is presented. Section 5.3 illustrates the scenario under investigation, while Section 5.4 describes in details all MtMS-stD2D procedures. Obtained results are shown in Section 5.5, while conclusive remarks are given in the last Section.

5.2 Background

This Section starts with the description of the basics of NB-IoT, the cellular technology which is the reference of the proposal of this Chapter. Then, the management of multicast transmissions in NB-IoT will be discussed. Afterwards, research works related to security will be surveyed.

5.2.1 The NB-IoT technology

NB-IoT is a cellular technology, first defined in 3GPP Release 13, designed to meet the requirements of low-cost IoT devices located in weak-coverage signal areas. Energy saving, coverage extension, and capacity increase are among its main benefits. It can extend device battery lifetime by up to 10 years, improve coverage by 20 dBm compared to LTE, and manage the massive capacity of IoT scenarios [168].

NB-IoT is not the only solution in licensed spectrum proposed for IoT applications, as two other alternative technologies actually exist: LTE for Machines (LTE-M), also introduced in 3GPP Release 13, and Extended Coverage Global System

for Mobile Communications (EC-GSM), created from the GSM standard. NB-IoT stands out for the reduced amount of required resources. In fact, only 180 kHz of bandwidth can be used for both downlink and uplink. This choice makes NB-IoT compatible with other technologies. It can be implemented in a 200 kHz GSM carrier or, within an LTE carrier, using a 180 kHz Physical Resource Block (PRB).

NB-IoT can be deployed by choosing among three different operation modes: *(i)* in *standalone* mode, it is implemented as a dedicated carrier, using one of GSM; *(ii)* in *in-band* mode, it is deployed inside an LTE carrier, occupying one or more PRBs; *(iii)* in *guard band* mode, it can use the frequencies of the LTE carrier guard bands. As regards the in-band and guard-band modes, resources must be properly assigned to NB-IoT not to create interference with legacy LTE signals. Therefore, although NB-IoT is an independent RAN technology, it is compatible with the previous ones, because it offers a good flexibility in the implementation.

The physical layer of NB-IoT is characterized by innovative features, required for the management of the narrow bandwidth. In Release 13, the Frequency Division Duplexing (FDD) mode is required. Thus, in NB-IoT, uplink and downlink are frequency divided. In addition, half-duplex mode is supported by devices that, therefore, can not simultaneously receive and transmit. In the downlink, NB-IoT supports OFDMA with 15 kHz subcarrier spacing. A frame is composed of ten subframes, each lasting 1 ms, and each subframe is composed of two 0.5 ms slots. Therefore, the downlink transmission scheme is the same as that of LTE. In the uplink direction, the SC-FDMA is used and both single-tone and multi-tone transmissions are feasible. For the single-tone transmission, it is possible to choose between a 3.75 kHz or 15 kHz subcarrier spacing. If the 3.75 kHz option is selected, slot will last 2 ms. Multi-tone transmission modes are the same as those of the LTE uplink: 15 kHz subcarrier spacing with 0.5 ms time slot [169].

5.2.2 Multicast support in NB-IoT

SC-PTM has been standardized by 3GPP to manage multicast transmissions in NB-IoT networks. It extends the MBMS standard, from which it inherits many features, including procedures.

The main nodes of the MBMS architecture are: the *BM-SC*, which is the source of the multicast content and is responsible for the initialization of the MBMS session and for some security functions, such as the management of the authorizations for the MBMS subscribers; the *MBMS-GW*, which is in charge of forwarding MBMS packets to the Base Station (BS) involved in service delivery; the *MCE*, which has to manage admission control and radio resource allocation to the BS [124].

MBMS service is subscription-based and it foresees the implementation of the following procedures: *subscription*, *service announcement*, *joining*, *MBMS notification*, *session start*, *data transfer*, *session stop*, and *leaving*. Devices subscribe to the network their interest in receiving MBMS services and the network periodically announces them the available services. A device, interested in receiving a certain service, joins the multicast group to which the service will be offered, through the joining procedure. Subscribed devices must constantly monitor the Multicast Control Channel (MCCH) for service information and listen for future service announcements. Despite the many advantages that MBMS can bring to cellular networks [170], this latter aspect is one of the most critical for IoT networks, since it can affect the Discontinuous Reception (DRX) cycle of the IoT devices and, therefore, cause a relevant energy wastage. For these reasons, SC-PTM procedures have to be modified in order to properly meet the requirements of the NB-IoT resource-constrained devices [171].

5.2.3 Securing communications

In [57], among the listed 5G requirements, improved security mechanisms, that can work effectively in the presence of a likely huge amount of data transmitted over cellular networks, are recommended. In the IoT landscape, devices often communicate sensitive data over the insecure wireless channel, thus, security and privacy requirements have to be satisfied to guarantee both data and device protection [172]. Many works in the literature deal with the security problem in the 5G mobile networks, the most significant of which are collected in [50]. Among the different covered topics, the authors highlight the most effective solutions proposed in the literature to overcome some challenging security issues. Solutions are grouped in access con-

trol, authentication, communication, and encryption areas, the same targeted by the protocol proposed in this Chapter.

In the 5G network, D2D communications are a widely accepted technology for enhancing spectrum efficiency, improving network resource utilization, and extending battery lifetime [121]. However, as also stated in [118], the establishment of secure D2D communications is a critical point, because of the additional problems caused by the fact that data are exchanged directly between devices in proximity. A malicious transmitter may decide to drop the data packets directed to the D2D receiver or may modify them, without the network or recipient being aware of the misbehaviour.

Among proposals for securing D2D communication, an interesting solution is presented in [119]. This is the work that inspires the protocol presented in [166], which satisfies many security requirements, such as non-repudiation, authentication, authorization, confidentiality, and integrity. It uses some security mechanisms, such as encryption, HMAC, and signature to manage the messages exchanged between the two peers involved in direct communication. To this aim, the encryption of transmitted data is performed through a symmetric (i.e., private-key) encryption algorithm. The private key is generated through an enhanced version of the DHKE protocol. The enhancement consists in charging a trusted third party (i.e., the BS) to manage the public keys necessary for the generation of the secret key. In detail, the DHKE algorithm states that each of the two peers, involved in the generation of the secret key, produces a preliminary public key to be sent to the other, so that it can calculate the same private key. According to DHKE, the peer i can compute the secret key K_{ij} as follows:

$$K_{ij} = Y_j^{Xi} \bmod q = (\alpha^{X_j})^{X_i} \bmod q = \alpha^{X_i X_j} \bmod q \tag{5.1}$$

where, $Y_j = \alpha^{X_j} \bmod q$ is the public key of peer j, α is a fixed primitive element of $GF(q)$ and q is a prime number (both known to the two involved peers), X_i and X_j are independent random numbers respectively chosen and kept secret by peer i and peer j. Similarly, peer j computes the same secret key thanks to the knowledge of Y_i, that is the public key of peer i:

$$K_{ij} = Y_i^{X_j} \bmod q = (\alpha^{X_i})^{X_j} \bmod q = \alpha^{X_i X_j} \bmod q \tag{5.2}$$

In legacy DHKE, the peers directly exchange their public keys. Differently, in the proposed enhanced version, each peer sends its public key to the BS, which will forward it to the other peer, following a request coming from it and only after having verified its identity and legitimacy to request for that information. The literature on the subject confirms that these design choices are well suited to IoT scenarios, like the one examined in this Chapter. In fact, many research works assume the intervention of a trusted third party in the key generation mechanism between resource-constrained devices [173] or of a centralized security framework to detect incoming attacks [174]. In [175], the authors propose GT-QoSec, a game-theoretic joint optimization of QoS and security in Heterogeneous Networks (HetNet) that can also serve a large number of devices requesting various types of applications. In this scenario, the eNB implements intrusion detection techniques to monitor threat levels of the network and plays a key role in ensuring adequate security ranks to each device. Regarding the choice of symmetric encryption, many works in the literature confirm that this is the best choice for resource-constrained devices. Works [176] and [177] proposed symmetric encryption algorithms, that are less demanding in terms of energy consumption compared to an asymmetric approach.

So far, the advantages of the algorithm presented in [166] have been illustrated in order to legitimize whether this algorithm is partly used also in the protocol presented in this Chapter. In fact, similarly to [166], the presented protocol exploits an enhanced version of the DHKE protocol, where the BS acts as a trusted third party in order to avoid the Man-in-the-Middle attack, a well-known vulnerability of DHKE. In this proposal, the BS contributes to the establishment of secure D2D communications and to the detection of any malicious behaviour of devices that may have been intentionally deployed for breaching network security. Since both DHKE and D2D communications are distributed by nature, the BS (already in charge of delivering data from/to devices) also exploits, at a global level, any security information gathered by devices in local data exchanges. In order to enhance the protocol presented in [166], it was necessary to think about how to reduce the number

of undetected malicious devices selectable as D2D transmitters (or relay nodes). So, in addition to [166], the prtocol presented in this Chapter foresees that the BS implements a careful selection of the D2D transmitters by considering, not only the malicious behavior of the nodes that have already played the role of relays, but also taking into account the "social" reputation of the devices within the network.

5.3 System model

This Chapter considers an IoT scenario, wherein the MTC multicast traffic is managed through the proposed algorithm, named *MtMS-stD2D*. D2D communications are established between devices directly served by the BS and the terminals excluded from the multicast transmission, because of their adverse channel conditions. A secure protocol is implemented over sidelinks in order to protect the transmitted data. The protocol aims to avoid giving a forwarding role to devices that exhibited a malicious behavior in the past. Since a node cannot be considered as "not secure" (i.e., unreliable) until it behaves maliciously, the protocol also estimates the reliability of network nodes by leveraging a simple, yet effective, trust model available from the literature and based on the SIoT paradigm [152]. Social relationships that can be established among nodes are: POR, among objects created by the same producer in the same period; C-LOR, that affects smart things that always work in the same place; C-WOR, between objects that collaborate to achieve a common goal; OOR, that binds objects owned by the same holder; SOR, due to the meeting, sporadic or continuous, of the owners of the objects, that consequently get in touch. Examples of applicative use-cases that could benefit from the presented protocol are massive media distribution, software update of a group of machines owned by a customer/Tenant, or delivery of alerting messages.

A common trend in cellular technology is to deploy femtocells which are small, inexpensive, and low-power base stations that represent a cost-effective means of data traffic offloading from the macrocell. Femtocells are generally consumer-deployed and connected to their own wired backhaul connection. It is expected that 70% of wide-area IoT devices will use cellular technology in 2022 [178]. Thus, it appears

clear that femtocells will play a significant role in the next-to-come scenario, and will drive the fast realization of the IoT, because of their ability to provide high data rate services in a less expensive manner [179]. For this reason, a femtocell is considered for the formulation of the MtMS-stD2D protocol, in which an *Home-evolved NodeB (HeNB)* provides connectivity to a small-cell of devices, thus guaranteeing latency and energy consumption reductions and improving coverage and reliability compared to the traditional macrocell. In particular, NB-IoT is exploited for radio links between the HeNB and devices, whereas proximity-based transmissions (i.e., D2D) are established among devices in mutual proximity. The idea to investigate is to offload the portion of traffic that cannot be handled by NB-IoT via short-range sidelinks. The motivation behind this choice is that, by utilizing a low-power technology, energy consumption of the devices can be reduced, even if the lack of support of D2D communication in NB-IoT must be obviated. Thus, it is assumed that the relay nodes are equipped with two radios: a NB-IoT interface, connecting the relay node to the HeNB, and an LTE-A radio, for the direct communication with cell-edge users. This assumption is realistic since IoT devices are currently equipped with a wide range of radio technologies, that include both long- and short-range connectivity, such as Long Range (LoRa), LTE, NB-IoT, Bluetooth, and LTE Cat-M1. This requirement can be seen as a further "hardware constraint" in the relay node selection process.

The MtMS-stD2D architecture, depicted in Fig. 5-1, derives from the MtMS architecture (defined in [163]) and properly enhances it to support secure D2D communications. It is composed of the following nodes: *HeNB*, which provides connectivity to a small-cell of devices; *HeNB gateway (HeNB-GW)*, which aggregates control and data traffic of various HeNBs; *MtMS serving center (MtMS-SC)*, implemented at the Service Capability Server (SCS), it is responsible for initializing the MtMS session, obtaining the multicast content and the information about the receiving devices; *MtMS coordination entity (MtMS-CE)*, which manages the joining procedure by paging the indicated devices; *MtMS gateway (MtMS-GW))*, which receives data from the MtMS-SC and forwards them to the cells with paged devices. MtMS-GW and MtMS-CE are implemented at the HeNB-GW.

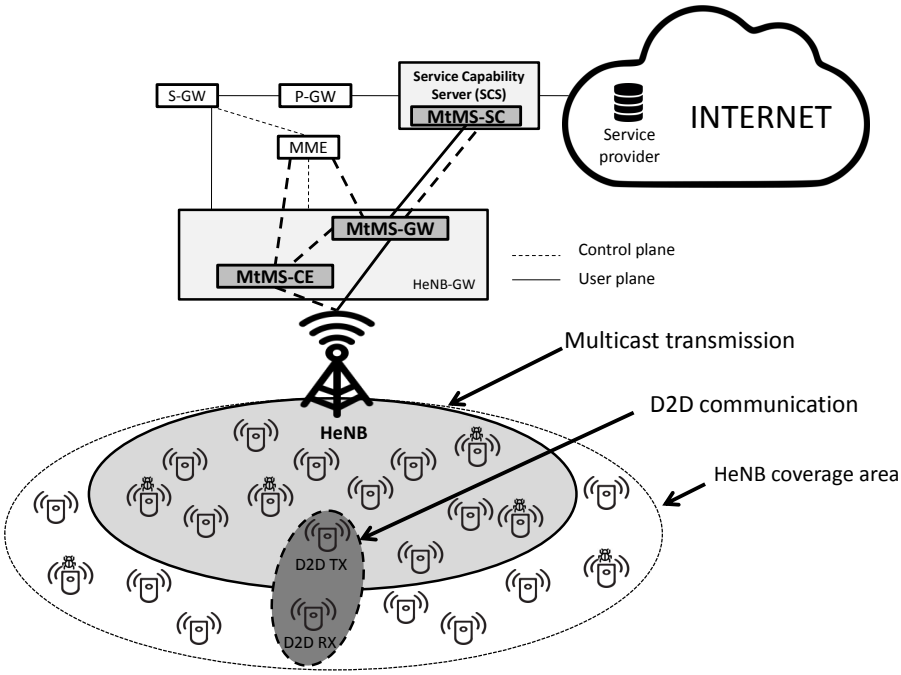


Figure 5-1: Reference architecture of MtMS-stD2D protocol

Despite the proposed MtMS-stD2D architecture strictly relies on the presence of the HeNB, it does not pose severe scalability problems. First of all, the number of devices under coverage of the HeNB is limited, since femtocells are considered. In addition, not all devices in the cell must implement the security protocol; in fact, only D2D communications, which involve a limited portion of devices over the total number of nodes in the femtocell, are designed to be secured.

In view of the goal of serving resource- and energy-constrained IoT devices, the overhead introduced by the proposed security mechanism, which is then evaluated through an energy consumption analysis, needs a keen attention.

5.4 MtMS-stD2D

In the reference IoT environment, resource-constrained devices have to receive multicast data from the network. In many IoT scenarios, the UL direction is the most analyzed, since IoT devices are assumed to have the task of sending data to the network (sensing). Actually, use cases such as massive media distribution, software update, and delivery of alerting messages are equally important and frequent in

IoT. For this reason, this Chapter focuses on procedures for *efficient* and *secure* DL service delivery.

The procedures and sub-procedures of the MtMS-stD2D protocol are described below and summarized in Table 5.1.

Table 5.1: Procedures and sub-procedures of MtMS-stD2D protocol

Procedures	Sub-procedures
A) Subscription	
B) Initialization	
C) Joining	1) Paging 2) Random access 3) D2D pairs selection 4) Service request 5) D2D pair announcement
D) Data transfer	1) Multicast transmission 2) stD2D communication 3) Report 4) Public key exchange 5) Alarm beacon or null
E) Session stop	

5.4.1 Subscription

The subscription procedure is performed by the service provider. For example, in the case of massive media distribution, it is realistic to assume that the owner of devices communicates to the network which devices must receive the multimedia data. This allows energy saving, since it prevents devices from interrupting their DRX cycle to monitor service announcements.

5.4.2 Initialization

MtMS-SC is responsible for the initialization of the MtMS session. It receives data from the service provider and forwards them to the MtMS-GW.

5.4.3 Joining

Paging

The joining procedure starts with paging, aimed at waking up the subscriber devices before data transmission. The MtMS-stD2D protocol includes an enhanced DRX-based group paging, which consists in the creation of subgroups of devices to be paged on the basis of their DRX cycle, at different times. The HeNB is in charge of performing paging to wake up target subgroups of devices, when necessary, since it is assumed that the network is already informed on which devices should receive the multicast data. This assumption is realistic in IoT scenarios, since one of the main applications of group-oriented communications are massive media distribution and software update. In these cases, the service provider (e.g., the owner of the devices) can communicate to the network which devices must receive the service. The enhanced DRX-based group paging allows to: *(i)* minimize the number of multicast transmissions required to deliver data to all devices in the cell, and *(ii)* prevent the waste of energy caused by the interruption of the DRX cycle for service announcements monitoring.

