future internet

Article

Enabling Trustworthy Multicast Wireless Services through D2D Communications in 5G Networks

Sara Pizzi [1], Chiara Suraci [1], Leonardo Militano [1], Antonino Orsino [2], Antonella Molinaro [1], Antonio Iera [1] and Giuseppe Araniti [1,*]

[1] DIIES, University "Mediterranea" of Reggio Calabria, Via Graziella, Loc. Feo di Vito, 89100 Reggio Calabria, Italy; sara.pizzi@unirc.it (S.P.); chiarasur@outlook.it (C.S.); leonardo.militano@unirc.it (L.M.); antmolin@unirc.it (A.M.); antonio.iera@unirc.it (A.I.)

[2] Ericsson Research, Hirsalantie 11, 02420 Jorvas, Finland; antonino.orsino@ericsson.com

* Correspondence: araniti@unirc.it; Tel.: +39-0965-1693420

Received: 9 June 2018; Accepted: 9 July 2018; Published: 11 July 2018

Abstract: Device-to-device (D2D) communication is considered as one of the key enabling technologies for fifth-generation (5G) networks as it allows data offloading 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 the 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 systems, 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 network, this work proposes 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 of the establishment of secure D2D communications and efficiently utilize network resources.

Keywords: device-to-device (D2D) communication; 5G networks; security; multicasting

1. Introduction

Future fifth-generation (5G) networks are expected 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 are expected to play a key role in helping to satisfy the demanding requirements of the foreseen use cases. Device-to-device (D2D) communications and multicasting are certainly among these. The former, because of its capability to offload cellular data traffic, enhances spectrum efficiency and extends cell coverage [1]. 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 [2]).

Regarding 5G in general, in the 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, cMTC, V2X or 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 that nowadays are very close (if not the same) to those of the future 5G systems.

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 multicast and broadcast services over cellular networks, the 3rd Generation Partnership Project (3GPP) has standardized the evolved Multimedia Broadcast Multicast Service (eMBMS) [3]. Although it represents the current standard to support group-oriented services over mobile networks, significant work must be done in order to effectively support multicast/broadcast traffic in 5G networks. The approach for delivering multicast traffic in cellular networks, the so-called Conventional Multicast Scheme (CMS) [4], 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 guaranteeing 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 our earlier work in [5], we proposed a D2D-aided radio resource management policy for eMBMS, called 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. 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 [6]. 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 [7].

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 [8,9], wherein a comparison of the different approaches is also 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 [10] is identified as the more effective, since it is able to satisfy most of the security requirements posed by future 5G networks [8,9].

The purpose of this work is to present 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 [5], D2D clusters are formed in order to forward data towards users with the worst channel conditions, which are excluded from a first multicast transmission by the eNodeB (eNB). In this paper, we enhance the work in [5] by selecting the relay node (i.e., the 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, our proposed scheme can be seen as a clear security enhancement with respect to [5] in that it takes into account, in the D2D communications' procedure, security aspects previously not considered at all. In particular, security procedures inspired from [10] are implemented in order to guarantee confidentiality and integrity of data transmitted in D2D communications, and D2D users' privacy protection. Security mechanisms as encryption, keyed-hash 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 eNodeB, 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 reduces the reliability of the node and, consequently, the probability of being selected as data forwarder.

The remainder of the paper is organized as follows. Sections 2 and 3 present, respectively, the related works in this field and the basics of the proposed eCMS-sD2D. Section 4 describes the designed algorithm in details. Results from our simulative analysis are shown in Section 5. Conclusive remarks are given in the last section.

2. Related Work

In the literature, many works deal with the candidate supporting technologies for enabling future 5G networks [11,12]. 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 [13] 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 an 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 [14] or in closely related fields [15].

An interesting usage scenario for the D2D technology is multicasting. Multicast and broadcast services are enabled in 3GPP Release 8 networks through the evolved Multimedia Broadcast Multicast Service (eMBMS) architecture. According to [16], the group-oriented services will be protagonists in 5G networks, and multicasting will be the effective means to offer these services. Establishing direct communications between devices in proximity has been shown to improve the multicasting performance. In [5], the D2D-enhanced CMS with Single Frequency (D2D-SF) approach was designed to improve the performance of the Conventional Multicast Scheme (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 multicasting technologies can be found in [17]. 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 relationships. Another work that addresses a similar topic is presented in [18]. Here, the authors considered 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 [19], 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 [20], 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 that represents an important aspect for future 5G networks; this is the focus of this paper. According to [21], privacy and security issues must be faced in order to definitely make D2D a successful technology. In [8], 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 [10] 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 Diffie–Hellman key exchange protocol. The strength of this strategy lies in the intervention of the eNodeB that represents a trusted third party and protects against malicious behaviors such as the man-in-the-middle attack. In [9], security solutions proposed improving D2D in 5G networks are analyzed. In addition to reporting D2D security requirements, threats and solutions, this work hints at 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 this work, we aim to add the security dimension to the D2D-SF solution we proposed in [5] in order to make it suitable to 5G networks and cope with typical D2D vulnerability attacks.