Random Access

Whenever a subgroup is paged, the awakened devices must perform the random access procedure to synchronize with the network. On this occasion, each device also sends information about: *(i)* the conditions of the direct channel towards the HeNB (i.e., CQI), *(ii)* the CQIs of the sidelinks which connect it to the nearby nodes in the network (i.e., D2D CQIs), and *(iii)* the values of social relationships with other network nodes to allow HeNB estimating nodes' reliability.

D2D pairs selection

This phase represents the heart of the proposal of this Chapter, since it involves the use of social trustworthiness and security metrics in the selection of D2D transmitters. Based on their CQI, the network determines which devices to serve directly and which to serve in D2D. In selecting the best D2D transmitters for the given receivers, the network, particularly the MtMS-CE, considers both the reliability of the possible relays and the D2D CQIs. In [114], the authors demonstrate the convenience of considering the conditions of the D2D channel in the selection process of the best transmitter for a given receiver. First, the MtMS-CE computes the reliability value for each possible relay as:

$$NRV_k^t = \begin{cases} SRF_k^t, & MDC_k^{t-1} = 0 \\ MDC_k^{t-1}, & MDC_k^{t-1} \neq 0 \end{cases} \tag{5.3}$$

where:

- NRV_k^t is the Node's Reliability Value referred to node k at time instant t.
- SRF_k^t is the Social Relationships Factor for node k at time instant t. It derives from the social relationships between node k and the other nodes of the network. In fact, as in [180], a value $\in [0, 1]$ is assigned to each type of the five social relationships discussed in Section 5.3. The kind of social relationship established between network nodes affects their reputation as long as a node exhibits a malicious behaviour when working as a D2D transmitter. For this reason, the SRF value has a great impact on the protocol performance especially in the early stages, when very few D2D communications have been set up.
- MDC_k^{t-1} is the Malicious D2D-transmissions Counter of node k before the current time instant. More details on this counter will be given below. Briefly, it may be a value $\in [0, \infty)$, representing a measure of non-reliability of the node, since it tracks the number of times the node, selected as a D2D transmitter, behaved maliciously.

The MtMS-CE bans as non-eligible for the role of relays all nodes for which $NRV > 1$, because they evidently behaved maliciously at least in one D2D transmission. Afterwards, it splits eligible devices in three priority classes based on their NRVs: high, medium, and low. The MtMS-CE checks the D2D CQIs between the possible relays, belonging to the high class (i.e., the most reliable), and the D2D receivers. If there is a relay for each receiver, the selection ends. Otherwise, MtMS-CE considers the medium priority class. Only if no relay is found among the nodes with medium reliability values, then MtMS-CE considers the low priority class. In case MtMS-CE cannot find a transmitter for each recipient, D2D communications are not established and all network nodes are served via CMS.

Service request

In order to guarantee confidentiality and integrity of data transmitted over sidelinks, a secret key is generated by each transmitter and receiver by performing the DHKE protocol, as in [119]. The exchange, between the peers, of the public keys, required for the generation of the same secret key, is always mediated by a trusted third party, that is the HeNB. The D2D receiver, DEV_i, sends a service request message to the HeNB to communicate its identity and the public key generated for the implementation of the DHKE algorithm. In this and in the following messages exchanged between a device and the HeNB, the use of message authentication (i.e., HMAC) is envisioned for the integrity and authentication of each message.

D2D pair announcement

After receiving the service request message, the HeNB authenticates the requesting device in the normal cellular communication mode, checking if its ID is registered. In the positive case, the HeNB has to perform the D2D pair announcement, informing both the D2D receiver (i.e., DEV_i) and the D2D transmitter (i.e., DEV_j) of their imminent communication. Thus, it sends to each peer the identity of the other. Furthermore, it sends to DEV_j the public key received by DEV_i during the service request step.

5.4.4 Data transfer

Multicast transmission

As previously mentioned, during the initialization procedure, the service provider sends multicast data to the MtMS-SC, which forwards them to the MtMS-GW. The latter signs data before sending them to the HeNB. This way, it will always be possible to recognize the original data from the service provider. When data arrive at the HeNB, it performs the multicast transmission to the first paged subgroup by using CMS.

Secure-D2D (sD2D) communication

When DEV_j, which belongs to the served subgroup, receives data from the HeNB, it already knows it has to forward them to the previously notified D2D receiver; so, it carries out all the operations necessary to guarantee a secure D2D communication. In order to ensure confidentiality and integrity to data packets sent over sidelink, it encrypts them with a symmetric encryption algorithm using the secret key generated through the DHKE algorithm. In addition, it reports in the message its identity (i.e., ID_j) and signs it before sending it to the D2D receiver. This guarantees non-repudiation.

Report

As mentioned, the HeNB acts as a trusted third party in the public keys exchange, required by the DHKE algorithm for the two peers to generate the same secret key. To this aim, the relay node sends the HeNB the public key used in the previous step to derive the encryption key.

Public key exchange

After receiving data, DEV_i first verifies the identity of the transmitter. To this aim, it compares the identity reported in the message received over sidelink by DEV_j (i.e., ID_j) with that communicated by the HeNB. If they do not match, the packet is dropped; otherwise, it proceeds with next steps. Afterwards, it checks the signature

of the transmitter and, if it is valid, data are considered good because sent by the entity corresponding to ID_j. Once the identity of the sender is verified, DEV_i needs to generate the decryption key to obtain the plaintext. Thus, it sends a public key request message to HeNB.

Alarm beacon

Thanks to the reception of the public key, DEV_i can get the private key and obtain the plaintext data. To verify the origin of data, it also checks the signature of the MtMS-GW and, if it is valid, data are accepted, otherwise, it is possible that data have been tampered. In this case, DEV_i must send to the HeNB an alarm beacon as the evidence of the fake message and to track the malicious attacker. The HeNB waits for the beacon for a ΔT time after sending the public key to DEV_i, if any alarm beacon arrives during this time interval, then the HeNB first checks the validity of the signature of the MtMS-GW. If the signature is invalid, it assumes that the message did not come from the service provider and may be fabricated by the transmitter. So, HeNB also verifies the validity of the signature of the relay node to ensure that the fake message comes from the entity corresponding to ID_j. One counter is stored by the HeNB to track any malicious behavior of D2D relay nodes: the MDC. In case of a malicious transmission by DEV_j, HeNB increments its MDC by one. This counter contributes to define the node's reliability, as explained in Section 5.4.3.

5.4.5 Session stop

The MtMS session is completed when data are sent to all devices initially subscribed.

5.5 Performance evaluation

5.5.1 Security analysis

The features of a D2D communication make it willing to various security threats. 3GPP has released TS 33.303 in which it describes the security procedures that can

be implemented in Proximity-based Services (ProSe), in particular for the public safety use case [181]. The protocol presented in this Chapter aims at optimizing the encryption key generation procedures also making them eavesdroppers proof. Hence, first, the security requirements for reliable D2D communications are listed and, then, which of these requirements are met by the MtMS-stD2D protocol will be highlighted.

- *Data confidentiality and integrity.* Confidentiality prevents data from being accessed by unauthorized entities. Data integrity avoids an attacker from tampering data transmitted in a private communication.

- *Authentication.* It is important for identifying the entities that perform actions. It allows the association of identification credentials with the entity that owns them.

- *Privacy.* The protection of information related to network users concerns the privacy assurance. In the age of General Data Protection Regulation (GDPR), this is a fundamental requirement in many contexts, such as eHealth and smart wearables.

- *Non-repudiation.* The non-repudiation of an action is important for the detection of malicious entities. If this requirement is met, a malicious user cannot deny having done a bad deed, so network can possibly punish it.

The main contribution to security offered by the MtMS-stD2D protocol is the *reliability assurance*: thanks to the proposed selection mechanism, it is very likely that a reliable and efficient relay will be selected to forward data through D2D communications over sidelinks. As regards the protection of data packets transmitted in D2D, their *confidentiality* is guaranteed by the implemented symmetric encryption algorithm, while their *integrity* is assured by the use of the HMAC. The construction of the HMAC, in fact, implies that only who knows the used private key (i.e., in the MtMS-stD2D protocol, the owner device and the HeNB) can modify the message; in this way, also the *authentication* of the message is achieved, because only the owner of the private key can have generated it. Furthermore, thanks to the signature im-

plementation, *non-repudiation* is accomplished. This is particularly important in the sD2D communication step (see Section 5.4.4), when the relay has to sign data before transmitting it to the D2D receiver. Once the signature has been checked, if it is successful, the relay can not deny that it was the origin of data transmission and, if it has been malicious, the network is able to take into account its bad deed. Finally, it is worth mentioning that, in the MtMS-stD2D protocol, the exploitation of the BS as a *trusted third party* is an additional security guarantee, since, by centralizing the security control, it is possible to avoid attacks by distributed devices, such as Man-in-the-Middle and byzantine generals problem. The fact that the BS is fundamental for the existence of the network implies that it is also the most secure and protected node, lowering the risk of central entity vulnerabilities.

5.5.2 Simulation results

The performance of the proposed protocol have been tested via the MATLAB tool.

The considered scenario consists of 1000 devices distributed in the edge of a circular NB-IoT cell with a 1000 m radius. Inside the multicast group, including all terminals, a portion of devices is served according to a CMS approach through NB-IoT, while those in worst channel conditions receive data via D2D connections.

According to NB-IoT specifications, a bandwidth of 180 kHz is available for the communication between HeNB and device, and the in-band mode is deployed. As regards D2D communications on LTE-A, a bandwidth of 20 MHz, which corresponds to 100 RBs, is available. A TDD LTE frame type 2 configuration 3 is used. Each slot (or TTI) in the frame lasts 1 ms, so the entire frame has a duration of 10 ms. The Inband D2D mode is chosen, so uplink slots are reserved to D2D communications. In downlink slots, the multicast transmission takes place.

Simulations are conducted by varying the percentage of malicious devices and the dimension of the downloaded file. In particular, file dimension varies from 5 kb to 10 MB in order to analyze the performance of the proposed protocol (shown in the graphs as stD2D) in different use cases, spanning from alert messaging to high dimension file downloading. Security messages dimension is set according to [119]. Finally, for purely simulation purposes, an almost ideal situation has been considered

in which devices send to the HeNB accurate values of trustworthiness, computed as in [148]. In particular, values in the range [0,0.4] and [0,1] are respectively assigned to malicious and non-malicious nodes with the ultimate goal to select the most reliable nodes to work as relays.

The following metrics are used to assess the performance of the proposed protocol:

- *Percentage of wasted capacity* on the sidelink, caused by the selection of unreliable transmitters.
- *Mean number of non-corrupted received kbits*, which indicates the amount of data correctly downloaded in D2D, as transmitted by non-malicious relays.
- *Average wasted energy* by D2D receivers. In the D2D protocol (without security) the waste is caused by the reception of data sent by malicious relays; in the proposed protocol (stD2D) the waste is caused both by sending the data necessary to secure D2D communications and by receiving data sent by malicious relays.
- *Percentage of energy consumed to secure D2D communications*, computed with respect to the total energy required for the operation of D2D relays and receivers in the proposed protocol.
- *Energy consumed to download data*, computed for the stD2D protocol and in the case where data are sent directly by the HeNB to the node, in unicast mode (without D2D and security).

All these metrics are related to security assurance, since they measure at which extent the protocol is able to select reliable relays and limit the waste of device resources.

In Figures 5-2 and 5-3 three possible implementations of the D2D communication are compared: in the *D2D* case, the communication takes place without security; in the *sD2D* case, the reliability of network nodes keeps into account only the respective stored MDCs; in the *stD2D* case, the D2D communication is secure and the node's

reliability is based both on security and social trustworthiness. The dimension of the file to download is set to 500 kb.

Figure 5-2 shows that considering both security and social trustworthiness to evaluate the reliability of devices is the winning strategy, as it guarantees practically no data loss. Figure 5-3 confirms this claim. In fact, it shows that the proposed protocol allows to download practically the whole 500 kb file even with 60% of malicious devices. This happens because almost only non-malicious relays are selected as forwarding nodes towards D2D receivers.

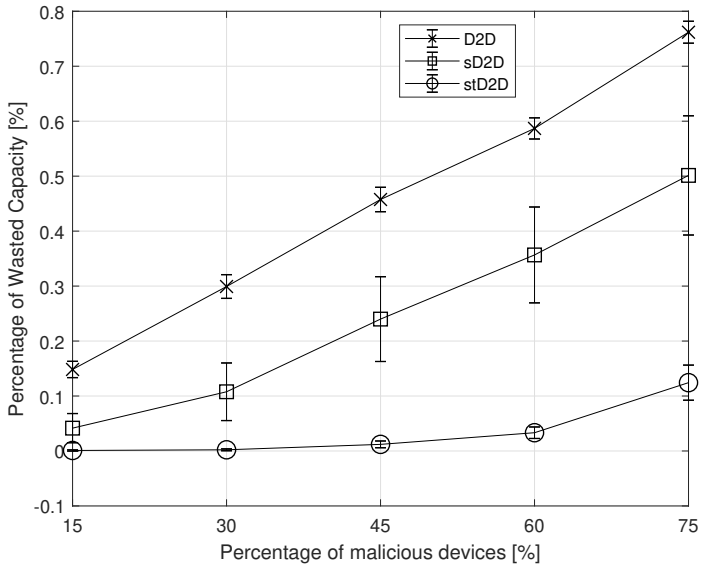


Figure 5-2: % of wasted capacity vs. % of malicious devices (for the evaluation of MtMS-stD2D protocol)

Figure 5-4 depicts the amount of energy wasted, on average, by D2D receivers for operations other than receiving useful data. The power consumption values are set as in [182]. In particular, the energy in the D2D protocol (which does not provide security in direct communication between devices) is wasted by the receiver that has to download useless data, as transmitted by a malicious relay. It is computed as:

$$E_{\text{wasted, D2D}} = \frac{E_{\text{malicious}}}{E_{\text{total}}} \tag{5.4}$$

As regards the stD2D protocol, the energy waste is caused by both the reception of useless data sent by a malicious relay, and the transmission of the data needed to

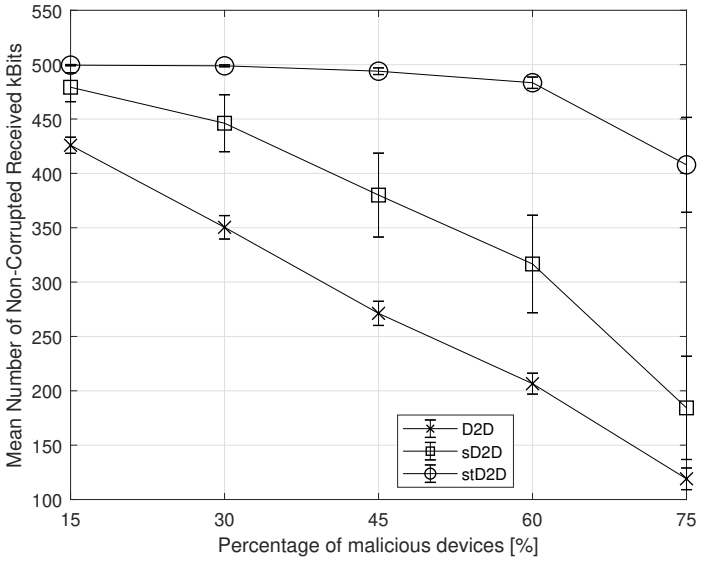


Figure 5-3: Amount of data correctly transmitted in D2D (i.e., by non-malicious relays) vs. % of malicious devices (for the evaluation of MtMS-stD2D protocol)

implement the security mechanism to both HeNB and forwarding node. The energy wasted in this case is calculated as:

$$E_{\text{wasted, stD2D}} = \frac{E_{\text{malicious}} + E_{\text{security}}}{E_{\text{total}}} \tag{5.5}$$

As shown in Figure 5-4, the energy waste for D2D protocol increases with the percentage of malicious devices in the network, as the number of D2D malicious transmitters is higher. Differently, stD2D exhibits a constant trend, indicating that the energy waste is caused mostly by the contribution E_{security}. In fact, unlike $E_{\text{malicious}}$, this does not depend on the percentage of malicious devices.

Figure 5-5 shows the total energy consumed by devices to secure D2D communications in the stD2D protocol. Results show, as expected, that securing D2D communications is a high energy-consuming task. However, it is important to point out that, without any security mechanism, some nodes will likely discharge their battery in the reception of corrupted (thus non-useful) data. This can be inferred by Figure 5-4. D2D receivers must handle more security data with respect to relays because the proposed protocol mainly requires the receivers to exchange information with the HeNB. Hence, the total energy consumption is greater for D2D receivers

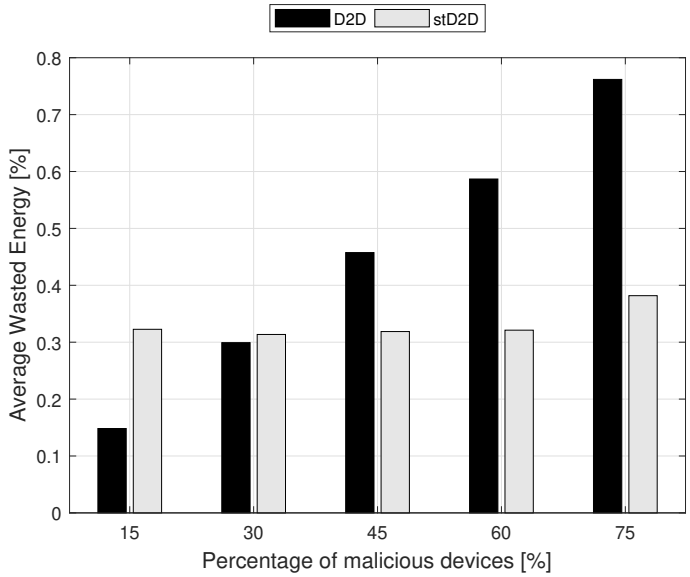


Figure 5-4: Avg. wasted energy by D2D receivers vs. % of malicious devices (for the evaluation of MtMS-stD2D protocol)

than for relays.

Figure 5-6 shows the energy consumption computed for stD2D and in the case of direct transmission (e.g., unicast), where data are sent directly by the HeNB to cell-edge devices (i.e., D2D links are not established). The graph shows that the stD2D protocol can offer greater advantages in terms of energy saving as the file dimension increases.

By summarizing, Figures 5-4, 5-5 and 5-6 highlight that stD2D protocol is able to guarantee the establishment of secure D2D communications while being not energy demanding, especially in case of large files.

It is worth noting that reliability, considered as the result of both social trustworthiness and security, is the main parameter that the proposed MtMS-stD2D protocol considers in the selection process of relay nodes. Despite the presented approach shows the best performance results, there is the possibility that relay nodes considered unreliable are not malicious, as well as the opposite case. An ineffective relay selection can worsen the performance of the D2D transmission, as efficient relays could be discarded, due to their low reputation, leading to possible throughput wastage, or unreliable nodes could be selected as data forwarders with a consequent data loss. The proposed protocol is 100% effective in the detection of malicious re-

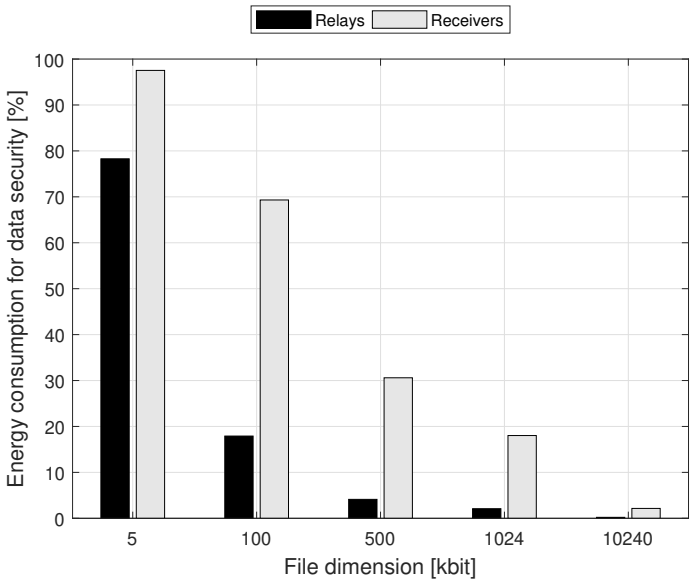


Figure 5-5: % of energy consumed for data security vs. file dimension in MtMS-stD2D

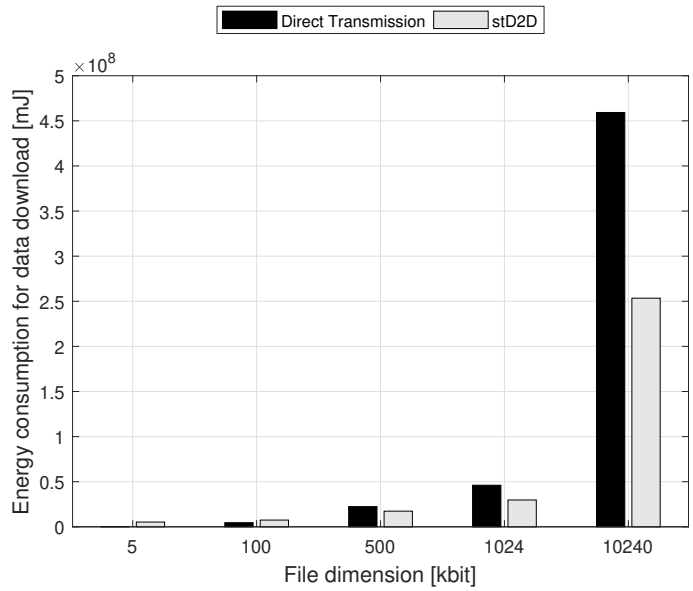


Figure 5-6: Energy used to download data under increasing file dimension (for the evaluation of MtMS-stD2D protocol)

lays when the NRV is based on the MDC value, as only the nodes that have shown malicious behaviour in the past are considered ineligible as D2D transmitters. Differently, when NRV is based on the SRF, an error is possible in the evaluation of the nature of the nodes, since the social relationships, which determine their reputation, could provide incorrect information.

5.6 Conclusions of Chapter

The MtMS-stD2D protocol, proposed in this Chapter, manages the delivery of multicast data to a group of IoT devices. Secure D2D communications to the edge-devices are established, over sidelinks, to improve the performance of the multicast transmission for the entire network. The security of D2D communications is guaranteed by using various means. First, D2D relays are selected based on their reliability, measured taking into account both security and social trustworthiness factors. Second, the DHKE protocol is used to generate the secret key used for encryption and decryption of data transmitted in D2D. This guarantees data confidentiality and integrity. Third, the protocol includes an exchange of messages that allows tracking any misbehaviour by malicious D2D transmitters.

Obtained simulation results demonstrate the effectiveness of the protocol in making a better selection of D2D transmitters, which allows to reduce data loss, thus guaranteeing almost no waste of capacity and resources. Furthermore, MtMS-stD2D proves to be not high demanding in terms of energy consumption, especially when nodes have to download large files, since it avoids that D2D receivers waste energy because of the establishment of non-secure D2D communications, thus representing an energy-efficient solution with respect to the direct transmission from the HeNB.

Chapter 6

6G: enabling technologies and security measures for the eHealth use case

The COVID-19 pandemic has changed the world. Today, the use of ICT in support of education, medicine, business and administration has become a reality practically everywhere. In particular, the digital Health (eHealth) sector is on the cusp of a revolution, fueled by the worldwide health emergency due to the spread of the new coronavirus. With a view to developing new 6G-oriented architectures, advanced eHealth services, like telemonitoring, would benefit from the support of technologies that guarantee secure data access, ultra-low latency and very-high reliability targets, which are hardly achievable by the 5G. This is the reason why this Chapter describes an innovative eHealth system architecture, in which low-latency enabling technologies, like D2D communications and MEC, are integrated and supported by security mechanisms for an optimal management of sensitive health data collected by Internet of Medical Things (IoMT) devices. A preliminary evaluation of the proposed framework is provided that shows promising results in terms of data security and latency reduction.

6.1 Introduction to Chapter

We are in the midst of a global pandemic which is bringing forth the importance of ICT in support of several fields. The worldwide emergency caused by the spread of COVID-19 has paved the way for the remote management of numerous services, including education, business and administration, and health.

In [183], *health* is identified as one of the verticals of the upcoming 6G networks, especially due to the booming average age of the population and to the sharply increasing number of chronic patients; the authors also state that a well-functioning management of healthcare services in 6G can be fostered by both the definition of new architectures and the management of security and privacy issues. Even in [184], eHealth is listed as one of the key 6G use cases that will gain by the benefits offered by enabling technologies in terms of QoS, reliability, latency, and mobility robustness. The 6G enabling technologies described in [184] include some paradigms already emerged with the 5G but not yet commercially available, which fall into the category of evolutionary technologies provided by the authors and different from that of revolutionary technologies. Among the evolutionaries are MEC and D2D communications.

The provision of cloud services represents an increasingly decisive factor in the evolution of mobile networks. Authors of [185] discuss that 6G will be pivotal in fostering a push towards edge computing paradigms able to significantly reduce latency and increase capacity. MEC is a distributed cloud paradigm came into the 5G picture for its capability to bring closer to users the storage, computation or network resources to be provided. Thereby, it can offer a wide range of beneficial properties, notably *(i)* providing additional storage space to devices that need it, *(ii)* reducing latency in data processing by leveraging proximity to the consumers, *(iii)* lightening the workload on resources-constrained devices by performing even computationally complex operations, and *(iv)* offering context-awareness information. The D2D paradigm allows two neighbor devices to communicate directly without going through the base station; this entails that latency in communications can be considerably reduced thanks to the mutual proximity between the devices. As

stated in Chapter 5, it is also known as *sidelink* transmission, since the D2D devices communicate on the direct sidelink interface, and it requires protection with security mechanisms designed to deal with security attacks to which it is vulnerable. Overall, the security requirement is a Key Performance Indicator (KPI) of 6G services, according to the authors of [186], therefore it is of prominent importance for the 6G design process. Especially with a view to providing 6G healthcare services, the protection of data transmitted by IoMT devices is essential given the sensitivity of the data and the vulnerability of the wireless medium [187]. Security solutions for cloud-based healthcare systems already exist in the literature, like in [188], where authors present a fine-grained searchable encryption scheme where a blockchain network is leveraged to execute computationally intensive tasks of a typical attribute-based searchable encryption scheme.

In light of these considerations, cloud (meant as MEC), D2D, and security can be seen as well-suited solutions to be exploited for the management of eHealth services that require low latency and high reliability. Table 6.1 outlines the most relevant works in the literature that introduce cloud-based solutions for the eHealth; for each paper, the presence or absence of a proposal that includes MEC and/or D2D and/or security mechanisms is highlighted. The ability of D2D to improve the transmission of health data from the collecting nodes to the MEC servers is not exploited enough in the literature. The lack of proposals on a secure management of health data transmitted and stored on MEC servers represents another significant shortcoming.

In line with the related work, a hierarchical architecture for the delivery of eHealth services in 6G-oriented networks will be introduced in this Chapter. It is characterized by the integration of *D2D* communications, *MEC* technology, and *security* mechanisms. The novelty of this proposal can be outlined in the following contributions:

- A hierarchical eHealth system is proposed that includes a novel architecture and groundbreaking security mechanisms to be applied for the protection of the sensitive health information and of the privacy of involved devices.

- The presented architecture is thoroughly described in Section 6.3. It comprises

Table 6.1: Related work on cloud-based solutions for eHealth

Reference	Topic	MEC	D2D	Security
[190]	A Cloud-centric IoMT solution is developed supported by security mechanisms and a D2D protocol for smart healthcare.	✗	✓	✓
[191]	The proposal of this work concerns an eHealth system improved by the implementation of D2D communications, to accelerate the transmission of health data, and the support of a mutual authentication protocol.	✗	✓	✓
[192]	A MEC-based hierarchical architecture is proposed for tracking the COVID-19 pandemic which includes the IoT end device, the edge, and the cloud levels and a user front-end.	✓	✗	✗
[193]	A system which combines 5G, MEC, and Artificial Intelligence is presented for remote health monitoring, data analysis, and high-quality data transmission.	✓	✗	✗
[194]	A Lightweight Privacy-preserving Medical diagnosis in Edge computing is introduced in order to offer timely and secure diagnosis to users who submit their requests to the edge.	✓	✗	✓
[195]	Authors face some issues related to clinical decision support systems by proposing a solution which integrates MEC and SDN technologies. Furthermore they rely on homomorphic encryption mechanisms to protect the privacy of medical information.	✓	✗	✓

three layers for the Sensing, Processing, and Storage of health data. The Sensing functionality is executed by IoT devices deployed for the collection of medical data, therefore classifiable as *IoMT*. In the middle layer, the Processing role is played by *controllers* that are not mere IoT gateways since, like in a SDN environment, they control the work of the sensing devices in addition to gather the data they collect. The Storage of information elaborated by controllers is delegated to *MEC servers*. This can be considered a 6G-oriented feature, as the controllers perform task offloading for the MEC servers, which could be congested in the 6G according to the claim of the authors of [189].

- D2D is leveraged in the data delivery from IoMT devices to controllers in order to reduce latency.

- As regards the security assurance, a primary requirement is faced that is the authentication of devices involved in the D2D communications. In order to obtain mutual authentication between the resource-constrained IoMT nodes and the controllers in charge of receiving data from them, an innovative lightweight protocol is introduced in this Chapter, which also generates a fake identity for each device running it in order to hide its real identity, thus protecting its privacy. The steps of the presented authentication procedure are deeply described in Section 6.4, where other security measures are also proposed.

- Different analyses are carried out to prove the ability of the proposal to provide a secure and lightweight solution for the support of eHealth services; these are discussed in Section 6.5.

The main purpose of the proposal formulated in this Chapter is to introduce a pragmatic architecture adaptable to the management of different eHealth services in 6G-oriented networks. Two possible use cases could be caring-at-home and caring-at-hospital: the IoMT devices can be deployed for the collection of health data useful for the monitoring of patients who are at home or of those hospitalized in intensive care, in order to minimize contacts between patients and medical staff; the latency reduction obtained thanks to the establishment of D2D communications for

the health data transmission can be really useful to ensure greater promptness in accessing the necessary care; the context-awareness provided by the MEC servers can improve the completeness of the patients-related information; the execution of the proposed security protocol can guarantee the protection of extremely sensitive health data.

Before going into the details of the proposal, a discussion on the usefulness of 6G enabling technologies to the extension of digitization and connectivity will be provided in Section 6.2, in order to highlight how, before being able to consider eHealth a widespread reality, it is necessary to ensure that the Digital Divide phenomenon is overcome, so that all the worldwide people can have access to digital services.

6.2 The 6G technologies for extending access to digital Health

6.2.1 The Digital Divide in the time of COVID-19

The digital divide has existed since access to the Internet began to spread among the worldwide population. This phenomenon consists of the gap between people who have access to the digital world and those who have not, for various reasons, such as geographical location, economic status, level of education, and general interests. Nonetheless, the health emergency triggered by the COVID-19 propagation has actually opened our eyes on the difficulties related to a life far from the digital world.

The origin of the digital divide dates back to the mid-nineties when in U.S., through the publication of some reports, the differences between people with access to the Internet ("haves") and those without ("have-nots") began to be analyzed. The phenomenon of the digital divide has evolved over time, passing from the *first-level*, related to the problems of access and connectivity, to the *second-level*, consisting in the lack of the necessary skills to properly exploit ICT, and finally to the *third-level*, concerning the differences in the outcomes and consequences obtained by using the Internet.

According to this, the different types of digital divide can be classified in two major categories: the *service-delivery divide* and the *service-fruition divide*. The former concerns the digital exclusion caused by the absence of network infrastructures necessary for Internet access and digital services delivery; the latter can be considered related to a person-specific divide, since an insufficient level of digital literacy or a set of physical inabilities could prevent people from enjoying the benefits deriving from the fruition of digital services.

The existence of these conditions not only affects the origin and the past of the digital divide phenomenon, but also concerns the current time. As a matter of fact, the state of health emergency we are still experiencing has exacerbated the digital gap. In the enterprise context, the resilience of companies has been enabled only for those that invested in technological innovation. This has represented a lifeline for the operational continuity of the businesses that had the readiness to carry out the *digital metamorphosis* path, necessary for survival in the period of COVID-19. Similarly, receiving the provision of numerous services in telematic and innovative modalities has proved to be straightforward only for the part of the population inclined to use ICT; all the others encountered not a few difficulties in adapting to the new set-up imposed by the measures implemented to limit the pandemic. It can be said that the digital exclusion corresponds to an exclusion from access to services by now. Indeed, going through the pandemic caused by COVID-19, we have realized how important technology is as a mean able to keep people in contact with the outside world by digitally receiving different types of services. This is the reason why a service-based classification is introduced in this Section to group the causes of the digital divide.

Regarding the future evolution of the digital gap phenomenon, *normalization* and *stratification* are the two contradictory predictions that have been defined in the literature. According to the first, over time the differences that cause the gap will gradually disappear until they reach saturation; it relies on the belief that government institutions will succeed in facilitating Internet access in the long run. Conversely, the second promotes the idea that the digital divide will unavoidably grow, owing to a continuing tightening of disparities within societies. This perspec-

tive appears to be more realistic, since increasing network coverage alone may not suffice to bridge the digital divide, instead, technology ought to be exploited to bring people closer to the digital world.

6.2.2 The technologies for bridging the service-delivery divide

Different technologies are expected to support 6G networks as possible solutions to the problems of extending network coverage and accessibility to connectivity. To understand how the technologies of the future can help facilitate the delivery of eHealth services by bringing connectivity to the entire world population, in the following, possible implementations of technologies that can be considered powerful tools for overcoming the service-delivery divide, as they would be able to offer Internet access even where traditional network infrastructures fall short, will be examined. Some of the 6G technologies that will be mentioned belong to the *evolutionary* category, which differ from the *revolutionary* as it includes technologies that have been already considered promising for the deployment of 5G but they are not yet suitably widespread.