3. Background

LTE-A is the solution proposed by 3GPP to bring broadband on mobile radio systems [22]. 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, resource blocks are either 12 × 15 kHz subcarriers or 24 × 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 eNodeB 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) that the user can support. The CQI to MCS mapping foreseen in LTE-A networks is reported in Table 1 [5].

The eMBMS architecture, depicted in Figure 1, has been standardized to support multicast and broadcast services over LTE-A networks [3]. As explained in [16], the eMBMS architecture defines nodes belonging both to the radio access network (E-UTRAN) and to the evolved packet core (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, and the latter has to manage the coordination of the various eNBs. It allocates resources to each eNB and coordinates admission control and reporting necessary to the MBMS session. The EPC is composed of the broadcast multicast-service center (BM-SC) and the MBMS-gateway (MBMS-GW). The first is responsible for the initialization of the 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 future 5G networks.

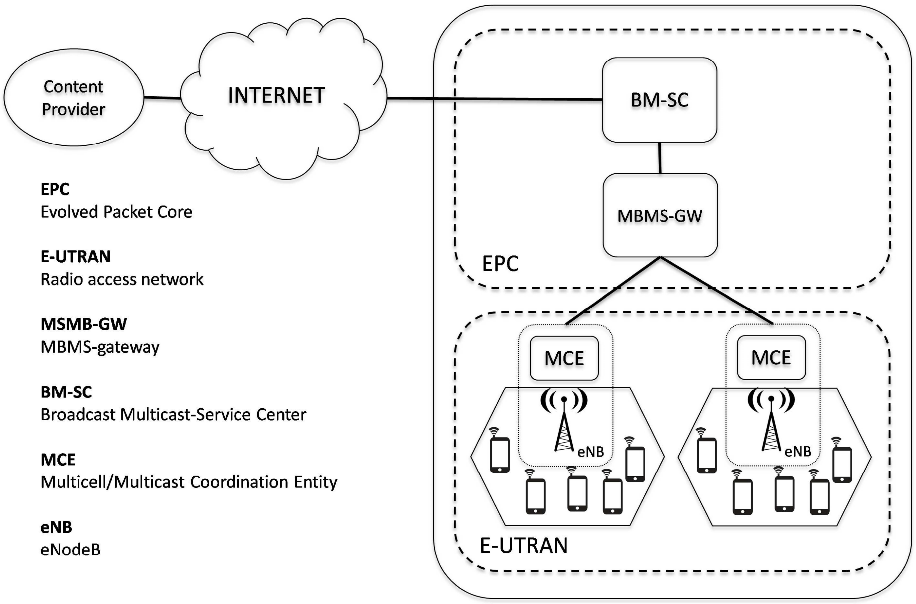

Figure 1. eMBMS architecture.

Table 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

In order to efficiently manage the multicast and broadcast services over the forthcoming 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 [4] has been traditionally utilized for delivering multicast content because of its native short-term fairness capability. The possibility to improve the performance of CMS by exploiting D2D communication has been proposed in [5]. However, since D2D communications are managed directly by the users, serious security problems arise.

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 [23], they proposed a public key distribution system suited to the scenario of two peers that 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:

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

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:

$$X = \log_\alpha Y \bmod q, \qquad \text{for } 1 \leq Y \leq q-1. \tag{2}$$

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:

$$Y_i = \alpha^{X_i} \bmod q. \tag{3}$$

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

$$K_{ij} = \alpha^{X_i X_j} \bmod q. \tag{4}$$

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

$$K_{ij} = Y_j^{Xi} \bmod q = (\alpha^{X_j})^{Xi} \bmod q = \alpha^{X_i X_j} \bmod q. \tag{5}$$

Similarly, user j obtains K_{ij} as:

$$K_{ij} = Y_i^{X_j} \bmod q. \tag{6}$$

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 [23]. 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.

4. The Proposed eCMS-sD2D Protocol

The reference scenario of this work is composed of 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 of all the nodes foreseen in the eMBMS standard architecture, but procedures must be improved to make multicast transmission more suitable for future 5G networks. Our proposed solution called enhanced CMS with secure D2D communications (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 2.

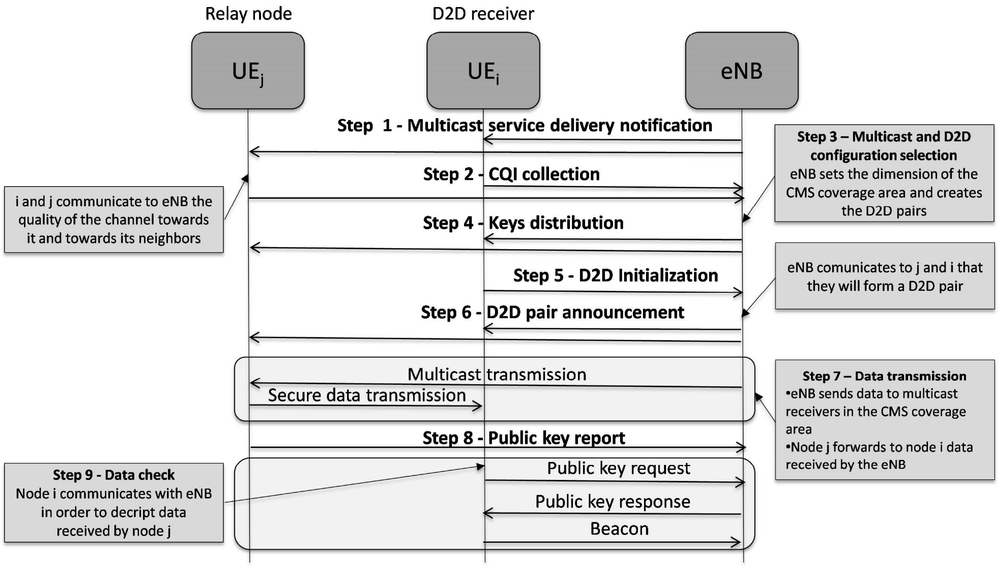
Relay node
D2D receiver
UE$_j$
UE$_i$
eNB
Step 1 - Multicast service delivery notification
Step 2 - CQI collection
Step 4 - Keys distribution
Step 5 - D2D Initialization
Step 6 - D2D pair announcement
Multicast transmission
Secure data transmission
Step 8 - Public key report
Public key request
Public key response
Beacon
i and j communicate to eNB the quality of the channel towards it and towards its neighbors
Step 3 – Multicast and D2D configuration selection
eNB sets the dimension of the CMS coverage area and creates the D2D pairs
eNB comunicates to j and i that they will form a D2D pair
Step 7 – Data transmission
•eNB sends data to multicast receivers in the CMS coverage area
•Node j forwards to node i data received by the eNB
Step 9 - Data check
Node i communicates with eNB in order to decript data received by node j

Figure 2. eCMS-sD2D procedures.

Our proposal is tailored to cellular 5G networks where the eNodeB acts as a central coordinator of both D2D and traditional communications. In fact, we focus on network-assisted D2D communications in a licensed spectrum, which is the preferred solution because of the expected gains it offers [1]. In such a scenario, it is a natural choice to also make the eNodeB work a trusted third party for the implementation of the security mechanisms. Differently, in a distributed scenario (that is not the case analyzed in this paper and that is not the preferred option for D2D communications), the selection of the node that will act as a trusted third party is a tricky choice that needs to be carefully investigated.

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 UE to serve through the multicast transmission; (ii) the MCS to use for the multicast transmission in the CMS coverage area; (iii) the users served in a multicast that 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 sD2D-eCMS approach foresees the formation of some D2D clusters. The cluster formation and resource allocation are important factors for the D2D-based multicast performance. This is true in general and not only for the eCMS-sD2D solution specifically presented in the current paper. However, in our previous research on the topic, we have investigated these aspects in detail. Since in this paper these aspects are not in focus, we rely on the results of our previous research. In particular, for the eCMS-sD2D proposal, we implement the best performing solution obtained in Reference [5]. The resulting configuration of each cluster is a cluster composed of 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 by means of 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 UE that can decode data transmitted with the correspondent MCS and the subset of UE, which, on the contrary, are in the worst channel conditions and must be served through D2D communications. Among all the eligible configurations (i.e., those in which all UE, 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 [5] 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 [10].