Non-Terrestrial Networks

Non-Terrestrial Networks (NTNs) encompass spaceborne and airborne systems. Satellites may be either geostationary (*i.e.*, GEO) or orbit around the Earth at low or medium orbits (*i.e.*, LEO and MEO). Among LEO satellites, a growing interest has risen towards CubeSats, a new class of miniaturized satellites known for their very small dimension and low cost, hence enabling their deployment in mega-constellations to provide global connectivity and large throughput. Equally interesting are Unmanned Aerial Vehicles (UAVs) that may be deployed in swarms to provide on-demand aerial infrastructure where needed. Based on these features, NTNs can come into play to mitigate the digital gap, by ensuring connectivity to massive number of Internet of Everything (IoE) devices where terrestrial networks can fail, therefore in disadvantaged areas, in emergency scenarios, and in highly

crowded environments.

Exploiting Higher Frequencies

To truly bridge the digital divide, ultra-high-speed communications required to deliver 6G services need to be enabled. A very promising solution in this direction is to exploit new portions of the spectrum [197]. While the millimeter wave band has been already considered in 5G mobile networks, now the interest is moving towards TeraHertz and even optical bands, motivated by the very recent advances in electronics and photonics that enabled the manufacturing of portable equipment operating at such frequencies. However, signal propagation becomes critical due to severe path loss, high molecular absorption, and the requirement for very precise antenna pointing. Coverage extension may be achieved by means of Intelligent Reflecting Surfaces (IRS) [198] that allow to realize a virtual Line-of-Sight (LoS) link by smartly reconfiguring the wireless propagation environment. Mainly, IRS exploit massive low-cost passive reflecting elements integrated on a planar surface that independently reflect the incident signal to collaboratively achieve fine-grained three-dimensional (3D) passive beamforming for directional signal enhancement. Service-delivery divide could benefit from the use of higher frequencies in application scenarios that span from indoor coverage to Earth-to-ground communications.

Device-to-Device

Although technologies such as SDN have emerged as enablers in the evolution process of 5G networks, the trend to evaluate distributed networking approaches in order to extend the network coverage and scalability has gained great momentum. On the eve of 6G, this still represents a key solution to boost the access to connectivity, therefore also to bridge the digital divide. Particularly, D2D communications could be harnessed to master the problem of the limited distance that the higher frequency waves exploited in future 6G networks can cover [189]. Actually, relay nodes could be exploited to forward the signal through the establishment of direct communications, thus extending network coverage and facilitating access to services even to devices outside the antenna's LoS. Thanks to the proximity between end-devices, D2D can

enable very high speed and low latency communications, hence they can be exploited by IoE devices to improve the transmission of the big data produced in the remote execution of 6G services.

Multi-access Edge Computing

In the vein of the previous statement on the shifting to distributed networking paradigm, also the MEC is increasingly catching the eye, since it allows to improve the delivery of services in several respects. First of all, the resources of MEC servers can be provided, through virtualization, to limited-resources consumers based on the most appropriate service model (IaaS, PaaS, SaaS). Then, the proximity of the MEC to users enables various benefits, including low latency and context-awareness, which allows to customize the service delivery to the needs of the consumers. The authors of [199] cite the efficacy of MEC in providing support to communication, computing, and storage, thus improving the QoS provided to users. This can be considered as a plus in bridging the digital gap as poor QoS is seen as an impediment to the effective delivery of bandwidth-intensive services.

6.2.3 The technologies for bridging the service-fruition divide

Over the past couple of years, the presence of a pandemic has accentuated the problem of the service-fruition divide, affecting those who have inabilities to access digital services, not because of infrastructural issues, but rather of their physical conditions, handicaps, age or digital illiteracy. To integrate eHealth services into the health systems of the different countries of the world, inclusive solutions should be designed to allow access to digital services even for people culturally far away from the world of technology. The most debated solutions to the service-fruition divide will be presented in the following.

Extended Reality

Extended Reality (XR), which encompasses key terms such as Virtual Reality (VR) and Augmented Reality (AR), is believed to drive several IoE-based applications

in the 6G era whose requirements cannot be satisfied by 5G [200]. In particular, XR pervasive applications will depend not only on the networking constraints, but also on the perceptual and sensory ones, which should be aligned with the above (i.e., tolerate delays that are imperceptible to the human senses). If requirements are met, XR is an extremely powerful tool to overcome the service-fruition divide, as even digital illiterates would be able to interact with a controlled digital world through actions and perceptions that leverage all five senses (haptic, gestures, sound and speech, virtual sight, etc.).

Brain-Computer Interfaces

Brain Computer Interfaces (BCI) have been used extensively in assisting elderly or disabled people. With EEG interfaces, humans can interact with electronic devices without involving physical motion. While wired BCI have been active for years, wireless BCI are less supported due to their stringent QoS and QoE requirements. Over the last years, a handful of wireless BCI implemented through short-range communication technologies in local area networks can be observed, for use cases like home automation and digital healthcare [201]. However, these technologies are far from bridging the service-fruition divide, as their pervasiveness is limited to localized areas and hardcoded functions (e.g., switching on and off smart bulbs, etc.). With the perspective of 6G, requirements for deploying BCI at large could be met and the deployment of a set of compelling applications in, for instance, urban environments could become a reality. Just like (and probably more than) XR, BCI may be the new frontier of Human-Computer Interaction, involving IoT devices that will pervade our urban realities and will enable 6G ultra low-latency connections.

Affective computing

Affective computing encompasses a set of use cases that will be particularly enhanced by 6G technologies. It refers primarily to devices that can adapt their service provisioning schemes according to the mood and the emotions of the final user. The 6G brings on the table a set of concepts that will change the way in which service provisioning takes place. One such is Human-Centric Services (HCS), a set of ser-

vices that put the final user in the foreground and match her or his requirements to network performances, making affective computing potentially more pervasive than ever. This is especially tailored to the educational use case, for instance in enhancing the relationship between teacher and student in online classes through online automatic learning processes fed by physical parameters (e.g., posture, speech and expression) [202]. This results into involving more individuals who would instead be cut out due to, e.g., lack of attention.

Table 6.2 shows a classification based on the possible employment of each technology described in Sections 6.2.2 and 6.2.3 for the resolution of the major categories of digital divide (i.e., service-delivery and service-fruition).

Table 6.2: Technologies classification based on the mastered type of Digital Divide

Technology	**Service-Delivery**	**Service-Fruition**
Affective Computing	✗	✓
Artificial Intelligence (AI)	✓	✓
Brain Computer Interfaces (BCI)	✗	✓
Device-to-Device (D2D)	✓	✗
Exploiting Higher Frequencies	✓	✗
Extended Reality (XR)	✗	✓
Multi-access Edge Computing (MEC)	✓	✗
Non-Terrestrial Networks (NTNs)	✓	✗

6.2.4 Artificial Intelligence: the ultimate breakthrough?

AI plays a role of paramount importance in the evolution process that wireless networks are experiencing. Its use can enhance the performance of many applications by providing a wide range of beneficial properties. In particular, Machine Learning (ML) is a branch of AI that is considered a top solution in many tricky 6G applications. The ML technology allows to train systems that, by the processing of collected data, can learn patterns by experience and, consequently, improve the performance and quality of the offered services. In particular, following the recent progress in deep learning as well as the advent of smart devices that are capable of processing ML algorithms on the edge, the wireless community has gained a renewed and huge

interest in such technologies, which can now be leveraged in use cases that were unable to support them before. Now, with edge AI and ML, networks of heterogeneous objects that are self-organizing and can meet high KPIs can be envisioned even in harsh scenarios via, e.g., reinforcement learning [200]. In this context, we are witnessing the shift of AI and ML components closer and closer to the edge, to the point that ML is projected to be an actual part of 6G technologies, rather than something that builds on top of them as it was with previous generations. Another remark is that this transition is expected to take place *transversely*, which means that potentially all 6G technologies will be affected at once.

This discussion aims to bring forth the potential achievable by applying AI to the purpose of lowering the gap brought by the digital divide. Current trends suggest that both the service-delivery gap and the service-fruition gap would benefit greatly from embedding AI into shared resources. In such a context, any single node of the network will produce data about connectivity, environment and such, and the collection of big-data from IoT scenarios is a key enabler to better understand the challenges of various nature in Internet access. Specifically, data is then analysed through ML to create more inclusive and scalable networks. For example, data could be gathered and investigated to comprehend which categories of people make better use of the benefits provided by ICT and which ones find difficulties in doing so. According to [203], ML can improve the network performance through the undertaking of *adaptive network optimization actions*, enabled by the ability to learn from the wireless environment that ML provides to the network infrastructure. In such sense there are a lot of potential usages that meet the purpose of bridging the digital divide. Certain types of network traffic, if their nature is well understood by an AI engine, could be privileged (e.g., remote health diagnosis, online lectures) in contrast to others (e.g., entertaining). Historical network parameters observed by edge nodes can also feed a fog/edge ML model so that the distribution of network resources could be locally automated. Moreover, *planning* capabilities could be introduced to lower the risks of shortages under normal resource usage. This is also crucial to coordinate with mobile and on-demand network resources, as in NTNs, forming a real "collective network intelligence" [200] to overcome the service-delivery

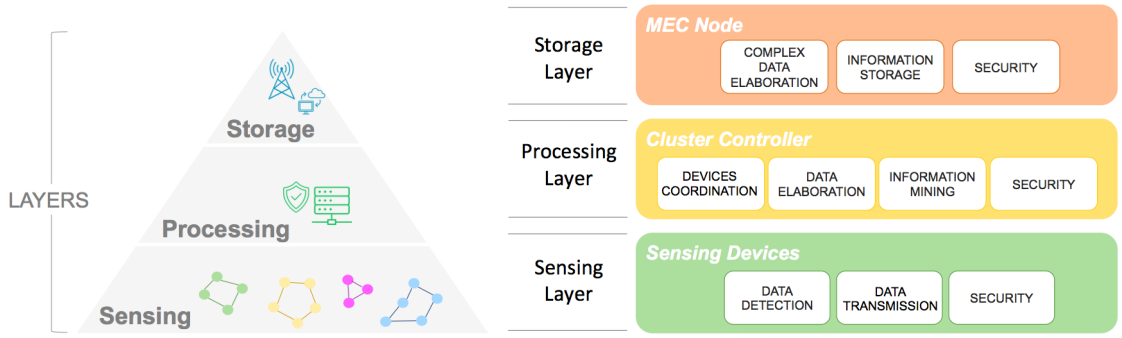
gap and bring resources where and when they are most needed. On the other hand, AI is also a powerful tool for improving the accessibility of innovative digital services for people with a low level of digital literacy, notably the elderly, people with disabilities, people living underdeveloped areas. Usages in this direction are often mentioned in the literature, for example in [204], where authors survey some works concerning the application of technology to the provision of accessible cultural heritage sites experiences, also highlighting the importance of the role of AI in adapting the offered experiences to the target audience. Moreover, most of the technologies presented for bridging the service-fruition gap rely on AI and ML as their core enablers. This entails that AI could be a powerful tool for overcoming the digital cultural and cognitive gap, as it could be used to support those who would otherwise remain "digitally excluded".

6.3 The proposed architecture to support 6G eHealth systems

A MEC-based architecture for the D2D-aided collection of health data coming from low-end IoMT devices is proposed in this Chapter. The security and privacy issues, which arise from the transmission and storage of highly sensitive health data, are addressed and an innovative solution for the fulfilment of the mutual authentication requirement between D2D communicating devices is proposed. Figure 6-1 shows the hierarchical eHealth system that represents the main novelty of the proposal elaborated in this Chapter. In Figure 6-1(a) the three layers that compose the proposed architecture are depicted at a high level, only showing the major functionality of each one, i.e., Sensing, Processing, and Storage. In Figure 6-1(b) the functional components of the three layers are illustrated, each with corresponding block of executable operations. In particular, the Sensing Devices are the functional component of the Sensing layer since they execute Data Detection, Data Transmission, and Security operations; the Cluster Controller (CC) (or CC node) performs Devices Coordination, Data Elaboration, Information Mining, and Security management in the Processing layer; finally, the MEC node is the functional component of the Stor-

age layer, being it in charge of carrying out Complex Data Elaboration, Information Storage, and Security supervision.

Hereinafter, more details will be provided on the three layers of the proposed architecture, on the related functional components, and on the operations executed by each.



(a) (b)

Figure 6-1: (a) Layers and (b) functional components of the proposed hierarchical eHealth system architecture

Sensing

The lowest level is that of Sensing, consisting of the IoMT devices deployed for the health data detection and organized in clusters based on an established criterion, for example the monitored patient in the case of the Telemonitoring service (*Data Detection*). The measured data are sent from the devices to the CC node via D2D communications, enabled by the proximity between the IoMT devices and the CC node (*Data Transmission*).

Processing

Each cluster is managed by a CC node, belonging to the Processing layer of the proposed architecture and deployed with the aim of reducing the workload on low-end IoMT devices, but also of offloading the tasks executed by the MEC servers. The CC node is not a simple gateway, since it does not just gather the data detected by the Sensing layer, but it represents a *Broker* in the interaction between MEC server and IoMT devices, and a "smart leader" for the latter. In fact, similar to a

SDN solution, the controller represents the software and smart component of the cluster, in charge of instructing sensing devices on the operations to carry out and the modalities to be engaged (e.g., it communicates the timing of data collection). In addition, it collects the data obtained within its own cluster and extracts information from it. For example, let us consider using a smart-oximeter on a patient: the CC node instructs the oximeter on the time intervals that must elapse between one measurement and another (*Devices Coordination*); once the controller receives the data coming from the oximeter, it can process and translate it into information useful for monitoring the patient (*Data Elaboration*); hence, the controller can perceive if an anomalous value has been detected (*Information Mining*).

Storage

The MEC node represents the highest level of the proposed architecture and is located in the base station. Its main function concerns the storing of information obtained from various controllers (*Information Storage*). This is an eHealth-oriented benefit offered by the proposed architecture as data, being stored in the edge, are accessible with low latency. Besides, MEC can be delegated by a CC node to perform a particularly computationally complex data processing (*Complex Data Elaboration*). Thanks to its strategic position, the MEC node enables two additional features: *(i)* it can collect context-awareness information; *(ii)* it can offer the possibility of quickly implementing the service models characteristic of cloud computing environments, namely IaaS, PaaS, and SaaS. For example, the MNO managing the MEC server could offer a platform to software developers working for an hospital; or even, the MNO itself could develop applications useful for identifying COVID-19 or for its tracking as off-the-shelf solutions for interested Tenants.

6.4 Introduced security measures

A *Security* functional block is present in each layer of the proposed architecture as security is one the foremost requirements in the management of health data. Particularly, before establishing data transmission, IoMT devices (i.e., sensors) and

controllers must accomplish an *authentication procedure* in which the MEC node is involved as a supervisor and trusted third party; in addition, the controllers should also cater for the *encryption* of data and information transmitted to the MEC node. As part of the novelty of the proposal of this Chapter, an innovative mutual authentication protocol is presented in the following.

A lightweight mutual authentication procedure

In order to ensure security within each cluster, sensors have to be certain of the identity and genuineness of the CC node towards which they send data and, vice versa, it is of paramount importance that only authorized devices transmit data to the controller. For this purpose, a Lightweight Mutual Authentication procedure for D2D communications (LiMAD) is proposed in this Chapter that is suited to the constrained nature of IoMT sensing devices and aimed at protecting the data exchanged in D2D communications. The flow of the operations performed in the proposed authentication procedure is shown in Figure 6-2 and detailed in the following; used notations are listed in Table 6.3.

Starting with the first group of operations ($GO()$), the MEC node receives the identity (ID) (e.g., the SIM serial number) both from the sensor i and the CC node j via secure channels. Then, it generates: *(i)* a secret random number sn_i associated to the sensor i; *(ii)* a secret key K_j which it will securely share with the CC node j; a key for the ID encryption of both *(iii)* the sensor i (i.e., KI_i) and *(iv)* the CC node j (i.e., KI_j). Consequently, it computes the $GO(1)$:

$$\begin{aligned} D_1 &= H(ID_i||sn_i); \\ D_2 &= D_1 \oplus K_j; \\ eID_j &= ID_j \oplus KI_j; \\ eID_i &= ID_i \oplus KI_i; \\ FID_j &= H(eID_j); \\ FID_i &= H(eID_i); \end{aligned} \tag{6.1}$$

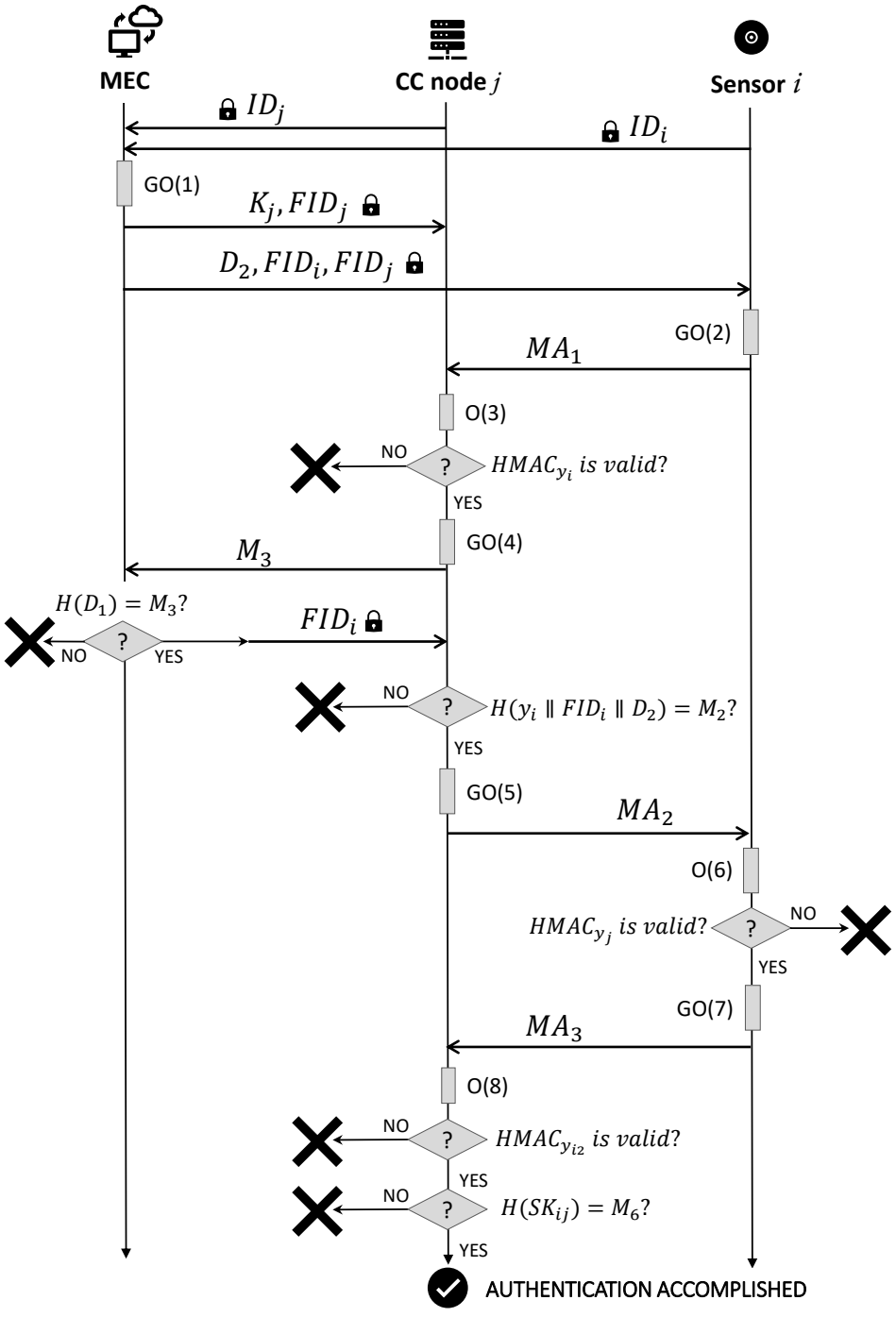


Figure 6-2: The LiMAD authentication procedure

Table 6.3: Notations used in the LiMAD authentication procedure.

Notation	Description
sn_i	A Secret random Number generated by the MEC node and associated to sensor i
y	A secret random number (e.g. y_i is the one generated by sensor i)
K_j	A secret key generated by the MEC node and shared only with the legitimate CC node j
KI	The Key used for the encryption of the ID (e.g. KI_i is the key used for ID_i)
ID	Identity (e.g. ID_i is the identity of sensor i)
eID	Encrypted Identity (e.g. eID_i is the encrypted identity of sensor i)
FID	Fake Identity (e.g. FID_i is the fake identity of sensor i)
$H()$	A secure hash function
$HMAC$	Hashed Message Authentication Code (e.g. $HMAC_{y_i}$ is computed using the key y_i)
D	Preliminary Data
$GO()$	Group of Operations (e.g. $GO(1)$ is the group of operations number (1))
MA	Message for Authentication
$O()$	Operation (e.g. $O(3)$ is operation number 3)
M	Generic Message
SK_{ij}	The Secret Key shared only between the two authenticating entities

where, D indicates preliminary data, $H()$ is a secure hash function, eID represents an encrypted ID, and FID stands for a fake identity.

After that, the MEC node sends, via secure channels, K_j, FID_j to the CC node j and D_2, FID_i, FID_j to the sensor i. The latter generates a secret random number y_i and executes the second group of operations $GO(2)$:

$$M_1 = FID_j \oplus y_i;$$

$$M_2 = H(y_i||FID_i||D_2);$$

$$MA_1 = D_2||M_1||M_2||HMAC_{y_i}(D_2||M_1||M_2), \tag{6.2}$$

where, M discloses a generic message and MA_1 denotes the first message used for the mutual authentication. Subsequently, it sends MA_1 to the CC node which performs the following operation ($O(3)$):

$$y_i = M_1 \oplus FID_j, \tag{6.3}$$

necessary to continue the authentication procedure because it is preparatory to the check of the HMAC previously computed by the sensor i with y_i. In fact, if the CC node computes $HMAC_{y_i}(D_2||M_1||M_2)$ and obtains a different value from the one received by the sensor in MA_1, then the procedure fails because, clearly, the integrity and authenticity of the message have been breached. Differently, if the HMAC check is successful, the CC node accomplishes the fourth group of operations $GO(4)$:

$$\begin{aligned} D_1 &= D_2 \oplus K_j; \\ M_3 &= H(D_1). \end{aligned} \tag{6.4}$$

Therefore, it sends M_3 to the MEC which can check that this matches with its computation of $H(D_1)$; if the check is successful, the MEC sends the FID_i to the CC node over a secure channel. This step allows the controller to verify the integrity of M_2 to proceed with the generation of y_j and the execution of the fifth group of operations $GO(5)$:

$$\begin{aligned} SK_{ij} &= H(y_i||y_j); \\ M_4 &= FID_i \oplus y_j; \\ MA_2 &= M_4||HMAC_{y_j}(M_4), \end{aligned} \tag{6.5}$$

where, SK_{ij} is the secret key that must be shared only between the two authenticating entities. Thereby, the CC node sends MA_2 to the sensor, which performs the following operation $O(6)$ with the aim of computing y_j and checking the HMAC included in MA_2:

$$y_j = M_4 \oplus FID_i. \tag{6.6}$$

If the control of the HMAC is successful, the sensor generates a different y_{i2} to compute the HMAC of a new message. In fact, according to LiMAD, sensor and CC node must use a unique HMAC key for each message exchange session. Then, the sensor executes the seventh group of operations $GO(7)$:

$$\begin{gathered} SK_{ij} = H(y_i||y_j); \\ M_5 = FID_j \oplus y_{i2}; \\ M_6 = H(SK_{ij}); \\ MA_3 = M_5||M_6||HMAC_{y_{i2}}(M_5||M_6), \end{gathered} \tag{6.7}$$

sending the resulting MA_3 to the CC node. By now, the final operations of the procedure begin. In order to verify the validity of the HMAC, the CC node carries out the following operation $O(8)$:

$$y_{i2} = M_5 \oplus FID_j. \tag{6.8}$$

If the HMAC is valid, it performs the last check for the assessment of the SK_{ij}: if the key is the legitimate one, then the authentication procedure is successfully accomplished.

Other security measures

The layers of the proposed architecture can be managed by different stakeholders. For example, it is reasonable to assume that an MNO owns and operates the MEC node, while the Hospital, as a Tenant, could administer the Processing and Sensing levels. According to the definition of 5G stakeholders given in Chapter 2, the MNO is defined as *the entity operating its mobile network infrastructure to provide connectivity to end-users*, while a Tenant is *a service provider which acquires the virtual*

network services to make them available to its users. As also stated in Chapter 2, numerous actors can populate 5G environments with the effect that the deployment of different stakeholders in a virtualized architecture makes the system vulnerable to many security threats. Among these, the problem of storing data relating to hospital and patients on a MEC managed by an external entity is one of the most concerning. The use of homomorphic encryption can be a valid solution to this problem, as it allows processing on encrypted data while keeping plaintext hidden. Referring to the architecture proposed in this Chapter, cluster controllers could apply homomorphic encryption on the data before sending them to the MEC, so that it stores encrypted information and cannot operate on plaintext. This represents a proper countermeasure to the threat of Data Breach in multi-tenant environments.

6.5 Results

6.5.1 Security analysis

Similarly to [205][206][119], first, a security analysis of the proposed LiMAD authentication protocol is carried out by discussing the security requirements it is able to guarantee.

Identity privacy protection

This is a requirement of paramount importance in the health ecosystem, also when dealing with COVID-19 [207]. The fear of a violation of patient data privacy represented a big obstacle to the use of ICT to fight against the COVID-19. The proposed LiMAD is aimed at the protection of the privacy through the definition of a secure method for identifying nodes in the network even apart from the authentication procedure. In fact, the MEC computes an encrypted version of both sensor and controller IDs, by means of secret keys, and further protects their privacy by computing fake identities. In LiMAD, the MEC is in charge of performing all operations required for the safeguard of the privacy in order to move, as much as possible, the computational burden of security towards the network.

Message authentication

The implementation of message authentication is important to foster the assurance of two remarkable properties for the exchanged messages: integrity and authenticity. The former implies that who does not know the key used for message authentication cannot modify the message; the latter guarantees that the key generator is the sender of the message. HMAC is a message authentication method that is well suited to lightweight authentication protocols; for example, it is used in the protocol for low-end IoT devices introduced in [208]. Also in LiMAD, the HMAC is implemented by network nodes in all the messages for authentication (MAs) in order to ensure their integrity and authenticity. For example, the sensor i inserts in MA_1 the HMAC computed with the random number y_i, previously selected and never exchanged in clear; only the legitimate receiver, associated to the FID_j, is able to compute y_i in $O(3)$, then to calculate $HMAC_{y_i}(D_2||M_1||M_2)$ and to verify that this matches the one received by the sensor. As regards messages coming from the MEC node, it represents a trusted third party, from which, along with receiving a wide range of beneficial properties, nodes obtain information that are considered undoubtedly true. Actually, the MEC establishes only secure connections with the nodes so as to deliver unbreakable messages.

Mutual authentication

In [209], mutual authentication is considered a necessary measure for the realization of edge computing integration in time-sensitive IoT applications expected for future 6G networks. The LiMAD is effective in mutual authentication between sensor and controller thanks to the exchange of a set of MAs. In particular, the sensor is authenticated thanks to MA_1 and to the check on M_3 performed by the MEC, as only the legal node can own information on D_1. Whereas, the controller is authenticated trough MA_2, as it contains the FID_i only sent by the MEC to the licit CC node. The further steps, including MA_3, are aimed at generating a shared secret key between sensor and controller able to strengthen their mutual authentication.

Resistance to replay attacks

A replay attack occurs when a malicious entity intercepts the communication between two parties and delays the sending of messages (or replicates them) to manipulate the receiver. The susceptibility to this type of attack of some contact tracing apps used to thwart the spread of COVID-19 is known and declared in the literature, for example in [210], where authors state that authentication procedures represent a valid countermeasure to these attacks. The LiMAD is resistant to replay attacks thanks to the use of random session keys. In fact, during the authentication procedure, in each communication between sensor and controller, a different secret random number y is used which also acts as a session token useful to prevent someone else from replying the message. If a receiver gets two messages containing the same session token, it knows that a replay attack has occurred.

Resistance to Man-in-the-Middle attack

The Man-in-the-Middle attack allows a malicious entity to meddle in a communication between parties without being noticed, for example, by pretending to be one of them and sending messages on its behalf. This threat represents a significant vulnerability of D2D communications, so, it is important to face it. The occurrence of such an attack during the authentication process would pose a serious threat to the protection of health data. Actually, an attacker could be able to impersonate a controller, thus receiving data sent by the sensing nodes and using the obtained information at its own discretion. To prevent this, LiMAD provides for the implementation of several measures. First of all, the impossibility for malicious entities to replicate the MAs thanks to the intervention of the trusted third party, which ensures that only legitimate nodes have important information for authentication purposes (e.g., D_2 and K_j).

6.5.2 Communication and Computational overhead

Likewise other papers in the literature that present security proposals (e.g., [211]), a measurement of the communication and computational overhead due to LiMAD

is provided in this Chapter. The operations referred hereinafter are represented in Figure 6-2 and detailed in Section 6.4.

Starting with the *Communication Overhead*, the performed evaluation is based on the hypothesis of using SHA-256 as hash function, also for the computation of the HMAC. Actually, thanks to an interesting comparison among three well-known hashing algorithms (i.e., SHA-256, SHA-1, and MD5) probed by authors of [212], it can be inferred that SHA-256 represents the best trade-off in terms of latency, energy consumption, and security level. In view of this, the assessment of the bytes required by the messages exchanged in LiMAD follows. The transmission of the IDs by the sensor and the CC node requires roughly $16B$ each. The MEC node has to deliver the message with K_j, FID_j (i.e., $64B$) to the CC node and the one with D_2, FID_i, FID_j (i.e., $96B$) to the sensor, hence it has to send $64+96 = 160B$. The MA_1 costs $128B$ to the sensor. The CC node sends $32B$ for M_3 to the MEC, which replies with the $32B$ of FID_i. Finally, the MA_2 requires $64B$ to the CC node to which the sensor responds with $96B$ for the MA_3. The authentication protocol described in [205] uses security mechanisms comparable with those implemented by LiMAD, therefore it represents the best touchstone in the literature. To carry out the comparison, it can be assumed: to use the same parameter setting for the IDs and for the hash function; to consider the router of the architecture of [205] as the equivalent of the CC node of the LiMAD architecture and the authentication server as the LiMAD MEC. In so doing, LiMAD results in an overall bandwidth overhead of $288B$, against $240B$ of [205]. The greater overhead of LiMAD affects only the MEC node and is due to additional security controls that require the involvement of the trusted third party, hence are aimed at increasing the security of the authentication procedure. The resulting comparison is shown in Table 6.4.

Table 6.4: Communication Overhead and comparison

	LiMAD	**[205]**
MEC	$256 + 384 + 128 = 768b = 96B$	$256b = 32B$
CC node	$128 + 128 + 256 = 512b = 64B$	$640b = 80B$
Sensor	$128 + 512 + 384 = 1024b = 128B$	$1024b = 128B$

With regard to the *Computational Overhead*, distinction should be made among the computational cost required by: the XOR operation (i.e., c_x), the computation of hash function including HMAC (i.e., c_h), and the generation of a random number (i.e., c_r). Starting with the MEC, it has to spend $4 * c_r + 3 * c_h + 3 * c_x$ for the execution of $GO(1)$. Then, the sensor performs $GO(2)$, which requires $c_r + c_x + 2 * c_h$. In reply, $2 * c_x + 2 * c_h$ are needed to the CC node to carry out: $O(3)$, one HMAC check, and $GO(4)$. After that, one c_h is required to the MEC node for the M_3 check, followed by the $3 * c_h + c_r + c_x$ yielded for the CC node to obtain MA_2. The last operations performed by the sensor cost $2 * c_x + 4 * c_h + c_r$. The CC node reaches the accomplishment of the authentication procedure by spending $c_x + 2 * c_h$. The total computational overhead for each node is shown in Table 6.5, which also includes the comparison with the lightweight authentication mechanism presented in [205]. As with the communication overhead, the router of the architecture of [205] is considered as the equivalent of the CC node of LiMAD architecture and the authentication server as the LiMAD MEC.

Table 6.5: Computational Overhead and comparison

	LiMAD	**[205]**
MEC	$4 * c_r + 3 * c_x + 4 * c_h$	$2 * c_x + 2 * c_h$
CC node	$c_r + 4 * c_x + 7 * c_h$	$c_r + 6 * c_x + 7 * c_h$
Sensor	$2 * c_r + 3 * c_x + 6 * c_h$	$c_r + 4 * c_x + 7 * c_h$

The resulting comparison evidences that the protocol presented in this Chapter satisfies the requirement of lightness imposed by IoT devices. In fact, LiMAD ensures an overall saving of the computational overhead on the constrained nodes of the network by slightly increasing the load on the central and most powerful node of the architecture (i.e., the MEC).

6.5.3 Performance evaluation

In order to prove the benefit of the proposal formulated in this Chapter, a performance evaluation has been carried out concerning both the authentication protocol

and the proposed architecture.

As previously stated, the proposed LiMAD protocol causes a higher communication overhead than the approach presented in [205]. Nonetheless, Figure 6-3 shows the benefits of the increase in bandwidth demanded by LiMAD, which requires a messages exchange with the trusted third party during the authentication phase. Although this step provokes a greater exchange of information compared to the protocol presented in [205] (denoted by "OTHER" in Figure 6-3), it can foster a bandwidth loss saving since it enables a prompt detection of any attacks against the CC node. Specifically, if a controller is malicious it sends an M_3 bogus message to the MEC node, which immediately realizes the attack and blocks the authentication procedure, thus allowing bandwidth savings to the involved nodes, with benefits especially for resource-constrained sensors. In [205], there is not any involvement of a trusted third party during the authentication phase as only the two authenticating nodes participate to the procedure; this justifies the higher bandwidth loss. In detail, Figure 6-3 shows the different values of bandwidth loss when the percentage of malicious CC nodes varies and considering different numbers of sensors controlled by each.

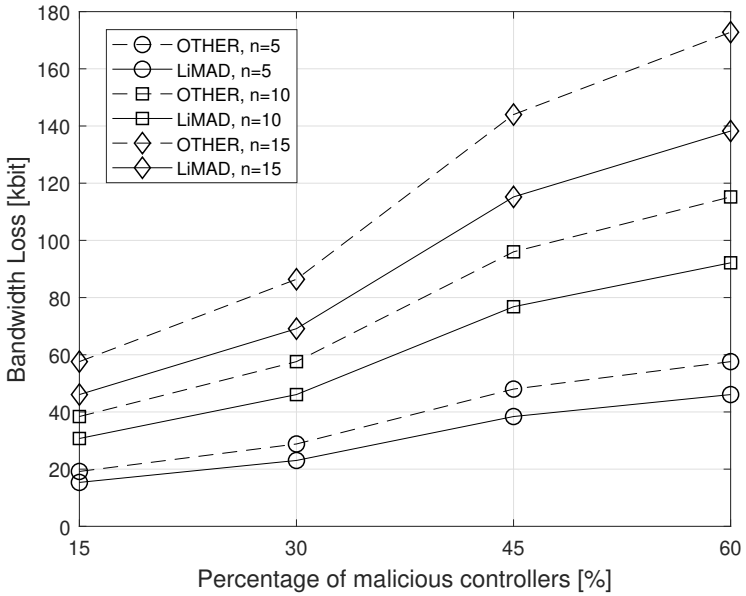


Figure 6-3: Bandwidth loss to varying of the percentage of malicious controllers (n is the number of sensors managed by each CC node)(for the evaluation of LiMAD protocol)

Figure 6-4 analyses the capability of the proposed architecture to improve the data delivery delay with respect to traditional sensors-to-MEC communication. In particular, the use of D2D combined with the execution of the authentication protocol proves to be mostly more effective than the direct data transmission to MEC. Two macro-scenarios are compared as the CQI of the sensors towards MEC increases (i.e., MEC-to-sensors distance decreases):

- **Direct:** sensing devices send data directly to the MEC, without going through the controllers.
- **D2D+Unicast:** the proposed architecture is implemented, therefore the use of cluster controllers as intermediaries for the communication between MEC and sensors is considered. The latter, following the execution of LiMAD, transmit the data in D2D to the controllers, which then forward them to the MEC. For this scenario, different cases are compared obtained by varying the position of the controller: CQI controller-MEC (cc-mec)= $3, 4, 5, 9, 11$. It is worth reminding that the communication via the controllers, due to the nature of proximity communications, is not feasible for devices that are too far from the controllers. For this reason, D2D+Unicast curves report non-zero values only if D2D communication is possible.

The graph highlights the gain that the implementation of the procedures envisaged by the proposed architecture brings in terms of transmission time savings. In particular, Figure 6-4 serves as a guidance to understand under which conditions the use of the presented approach is beneficial. As an example, in the case of the CQI cc-mec is equal to 3 (see the curve with circles), the proposed approach is able to guarantee a significantly lower data delivery delay w.r.t. the benchmark approach when CQI sensors-mec is lower than 3.

6.6 Conclusions of Chapter

The digital Health represents a future that the current global pandemic is showing not to be long in coming. The ICT is rich in means exploitable in support of the

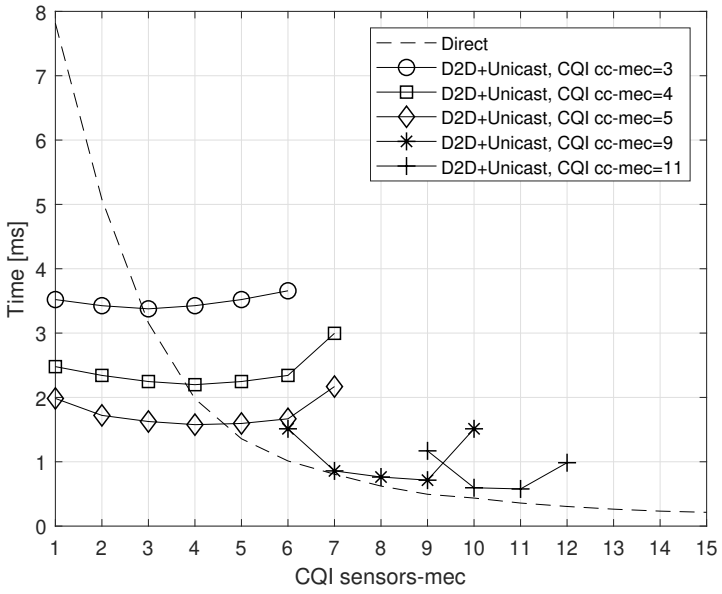


Figure 6-4: Data delivery delay experimented by means of the proposed LiMAD architecture w.r.t. traditional sensors-to-MEC communication

development of eHealth. Among the technologies that mostly attracted attention in the evolution process of the 5G network are *D2D* and *MEC*. As regards the major imperative requirements of the 5G network, *security* really caught the eye. The integration of these three factors (i.e., D2D, MEC, and security) can lead to a 6G-oriented implementation, given the requirements asked by the services that 6G will have to support. All these considerations led to the elaboration of the proposal of this Chapter which introduces a MEC-based hierarchical architecture for the execution of eHealth services in a 6G-oriented system. The proposal includes the use of D2D communications to improve the performance of data transmission and involves the accomplishment of a proposed lightweight authentication protocol suitable for resource-constrained IoMT devices that could be used, for example, for a Telemonitoring service. The proposal of this Chapter meets some of the main requirements that an eHealth system should have: *(i)* low latency in data transmission and processing, thanks to the use of D2D and MEC; *(ii)* availability of context-awareness information, offered by the use of the MEC; *(iii)* devices authentication and privacy protection, thanks to the proposed security protocol.

Chapter 7

Conclusion

Since the trend of subscriptions to mobile networks is constantly growing, guaranteeing consumer protection has become a crucial requirement that can determine the success of the services offered by telecommunications operators. This thesis has investigated the topic of *Network Security* by examining it in different contexts. The proposals presented in the various Chapters have provided useful means for protecting the privacy of devices connected to the network and the data they exchange, in both 5G and 6G environments and by considering different use cases, in order to propose off-the-shelf solutions for different types of devices. Initially, a security analysis for 5G networks has been formulated providing a risk assessment for each of the major 5G virtualization technologies, through the distribution of impact and responsibility of the assets to the mainly involved stakeholders. Afterwards, a protocol for managing secure multicast communications has been proposed which includes the implementation of protected D2D communications. The upgrade of this proposal has been, then, provided through the introduction of a trustworthiness model able to prevent the occurrence of security breaches thanks to the selection of reliable D2D transmitters. The application of security and trust mechanisms in scenarios characterized by mMTC traffic has been evaluated, later, shifting the focus of the performance evaluation of the proposed protocol to the ability of the implemented security mechanisms to optimize the energy consumption of resource-constrained IoT devices. Finally, security solutions for communications carried out in 6G-oriented eHealth environments have been presented and a discussion on the

phenomenon of the Digital Divide has been addressed, considering the impact that COVID-19 has had on it and the contribution that 6G could make for the problem resolution.

Glossary

3G Third Generation. 10

3GPP 3rd Generation Partnership Project. 53

4G Fourth Generation. 10

5G Fifth Generation. 10

5GPPP 5G Infrastructure Public Private Partnership. 16

6G Sixth Generation. 10

ADR Aggregate Data Rate. 70

AI Artificial Intelligence. 152

AP Application Plane. 34

APIs Application Program Interfaces. 22

AR Augmented Reality. 150

ARPF/UDM Authentication credential Repository and Processing Function / Unified Data Management. 79

B2B Business to Business. 19

B2B2C Business to Business to Consumer. 19

B2C Business to Consumer. 19

BCI Brain Computer Interfaces. 151

BM Business Model. 19

BM-SC Broadcast Multicast-Service Center. 59

BS Base Station. 121

C-LOR Co-Location Object Relationship. 98

C-WOR Co-Working Object Relationship. 98

CC Cluster Controller. 154

CMS Conventional Multicast Scheme. 52

CN Core Network. 30

CoI Community of Interest. 83

CP Control Plane. 32

CQI Channel Quality Indicator. 58

CSA Cloud Security Alliance. 21

D2D Device-To-Device. 11

D2D-SF D2D-enhanced CMS with Single Frequency. 54

D2MD Device-To-Device Multicast. 57

DDoS Distributed DoS. 23

DHKE Diffie-Hellman Key Exchange. 55

DL Downlink. 116

DoS Denial of Service. 23

DP Data Plane. 33

DRX Discontinuous Reception. 121

EAP-AKA' Extensible Authentication Protocol for Authentication and Key Agreement. 87

EC-GSM Extended Coverage Global System for Mobile Communications. 119, 120

eCMS-sD2D enhanced CMS with secure D2D communications. 55

eHealth digital Health. 141

eLTE evolution of Long Term Evolution. 53

eMBB enhanced Mobile Broadband. 78

eMBMS evolved Multimedia Broadcast Multicast Service. 54

eNB eNodeB. 54

EPC Evolved Packet Core. 35

ETSI European Telecommunications Standards Institute. 24

FDD Frequency Division Duplexing. 120

GDPR General Data Protection Regulation. 133

gNB Next Generation NodeB. 84

HCS Human-Centric Services. 151

HeNB Home-evolved NodeB. 125

HeNB-GW HeNB gateway. 125

HetNet Heterogeneous Networks. 123

HMAC Hashed Message Authentication Code. 55

IaaS Infrastructure as a Service. 20

ICT Information and Communications Technology. 10

IMSI International Mobile Subscriber Identity. 87

InP Infrastructure Provider. 15

IoE Internet of Everything. 148

IoMT Internet of Medical Things. 141

IoT Internet of Things. 11

IRS Intelligent Reflecting Surfaces. 149

ISG Industry Specification Group. 24

KPI Key Performance Indicator. 143

LiMAD Lightweight Mutual Authentication procedure for D2D communications. 157

LoRa Long Range. 125

LoS Line-of-Sight. 149

LTE Long Term Evolution. 42

LTE-A Long Term Evolution-Advanced. 56

LTE-M LTE for Machines. 119

MANO Management and Orchestration. 35

MAs Mobile Agents. 45

MBA malicious behavior amount. 68

MBMS Multimedia Broadcast Multicast Service. 59

MBMS-GW Multimedia Broadcast Multicast Service-gateway. 59

MCCH Multicast Control Channel. 121

MCE multicell/multicast coordination entity. 59

MCS Modulation and Coding Scheme. 58

MEC Multi-access Edge Computing. 10

MG Multicast Group. 62

ML Machine Learning. 152

MME Mobility Management Entity. 35

mMTC massive Machine Type Communications. 11

MNO Mobile Network Operator. 17

MSP Mobile Service Provider. 15

MtMS Machine-type Multicast Service. 117

MtMS-CE MtMS coordination entity. 125

MtMS-GW MtMS gateway. 125

MtMS-SC MtMS serving center. 125

MtMS-stD2D MtMS with secure and trust D2D. 118

NaaS Network-as-a-Service. 19

NB-IoT Narrowband IoT. 115

NBI Northbound Interface. 30

NC Network Coding. 57

NFV Network Function Virtualization. 10

NFVI NFV Infrastructure. 35

NFVIaaS NFVI as a Service. 35

NIST National Institute of Standards and Technology. 25

NOS Network Operation System. 32

NR New Radio. 53

NSaaS Network Slicing as Service. 19

NTNs Non-Terrestrial Networks. 148

OFDMA Orthogonal Frequency Division Multiple Access. 58

OOR Owner Object Relationship. 97

OS Operating System. 43

OSP Online Service Provider. 50

OTT Over-The-Top. 49

P2P Peer-to-Peer. 80

PaaS Platform as a Service. 20

PDF Probability Density Function. 97

PID pseudoidentity. 64

PIN Personal Identification Number. 41

POR Parental Object Relationship. 98

PRB Physical Resource Block. 120

ProSe Proximity-based Services. 133

PtM Point-to-Multipoint. 53

QoE Quality of Experience. 29

QoS Quality of Service. 20

RAN Radio Access Network. 30

RB Resource Block. 58

RN Relay Node. 55

RTOS Real-Time Operating Systems. 43

SaaS Software as a Service. 25

SBI Southbound Interface. 30

SC-FDMA Single Carrier Frequency Division Multiple Access. 58

SC-PTM Single Cell Point to Multipoint. 117

SCC Security Control Classes. 81

SCS Service Capability Server. 125

SDN Software Defined Networking. 10

SDWSN Software-Defined Wireless Sensor Network. 42

SeT-D2D Secure and Trust D2D. 75

SIDF Subscription Identifier De-concealing Function. 79

SIOT Social IoT. 80

SOR Social Object Relationship. 98

SORT Self-ORganizing Trust. 82

SP Service Provider. 15

SR Security Realms. 81

SUCI Subscription Concealed Identifier. 77

SUPI Subscription Permanent Identifier. 77

TDD Time Division Duplex. 69

TN Transport Network. 30

TTI Transmission Time Interval. 69

UAVs Unmanned Aerial Vehicles. 148

UE User Equipment. 62

UL Uplink. 116

URLLC Ultra-Reliable and Low Latency Communication. 78

V2X Vehicle to Everything. 53

VIM Virtual Infrastructure Manager. 35

VM Virtual Machine. 24

VNF Virtualised Network Function. 35

VNFaaS VNF as a Service. 36

VR Virtual Reality. 150

XaaS Anything as a Service. 20

XR Extended Reality. 150

Bibliography

[1] "Ericsson Mobility Report," Ericsson, June 2021.

[2] "EU-wide coordinated risk assessment of 5G networks security, " October 2019. Available at: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[3] P. Schneider, C. Mannweiler, and S. Kerboeuf, "Providing strong 5G mobile network slice isolation for highly sensitive third-party services," 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018.

[4] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User Privacy, Identity and Trust in 5G," is part of: A Comprehensive Guide to 5G Security, pp. 267-279, 2018.

[5] Deliverable D3.3, "5G NORMA network architecture – Final report," October 2017.

[6] V. Frascolla et al., "Millimeter-waves, MEC, and network softwarization as enablers of new 5G business opportunities," 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018.

[7] Deliverable D2.2 Trust model, "5G-ENSURE," August 2016.

[8] NGMN Alliance, "5G White Paper," v.1, February 2015.

[9] J. Magen, T. Lahnalampi, and Giulia Pastor, "The 5G PPP Stakeholders Glossary," 2017.

[10] S. Elayoubi et al., “5G innovations for new business opportunities,” 5GPPP white paper for the Mobile World Congress, March 2017.

[11] “Network Functions Virtualisation (NFV); Management and Orchestration; Network Service Templates Specification,” ETSI GS NFV-IFA 014, V2.1.1, October 2016.

[12] P. Ahokangas et al., "Business Models for Local 5G Micro Operators,” in IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 3, pp. 730-740, Sept. 2019.

[13] S. Yrjölä, P. Ahokangas, M. Matinmikko-Blue, “Novel Context and Platform Driven Business Models via 5G Networks,” 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), September 2018.

[14] X. Zhou, R. Li, T. Chen, and H. Zhang, “Network slicing as a service: enabling enterprises’ own software-defined cellular networks,” in IEEE Communications Magazine, vol. 54, no. 7, pp. 146-153, July 2016.

[15] “The Threacherous 12 - Top Threats to Cloud Computing + Industry Insights,” Cloud Security Alliance, 2017.

[16] “5G security – Package 3: Mobile Edge Computing, Low Latency, Consistent User Experience,” NGMN Alliance, v.2, February 2018.

[17] V. A. Cunha, E. da Silva, M. B. de Carvalho, D. Corujo, J. P. Barraca, D. Gomes, L. Z. Granville, and R. L. Aguiar, “Network slicing security: Challenges and directions,” Wiley Internet Technology Letters, vol. 2, no. 5, September 2019.

[18] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, “Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes,” Elsevier Journal of Network and Computer Applications, vol. 101, pp. 55-82, January 2018.

[19] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol 17, no. 4, pp. 2317-2346, August 2015.

[20] T. Islam, D. Manivannan, and S. Zeadally, "A Classification and Characterization of Security Threats in Cloud Computing," in International Journal of Next-Generation Computing, vol. 7, no. 1, March 2016.

[21] A. Aljuhani and T. Alharbi, "Virtualized Network Functions security attacks and vulnerabilities," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), January 2017.

[22] S. S. Tirumala, H. Sathu, and V. Naidu, "Analysis and Prevention of Account Hijacking Based INCIDENTS in Cloud Environment," 2015 International Conference on Information Technology (ICIT), December 2015.

[23] H. Zhou, C. Wu, C. Yang, P. Wang, Q. Yang, Z. Lu, and Q. Cheng, "SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices," in IEEE/ACM Transactions on Networking, vol. 26, no.5, pp. 2048-2061, October 2018.

[24] S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," in IEEE Communications Magazine, vol. 55, no.8, pp. 211-217, August 2017.

[25] T. Ubale and A. K. Jain, "Survey on DDoS Attack Techniques and Solutions in Software-Defined Network," is part of: Handbook of Computer Networks and Cyber Security, pp. 389-419, January 2020.

[26] "5G security recommendations Package #2: Network Slicing," NGMN Alliance, v.1.0, April 2016.

[27] "Mobile-Edge Computing – Introductory Technical White Paper," ETSI, September 2014.

[28] "MEC in 5G networks," ETSI White Paper No. 28, June 2018.

[29] "Multi-access Edge Computing (MEC); Framework and Reference Architecture," ETSI GS MEC 003, V2.1.1, January 2019.

[30] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," Elsevier Future Generation Computer Systems, vol. 78:2, pp. 680-698, January 2018.

[31] S. Shahzadi, M. Iqbal, T. Dagiuklas, and Z. U. Qayyum , "Multi-access edge computing: open issues, challenges and future perspectives," Journal of Cloud Computing, article number 30(2017), December 2017.

[32] M. Almorsy, J. Grundy, and I. Müller, "An Analysis of the Cloud Computing Security Problem," Proc. of the APSEC 2010 Cloud Workshop, September 2016.

[33] H. Liu, F. Eldarrat, H. Alqahtani, A. Reznik, X. de Foy, and Y. Zhang, "Edge Computing Security: State of the Art and Challenges," in IEEE Systems Journal, vol. 12, no. 3, pp. 2495-2508, September 2018.

[34] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Computer Security Resource Center, September 2011.

[35] "MEC Proofs of Concept," ETSI.

[36] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450-465, February 2018.

[37] Q. Pham et al., "A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art," in IEEE Access, vol. 8, pp. 116974-117017, 2020.

[38] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu and W. Lv, "Edge Computing Security: State of the Art and Challenges," in Proceedings of the IEEE, vol. 107, no. 8, pp. 1608-1631, Aug. 2019.

[39] A. R. Suraj, S. J. Shekar, and G. S. Mamathae, "A Robust Security Model for Cloud Computing Applications," 2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), March 2018.

[40] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, May 2017.

[41] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," in Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, January 2015.

[42] M. Pham and D. B. Hoang, "SDN applications - The intent-based Northbound Interface realisation for extended applications," 2016 IEEE NetSoft Conference and Workshops (NetSoft), June 2016.

[43] Z. Shu and T. Taleb, "A Novel QoS Framework for Network Slicing in 5G and Beyond Networks Based on SDN and NFV," in IEEE Network, vol. 34, no. 3, pp. 256-263, May/June 2020.

[44] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN Control: Survey, Taxonomy, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 333-354, Firstquarter 2018.

[45] M. Jarschel, T. Zinner, T. Hossfeld, P. Tran-Gia, and W. Kellerer, "Interfaces, attributes, and use cases: A compass for SDN," in IEEE Communications Magazine, vol. 52, no. 6, pp. 210-217, June 2014.

[46] A. Kliks, B. Bossy, S. N. Khan, R. Riggio, and L. Goratti, "An architecture for spectrum management and coordinated control in 5G heterogeneous networks," 2016 International Symposium on Wireless Communication Systems (ISWCS), September 2016.

[47] A. Al Hayajneh, M. Z. A. Bhuiyan , and I. McAndrew, "Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN)," MDPI Computers, vol. 9:1, February 2020.

[48] M. Shamseddine, I. Elhajj, A. Chehab, and A. Kayssi, "A virtual QoS-adaptive network connectivity service: An SDN approach," in 2016 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), November 2016.

[49] A. Farshad, P. Georgopoulos, M. Broadbent, M. Mu, and N. Race, "Leveraging SDN to provide an in-network QoE measurement framework," in 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), April 2015.

[50] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196-248, Firstquarter 2020.

[51] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, April 2018.

[52] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3682-3722, May 2019.

[53] F. Hu, Q. Hao, and K. Bao, "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2181-2206, May 2014.

[54] Y. D. Lin, T. L. Liu, J. H. Chen, and Y. C. Lai, "Soft Partitioning Flow Tables for Virtual Networking in Multi-Tenant Software Defined Networks," in IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 402-415, March 2018.

[55] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on Network Virtualization Hypervisors for Software Defined Networking," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 655-685, October 2015.

[56] "Network Functions Virtualisation (NFV); Architectural Framework," ETSI GS NFV 002, v. 1.1.1, October 2013.

[57] I. F. Akyildiz, S. Nie, S. C. Lin, and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," Elsevier Computer Networks, vol. 106, pp. 17-48, September 2016.

[58] A. U. Rehman, R. L. Aguiar, and J. P. Barraca, "Network Functions Virtualization: The Long Road to Commercial Deployments," in IEEE Access, vol. 7, pp. 60439-60464, May 2019.

[59] "Network Functions Virtualisation (NFV); Use Cases," ETSI GR NFV 001, v. 1.2.1, May 2017.

[60] "Network Functions Virtualisation (NFV); Use Cases," ETSI GS NFV 001, v. 1.1.1, October 2013.

[61] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View," in IEEE Access, vol. 6, pp. 55765-55779, September 2018.

[62] "Description of Network Slicing Concept," NGMN Alliance, v.1.0.8, September 2016.

[63] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network Slicing in 5G: Survey and Challenges," in IEEE Communications Magazine, vol. 55, no. 5, pp. 94-100, May 2017.

[64] R. Sanchez-Iborra, S. Covaci, J. Santa, J. Sanchez-Gomez, J. Gallego-Madrid, and A. F. Skarmeta, "MEC-Assisted End-to-End 5G-Slicing for IoT," in 2019 IEEE Global Communications Conference (GLOBECOM), December 2019.

[65] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, and C. S. Hong, "Network Slicing: Recent Advances, Taxonomy, Requirements, and Open Research Challenges," in IEEE Access, vol. 8, pp. 36009-36028, February 2020.

[66] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks," in IEEE Access, vol. 5, pp. 25408-25420, November 2017.

[67] M. Alrowaily and Z. Lu, "Secure Edge Computing in IoT Systems: Review and Case Studies," in 2018 IEEE/ACM Symposium on Edge Computing (SEC), October 2018.

[68] B.S. Archana, A. Chandrashekar, A. G. Bangi, B.M. Sanjana, and S. Akram, "Survey on usable and secure two-factor authentication," in IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), May 2017.

[69] J. M. Batalla and F. Gonciarz, "Deployment of smart home management system at the edge: mechanisms and protocols," Neural Computing and Applications, vol. 31, no. 5, pp. 1301–1315, May 2019.

[70] D. Mattos and O. Duarte, "AuthFlow: authentication and access control mechanism for software defined networking", Springer Annals of Telecommunications, vol. 71, pp. 607-615, March 2016.

[71] H. Cui, Z.Chen, L. Yu, K. Xie, and Z. Xia, "Authentication mechanism for network applications in SDN environments," in IEEE 20th International Symposium on WPMC, December 2017.

[72] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "SecMANO: Towards Network Functions Virtualization (NFV) Based Security MANagement and Orchestration," in IEEE 2016 IEEE Trustcom/BigDataSE/ISPA, August 2017.

[73] G. Xu, Y. Tang, Z. Yan, and P. Zhang, "TIM: A Trust Insurance Mechanism for Network Function Virtualization Based on Trusted Computing," Springer Se-

curity, Privacy, and Anonymity in Computation, Communication, and Storage, pp. 139-152, December 2017.

[74] J. Ni, X. Lin, and X. Sherman Shen, "Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 3, pp. 644-657, March 2018.

[75] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4755-4763, June 2019.

[76] S. W. Pritchard, G. P. Hancke, and A. M. Abu-Mahfouz, "Cryptography Methods for Software-Defined Wireless Sensor Networks," in IEEE 27th ISIE, June 2018.

[77] M. Bousselham, A. Abdellaoui, and H. Chaoui, "Security against Malicious Node in the Vehicular Cloud Computing using a Software-Defined Networking Architecture," in IEEE icSoftComp, December 2017.

[78] M. T. Raza, S. Lu, and M. Gerla, "vEPC-sec: Securing LTE Network Functions Virtualization on Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 12, pp. 3287-3297, December 2019.

[79] B. Bordel, A. B. Orúe, R. Alcarria, and D. Sánchez-De-Rivera, "An intra-slice security solution for emerging 5G networks based on pseudo-random number generators," in IEEE Access, vol. 6, pp. 16149-16164, March 2018.

[80] I. Farris, T. Taleb, H. Flinck, and A. Iera, "Providing ultra-short latency to user-centric 5G applications at the mobile network edge," Wiley Transactions on Emerging Communications Technologies, vol. 29, no. 4, April 2018.

[81] R. Di Pietro and F. Lombardi, "Virtualization Technologies and Cloud Security: Advantages, Issues, and Perspectives," From Database to Cyber Security, pp. 166-185, November 2018.

[82] M. Caprolu, R. Di Pietro, F. Lombardi, and S. Raponi, "Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues," in 2019 IEEE International Conference on Edge Computing (EDGE), July 2019.

[83] A. Bratterud, A. Happe, and B. Duncan, "Enhancing Cloud Security and Privacy: The Unikernel Solution," in Proceedings of the 8th International Conference on Cloud Computing, GRIDs, and Virtualization, February 2017.

[84] J.Talbot, P. Pikula, C. Sweetmore, S. Rowe, H. Hindy, C. Tachtatzis, and R. Atkinson "A Security Perspective on Unikernels," 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), June 2020.

[85] M. Compastié, R. Badonnel, O. Festor, and R. He, "From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models," Elsevier Computer & Security, vol. 97, October 2020.

[86] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective," in IEEE Journal on Selected Areas in Communications, vol. 35, pp. 2586-2595, October 2017.

[87] J. Grover and R. M. Garimella, "Reliable and Fault-Tolerant IoT-Edge Architecture," 2018 IEEE SENSORS, October 2018.

[88] H. Huang and S. Guo, "Proactive Failure Recovery for NFV in Distributed Edge Computing," in IEEE Communications Magazine, vol. 57, no. 5, pp. 131–137, March 2019.

[89] V. Sciancalepore, F. Giust, K. Samdanis, and Z. Yousaf, "A double-tier MEC-NFV architecture: Design and optimisation," 2016 IEEE Conference on Standards for Communications and Networking (CSCN), November 2016.

[90] P. Vizarreta, C. M. Machuca, and W. Kellerer, "Controller placement strategies for a resilient SDN control plane," in IEEE 8th International Workshop on Resilient Networks Design and Modeling (RNDM), September 2016.

[91] M. J. F. Alenazi and E. K. Çetinkaya, "Resilient placement of SDN controllers exploiting disjoint paths," Wiley Transactions on Emerging Telecommunications Technologies, vol. 31, no. 2, February 2020.

[92] M. Tanha, D. Sajjadi, R. Ruby, and J. Pan, "Capacity-Aware and Delay-Guaranteed Resilient Controller Placement for Software-Defined WANs," in IEEE Transactions on Network and Service Management, vol. 15, no. 3, pp. 991-1005, September 2018.

[93] L. Spitzner, "Honeypots: catching the insider threat," 19th Annual Computer Security Applications Conference, December 2003.

[94] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. A. Calero, "Virtual IoT HoneyNets to Mitigate Cyberattacks in SDN/NFV-Enabled IoT Networks," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1262-1277, June 2020.

[95] P. A Pandire and V. B Gaikwad, "Attack Detection in Cloud Virtual Environment and Prevention Using Honeypot," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), July 2018.

[96] S. Ravji and M. Ali, "Integrated Intrusion Detection and Prevention System with Honeypot in Cloud Computing," 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), August 2018.

[97] V. Mahajan and S. K Peddoju, "Integration of network intrusion detection systems and honeypot networks for cloud security," 2017 International Conference on Computing, Communication and Automation (ICCCA), December 2017.

[98] A. Mtibaa, K. Harras, and H. Alnuweiri, "Friend or Foe? Detecting and Isolating Malicious Nodes in Mobile Edge Computing Platforms," in 2015 IEEE 7th International Conference on Cloud Computing Technology and Science, December 2015.

[99] A. S. Sohal, R. Sandhu, S. K.Sood, and V. Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," Elsevier Computers & Security, vol. 74, pp. 340-354, May 2018.

[100] G. Xu, Y. Tang, Z. Yan, and P. Zhang, "Leveraging Machine Learning Approach to Setup Software-Defined Network(SDN) Controller Rules During DDoS Attack," Springer Proceedings of International Joint Conference on Computational Intelligence, Communication, and Storage, pp. 49-60, July 2019.

[101] C. Miranda, G. Kaddoum, E. Bou-Harb, S. Garg, and K. Kaur, "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2602-2615, February 2020.

[102] M. Bonfim, M. Santos, K. Dias, and S. Fernandes, "A real-time attack defense framework for 5G network slicing," Wiley Journal of Software: Practice and Experience, February 2020.

[103] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, "Virtual security as a service for 5G verticals," IEEE WCNC, April 2018.

[104] Available at: https://www.snort.org/

[105] Available at: https://suricata-ids.org/

[106] Available at: https://www.ntop.org/products/traffic-analysis/ntop/

[107] Available at: http://www.oracle.com/us/solutions/cloud/platform-as-a-service/shared-responsibility-model-wp-3497462.pdf

[108] Available at: https://aws.amazon.com/it/compliance/shared-responsibility-model/

[109] Available at: https://aws.amazon.com/it/iot/customers/

[110] G. Fodor et al., "Design aspects of network assisted device-to-device communications," in IEEE Communications Magazine, vol. 50, no. 3, pp. 170-177, March 2012.

[111] "Cisco Visual Networking Index: Forecast and Methodology," Cisco, 2017.

[112] "General aspects and principles for interfaces supporting Multimedia Broadcast Multicast Service (MBMS) within E-UTRAN," 3GPP TS 36.440 Release 11, 2012.

[113] J. Liu, W. Chen, Z. Cao and K. B. Letaief, "Dynamic Power and Sub-Carrier Allocation for OFDMA-Based Wireless Multicast Systems," 2008 IEEE International Conference on Communications, 2008

[114] L. Militano, M. Condoluci, G. Araniti, A. Molinaro, A. Iera and G. Muntean, "Single Frequency-Based Device-to-Device-Enhanced Video Delivery for Evolved Multimedia Broadcast and Multicast Services," in IEEE Transactions on Broadcasting, vol. 61, no. 2, pp. 263-278, June 2015.

[115] "5G security – Enabling a trustworthy 5G system," White Paper, Ericsson, 2018.

[116] P. Gandotra, R.K. Jha, and S. Jain, "A survey on device-to-device (D2D) communication: Architecture and security issues," Journal of Network and Computer Applications, vol. 68, pp. 9-29, 2017.

[117] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma and J. Ott, "Security and Privacy in Device-to-Device (D2D) Communication: A Review," in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1054-1079, Secondquarter 2017.

[118] M. Wang and Z. Yan, "A Survey on Security in D2D Communications," Mobile Networks and Applications, vol. 22, pp. 195-208, 2017.

[119] A. Zhang, J. Chen, R. Q. Hu and Y. Qian, "SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp. 2659-2672, April 2016.

[120] Understanding 5G: Perspectives on future technological advancements in mobile, White paper, GSMA Intelligence, 2014.

[121] A. Asadi, Q. Wang and V. Mancuso, "A Survey on Device-to-Device Communication in Cellular Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1801-1819, Fourthquarter 2014.

[122] F. Boabang, H. H. Nguyen, Q. V. Pham, and W. J. Hwang, "Network-assisted Distributed Fairness-aware Interference Coordination for Device to Device Communication Underlaid Cellular networks," Mobile Information Systems, 2017.

[123] Q. V. Pham, H. L. To, and W. J. Hwang, "A Multi-Timescale Cross-Layer Approach for Wireless Ad Hoc Networks," Computer Networks, vol. 18, pp. 471-482, 2015.

[124] G. Araniti, M. Condoluci, P. Scopelliti, A. Molinaro and A. Iera, "Multicasting over Emerging 5G Networks: Challenges and Perspectives," in IEEE Network, vol. 31, no. 2, pp. 80-89, March/April 2017.

[125] L. Feng et al., "Resource Allocation for 5G D2D Multicast Content Sharing in Social-Aware Cellular Networks," in IEEE Communications Magazine, vol. 56, no. 3, pp. 112-118, March 2018.

[126] J. R. Bhat, J. Sheu and W. Hon, "Resource Allocation Schemes for Revenue Maximization in Multicast D2D Networks," in IEEE Access, vol. 5, pp. 26340-26353, 2017.

[127] A. Antonopoulos, E. Kartsakli and C. Verikoukis, "Game theoretic D2D content dissemination in 4G cellular networks," in IEEE Communications Magazine, vol. 52, no. 6, pp. 125-132, June 2014.

[128] E. Datsika, A. Antonopoulos, N. Zorba and C. Verikoukis, "Cross-Network Performance Analysis of Network Coding Aided Cooperative Outband D2D Communications," in IEEE Transactions on Wireless Communications, vol. 16, no. 5, pp. 3176-3188, May 2017.

[129] L. Militano, G. Araniti, M. Condoluci, I. Farris, and A. Iera, "Device-to-Device Communications for 5G Internet of Things," EAI Endorsed Transactions on Internet of Things, 2015.

[130] "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)," 3GPP TS 36.300 Release 11, 2012.

[131] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976.

[132] H. Meshgi, D. Zhao and R. Zheng, "Optimal Resource Allocation in Multicast Device-to-Device Communications Underlaying LTE Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 9, pp. 8357-8371, Sept. 2017.

[133] F. Rinaldi, S. Pizzi, A. Orsino, A. Iera, A. Molinaro, and G. Araniti, "A novel approach for MBSFN Area Formation aided by D2D Communications for eMBB Service Delivery in 5G NR Systems," IEEE Transactions on Vehicular Technology, vol. 69, no. 2, pp. 2058-2070, Feb. 2020.

[134] "Security Architecture and Procedures for 5G System," 3GPP TS 33.501, Technical Specification Group Services and System Aspects.

[135] C. Campolo, A. Molinaro, A. Iera, and F. Menichella, "5G Network Slicing for Vehicle-to-Everything Services," in IEEE Wireless Communications, vol. 24, no. 6, pp. 38-45, Dec. 2017.

[136] "System Architecture for the 5G System; Stage 2 (Release 15)," 3GPP TS 23.501, Technical Specification Group Services and System Aspects.

[137] G. Arfaoui, et al., "A Security Architecture for 5G Networks," in IEEE Access, vol. 6, pp. 22466-22479, 2018.

[138] S. Andreev et al., "A unifying perspective on proximity-based cellular-assisted mobile social networking," in IEEE Communications Magazine, vol. 54, no. 4, pp. 108-116, April 2016.

[139] M. Nitti, V. Popescu, and M. Fadda, “Using an IoT Platform for Trustworthy D2D Communications in a Real Indoor Environment," in IEEE Transactions on Network and Service Management, vol. 16, no. 1, pp. 234-245, March 2019.

[140] F. H. Kumbhar, N. Saxena, and A. Roy, “Reliable Relay: Autonomous Social D2D Paradigm for 5G LoS Communications,” in IEEE Communications Letters, vol. 21, no. 7, pp. 1593-1596, July 2017.

[141] Bo Bai, Li Wang, Zhu Han, Wei Chen, and Tommy Svensson, “Caching based socially-aware D2D communications in wireless content delivery networks: a hypergraph framework,” in IEEE Wireless Communications, vol. 23, no. 4, pp. 74-81, August 2016.

[142] A. B. Can and B. Bhargava, “SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems,” in IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 1, pp. 14-27, Jan.-Feb. 2013.

[143] Z. Chen, R. Ling, C. Huang, and Xu Zhu, “A scheme of access service recommendation for the Social Internet of Things,” International Journal of Communication Systems, vol. 24, pp. 694-706, March 2016.

[144] X. Li and L. Liu, “Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities,” in IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843-857, July 2004.

[145] E. Damiani, S. De capitani di Vimercati, S. Paraboschi, M. Pesenti, P. Samarati, and S. Zara, “Fuzzy logic techniques for reputation management in anonymous peer-to-peer systems,” In EUSFLAT Conference, pp. 43-48, September 2003.

[146] F. Bao, R. Chen, and J. Guo, “Scalable, adaptive and survivable trust management for community of interest based internet of things systems,” 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), 2013.

[147] R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," in IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 6, pp. 684-696, 1 Nov.-Dec. 2016.

[148] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things," in IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), 2012.

[149] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," in IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 5, pp. 1253-1266, May 2014.

[150] R. Piqueras Jover and V. Marojevic, "Security and Protocol Exploit Analysis of the 5G Specifications," in IEEE Access, vol. 7, pp. 24956-24963, 2019.

[151] A. Josang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," In Proceedings of the 29th Australasian Computer Science Conference, pp. 85-94, 2006.

[152] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) - When Social Networks meet the Internet of Things: Concept, Architecture and Network Characterization," Computer Networks, vol. 56, pp. 3594-3608, Nov. 2012.

[153] S. Kosta, A. Mei, and J. Stefa, "Small World in Motion (SWIM): Modeling Communities in Ad-Hoc Mobile Networking," 2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2010.

[154] H. Alzaid, et al. "Reputation-based trust systems for wireless sensor networks: A comprehensive review," IFIP International Conference on Trust Management Springer, Berlin, Heidelberg, 2013.

[155] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, "Secure D2D Communication for 5G IoT Network Based on Lightweight Cryptography," Applied Sciences, vol.10, Dec. 2019.

[156] Y. Jiang, Y. Shen, and Q. Zhu, "A Lightweight Key Agreement Protocol Based on Chinese Remainder Theorem and ECDH for Smart Homes," Sensors, vol. 20, March 2020.

[157] "Ericsson Mobility Report," Ericsson, June 2019.

[158] S. A. Alvi, B. Afzal, G. A.Shah, L. Atzori, and W. Mahmood, "Internet of multimedia things: Vision and challenges," Elsevier Ad Hoc Networks, vol. 33, pp. 87-111, 2015.

[159] A. Martin et al., "Network Resource Allocation System for QoE-Aware Delivery of Media Services in 5G Networks," in IEEE Transactions on Broadcasting, vol. 64, no. 2, pp. 561-574, June 2018.

[160] A. Karaagac, E. Dalipi, P. Crombez, E. De Poorter, and J. Hoebeke, "Lightweight Streaming Protocol for the Internet of Multimedia Things: Voice Streaming over NB-IoT," Elsevier Pervasive and Mobile Computing, vol. 59, 2019.

[161] J. Bukhari and W. Yoon, "Multicasting in Next-Generation Software-Defined Heterogeneous Wireless Networks," in IEEE Transactions on Broadcasting, vol. 64, no. 4, pp. 915-921, Dec. 2018.

[162] J. Nightingale, P. Salva-Garcia, J. M. A. Calero and Q. Wang, "5G-QoE: QoE Modelling for Ultra-HD Video Streaming in 5G Networks," in IEEE Transactions on Broadcasting, vol. 64, no. 2, pp. 621-634, June 2018.

[163] M. Condoluci, G. Araniti, T. Mahmoodi, and M. Dohler, "Enabling the IoT Machine Age With 5G: Machine-Type Multicast Services for Innovative Real-Time Applications," in IEEE Access, vol. 4, pp. 5555-5569, 2016.

[164] A. Moubayed, A. Shami, and H. Lutfiyya, "Wireless Resource Virtualization With Device-to-Device Communication Underlaying LTE Network," in IEEE Transactions on Broadcasting, vol. 61, no. 4, pp. 734-740, Dec. 2015.

[165] A. Shaghaghi, M. Ali Kaafar, R. Buyya, and S. Jha, "Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions," Springer Handbook of Computer Networks and Cyber Security, pp. 341-387, January 2020.

[166] C. Suraci, S. Pizzi, A. Iera, A. Molinaro, and G. Araniti, "Delivering Multicast Content Through Secure D2D Communications in the Internet of Things," International Conference on Wired/Wireless Internet Communication, pp. 182-193, September 2019.

[167] "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 15)," 3GPP TS 36.300, Technical Specification Group Radio Access Network.

[168] L. Feltrin et al., "Narrowband IoT: A Survey on Downlink and Uplink Perspectives," in IEEE Wireless Communications, vol. 26, no. 1, pp. 78-86, February 2019.

[169] Y. -. E. Wang et al., "A Primer on 3GPP Narrowband Internet of Things," in IEEE Communications Magazine, vol. 55, no. 3, pp. 117-123, March 2017.

[170] J. Guo, X. Gong, J. Liang, W. Wang, and X. Que, "An Optimized Hybrid Unicast/Multicast Adaptive Video Streaming Scheme Over MBMS-Enabled Wireless Networks," in IEEE Transactions on Broadcasting, vol. 64, no. 4, pp. 791-802, Dec. 2018.

[171] G. Tsoukaneri, M. Condoluci, T. Mahmoodi, M. Dohler, and M. K. Marina, "Group Communications in Narrowband-IoT: Architecture, Procedures, and Evaluation," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1539-1549, June 2018.

[172] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Elsevier Computer Networks, vol. 76, pp. 146-164, January 2015.

[173] P.K. Jamshiya, and D.M. Menon, "Design of a Trusted Third Party Key Exchange Protocol for Secure Internet of Things (IoT)," International Conference on Inventive Communication and Computational Technologies (ICICCT), April 2018.

[174] M. Pavloski, G. Görbil, and E. Gelenbe, "Bandwidth Usage—Based Detection of Signaling Attacks," Information Sciences and Systems 2015, vol. 363, pp. 105-114, August 2015.

[175] Z. M. Fadlullah, C. Wei, Z. Shi and N. Kato, "GT-QoSec: A Game-Theoretic Joint Optimization of QoS and Security for Differentiated Services in Next Generation Heterogeneous Networks," in IEEE Transactions on Wireless Communications, vol. 16, no. 2, pp. 1037-1050, Feb. 2017.

[176] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1844-1852, Dec. 2017.

[177] D. Rivera, A. Garcìa, M. L. Martìn-Ruìz, B. Alarcos, J.R. Velasco, and A. Gòmez Oliva, "Secure Communications and Protected Data for a Internet of Things Smart Toy Platform," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3785-3795, April 2019.

[178] "Ericsson Mobility Report," Ericsson, November 2018.

[179] F. Al-Turjman, E. Ever, and Hadi Zahmatkesh, "Green Femtocells in the IoT Era: Traffic Modeling and Challenges - An Overview," in IEEE Network, vol. 31, no. 6, pp. 48-55, November/December 2017.

[180] L. Militano, A. Orsino, G. Araniti, and A. Iera, "NB-IoT for D2D-Enhanced Content Uploading with Social Trustworthiness in 5G Systems," Elsevier Future Internet, vol. 9, July 2017.

[181] "Proximity-based Services (ProSe); Security aspects," 3GPP TS 33.303, Technical Specification Group Services and System Aspects.

[182] J. Huang, F. Qian, A. Gerber, Z. Mao, S. Sen, and O. Spatscheck, "A close examination of performance and power characteristics of 4G LTE networks," 10th MobySis, June 2012.

[183] L. Mucchi et al., "How 6G Technology Can Change the Future Wireless Healthcare," 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 2020, pp. 1-6.

[184] A. Shahraki et al., "A Comprehensive Survey on 6G Networks:Applications, Core Services, Enabling Technologies, and Future Challenges," 2021, available at: `arXiv:2101.12475v2`.

[185] F. Tariq, M. R. A. Khandaker, K. -K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A Speculative Study on 6G," in IEEE Wireless Communications, vol. 27, no. 4, pp. 118-125, August 2020.

[186] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence," in IEEE Wireless Communications, vol. 27, no. 5, pp. 126-132, October 2020.

[187] M. Masud et al., "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," in IEEE Internet of Things Journal (Early Access).

[188] Mamta, B. B. Gupta, K. -C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, "Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System," in IEEE/CAA Journal of Automatica Sinica (Early Access).

[189] S. Zhang, J. Liu, H. Guo, M. Qi, and N. Kato, "Envisioning Device-to-Device Communications in 6G," in IEEE Network, vol. 34, no. 3, pp. 86-91, May/June 2020.

[190] M. Kumar and S. Chand, "A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System With Public Verifiability," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10650-10659, Oct. 2020

[191] A. P. G. Lopes and P. R. L. Gondim, "Mutual Authentication Protocol for D2D Communications in a Cloud-Based E-Health System," Sensors, vol. 20, no. 7, p. 2072, Apr. 2020.

[192] A. Feriani, A. Refaey, and E. Hossain, "Tracking Pandemics: A MEC-Enabled IoT Ecosystem with Learning Capability," in IEEE Internet of Things Magazine, vol. 3, no. 3, pp. 40-45, September 2020.

[193] Y. Zhang, G. Chen, H. Du, X. Yuan, M. Kadoch, and M. Cheriet, "Real-Time Remote Health Monitoring System Driven by 5G MEC-IoT," in Electronics, vol. 9(11):1753, no. 3, pp. 40-45, October 2020.

[194] Z. Ma et al., "Lightweight Privacy-preserving Medical Diagnosis in Edge Computing," in IEEE Transactions on Services Computing, 2020.

[195] Z. Xue et al., "A Resource-Constrained and Privacy-Preserving Edge Computing Enabled Clinical Decision System: A Federated Reinforcement Learning Approach," in IEEE Internet of Things Journal, 2021 (Early Access).

[196] F. Rinaldi et al., "Non-Terrestrial Networks in 5G & Beyond: A Survey," in IEEE Access, vol. 8, pp. 165178-165200, 2020.

[197] M. Polese, J. M. Jornet, T. Melodia and M. Zorzi, "Toward End-to-End, Full-Stack 6G Terahertz Networks," in IEEE Communications Magazine, vol. 58, no. 11, pp. 48-54, November 2020.

[198] Q. Wu and R. Zhang, "Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network," in IEEE Communications Magazine, vol. 58, no. 1, pp. 106-112, January 2020.

[199] H. Saarnisaari, S. Dixit, M.-S. Alouini, A. Chaoub, M. Giordani, A. Kliks, M. Matinmikko-Blue, N. Zhang, A. Agrawal, M. Andersson et al., "A 6G white paper on connectivity for remote areas," arXiv preprint arXiv:2004.14699, 2020.

[200] W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," in IEEE Network, vol. 34, no. 3, pp. 134-142, May/June 2020.

[201] S. R. A. Jafri, T. Hamid, R. Mahmood, M. A. Alam, T. Rafi, M. Z. U. Haque, and M. W. Munir, "Wireless brain computer interface for smart home and medical system," Wireless Personal Communications, vol. 106, no. 4, pp. 2163–2177, 2019.

[202] E. Yadegaridehkordi, N. F. B. M. Noor, M. N. B. Ayub, H. B. Affal, and N. B. Hussin, "Affective computing in education: A systematic review and future research," Computers & Education, vol. 142, p. 103649, 2019.

[203] M. Chen, U. Challita, W. Saad, C. Yin and M. Debbah, "Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3039-3071, Fourthquarter 2019

[204] G. Pisoni, N. Dìaz-Rodrìguez, H. Gijlers, and L. Tonolli, "Humancentred artificial intelligence for designing accessible cultural heritage," Applied Sciences, vol. 11, no. 2, p. 870, 2021.

[205] A. Esfahani et al., "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 288-296, Feb. 2019.

[206] M. Chuang and J. Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks," in IEEE Systems Journal, vol. 8, no. 3, pp. 749-758, Sept. 2014.

[207] M. Whaiduzzaman et al., "A Privacy-Preserving Mobile and Fog Computing Framework to Trace and Prevent COVID-19 Community Transmission," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 12, pp. 3564-3575, Dec. 2020.

[208] M. Nakkar, R. Altawy, and A. Youssef, "Lightweight Broadcast Authentication Protocol for Edge-Based Applications," in IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11766-11777, Dec. 2020.

[209] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar, and S. Kumari, "Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment," in IEEE Consumer Electronics Magazine, 2021 (Early Access).

[210] M. Casagrande, M. Conti, and E. Losiouk, "Contact Tracing Made Un-relayable," Nov. 2020, available at: `arXiv:2010.12641v2`.

[211] Y-H Chuang, N-W Lo, C-Y Yang, and S-W Tang, "A Lightweight Continuous Authentication Protocol for the Internet of Things," in Sensors, 18(4):1104, 2018.

[212] A. V. Mota, S. Azam, B. Shanmugam, K. C. Yeo, and K. Kannoorpatti, "Comparative analysis of different techniques of encryption for secured data transmission," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017.

Personal Publications

1. S. Pizzi, C. Suraci, L. Militano, A. Orsino, A. Molinaro, A. Iera, and G. Araniti, "Enabling Trustworthy Multicast Wireless Services through D2D Communications in 5G Networks," Future Internet 2018, vol. 10, no. 66.

2. C. Suraci, S. Pizzi, A. Iera and G. Araniti, "Enhance the protection of transmitted data in 5G D2D communications through the Social Internet of Things," 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Bologna, 2018, pp. 376-380.

3. C. Suraci, S. Pizzi, A. Iera, A. Molinaro, and G. Araniti, "Delivering Multicast Content Through Secure D2D Communications in the Internet of Things," in: Di Felice M., Natalizio E., Bruno R., Kassler A. (eds) Wired/Wireless Internet Communications. WWIC 2019. Lecture Notes in Computer Science, vol. 11618. Springer.

4. O. Vikhrova, C. Suraci, A. Tropeano, S. Pizzi, K. Samouylov and G. Araniti, "Enhanced Radio Access Procedure in Sliced 5G Networks," 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 2019, pp. 1- 6.

5. S. Pizzi, C. Suraci, A. Iera, A. Molinaro and G. Araniti, "A Sidelink-Aided Approach for Secure Multicast Service Delivery: From Human-Oriented Multimedia Traffic to Machine Type Communications," in IEEE Transactions on Broadcasting, vol. 67, no. 1, pp. 313-323, March 2021.

6. C. Suraci, S. Pizzi, A. Molinaro, A. Iera, and G. Araniti, "An RSA-based Algorithm for Secure D2D- aided Multicast Delivery of Multimedia Services," 2020 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2020, pp. 1-6.

7. C. Suraci, G. Araniti, A. Abrardo, G. Bianchi, and A. Iera, "A Stakeholder-Oriented Security Analysis in Virtualized 5G Cellular Networks," Computer Networks, vol. 184, 2021.

8. C. Suraci, S. Pizzi, D. Garompolo, G. Araniti, A. Molinaro, and A. Iera, "Trusted and Secured D2D- Aided Communications in 5G Networks," Ad Hoc Networks, vol. 114, 2021.

9. F. Rinaldi, C. Suraci, S. Pizzi, A. Molinaro, and G. Araniti, "Secure eMBB service delivery over 5G NR Non-Terrestrial Networks," 72nd International Astronautical Congress (IAC), Dubai, United Arab Emirates, 25-29 October 2021.

10. C. Suraci, S. Pizzi, F. Montori, M. Di Felice, and G. Araniti, "6G to Take the Digital Divide by Storm: Key Technologies for the Widespread Provision of IoT Services," under review.

11. C. Suraci, S. Pizzi, A. Molinaro, and G. Araniti, "MEC and D2D as Enabling Technologies for a Secure and Lightweight 6G eHealth System," in IEEE Internet of Things Journal, Early Access.