Step 4—Keys distribution

In order to protect privacy of registered UE, the eNB computes a pseudo-identity (PID) for each of them. For each UE_k that registered with the network using its real ID (RID_k), the eNB computes a pseudo-identity 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:

$$PID_i||P_i||z||h[(x_i^+ \oplus \text{opad})||h[(x_i^+ \oplus \text{ipad})||PID_i||P_i||z]], \tag{7}$$

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 (7), x_i^+ is the key padded out to size, *opad* and *ipad* are specified padding constants. In the remainder of the paper, $h[(k^+ \oplus \text{opad})||h[(k^+ \oplus \text{ipad})||m]]$ 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 the positive case, the eNB has to inform both D2D devices involved in the direct communication of their imminent communication. Thus, 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, which has been chosen as RN of the D2D communication, the eNB sends to it the following message:

$$PID_j||PID_i||z||u||P_i||h(\bullet, x_j). \tag{8}$$

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:

$$PID_i||PID_j||X_j||P_i||h(\bullet, x_i). \tag{9}$$

Step 7—Data transmission

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

$$\sigma_1 = H_1(P_i||M)^{x_0}, \tag{10}$$

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

$$\sigma_2 = H_1(PID_j||P_i||M'||T_s||\sigma_1)^{x_j}, \tag{11}$$

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:

$$PID_i||PID_j||P_i||M'||T_s||\sigma_1||\sigma_2. \tag{12}$$

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. Thus, it sends to the eNB a report:

$$PID_i||PID_j||P_i||Enc_{k_s}(y)||v||T_s||h(\bullet, x_j). \tag{13}$$

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. Thus, it checks the signature of the transmitter 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:

$$PID_i||PID_j||P_i||T_s||h(\bullet, x_i). \tag{14}$$

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:

$$PID_i||PID_j||P_i||y||T_s||T_i||h(\bullet, x_i), \tag{15}$$

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 sD2D-eCMS, 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 $k_c = y^c = g^{bc}$. Thus, 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:

$$\beta = PID_i||PID_j||P_i||M'||T_s||\sigma_1||\sigma_2||h(\bullet, x_i). \tag{16}$$

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 (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. Thus, 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 that does not transmit data correctly in the D2D communication. Thus, in the case of malicious behavior of UE_j, the eNB increments by one its MBA counter. When a user's counter exceeds a given threshold, called the 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:

$$MBA_k \leq THRESHOLD. \tag{17}$$

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 D2D communication. When it is set to zero, only users with an 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 malicious behavior in the past. As the value of the threshold increases, the algorithm is always less selective; this means that more users that, in the past, have already behaved maliciously can be chosen as RN.

We highlight that the MBA counter is incremented only in the case that a certain malicious behavior is detected (i.e., in case the eNodeB receives a beacon message from a D2D receiver UE_i alerting a malicious behavior from RN UE_j and the eNodeB verifies that UE_j has actually served as a data transmitter). Thus, an increment in the MBA counter can not be due to misdetection of a malicious behavior. Thus, for low values of the maliciousness threshold, the goodput increase is not at the expense of maliciousness misdetection. Setting the maliciousness threshold to a value higher than zero (i.e., choosing a not too selective approach in the relay election procedure) could be useful in case a node turns its malicious nature to non-malicious. In fact, in case a node stops exhibiting a malicious behavior, it will no longer be selected anyway as a relay node in case the maliciousness threshold with a goodput increase that can be relevant in case the node is in good channel conditions and can serve as relay for a high number of neighbors.

5. Performance Evaluation

A simulative analysis in MATLAB (MathWorks, Natick, MA, USA) 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 dimensions 100 m × 100 m, 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 for sending 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 an 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 Aggregate Data Rate (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, we will compare our proposed eCMS-sD2D with respect to the existing protocol presented in [5], in which the security of D2D communications is not guaranteed. Under eCMS-sD2D, we analyze its performance with three different values of the maliciousness threshold (equal to 0, 40, and 80). We assign to each node a nature (malicious or non-malicious) and we assume that it does not change over time. Thus, our analysis can be seen as a sort of worst case analysis.

The results in terms of mean throughput and goodput are presented in Figure 3a,b, respectively, under increasing percentage of malicious UE. By looking at Figure 3a, we can notice that curves are almost overlapping because throughput does not depend on security. In fact, D2D-SF and our proposed eCMS-sD2D achieved really similar throughput values and the experimented data rate is independent from the percentage of malicious users. Differently, the results in terms of goodput depicted in Figure 3b 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 nodes that behaved maliciously just once are also not selected as RN.

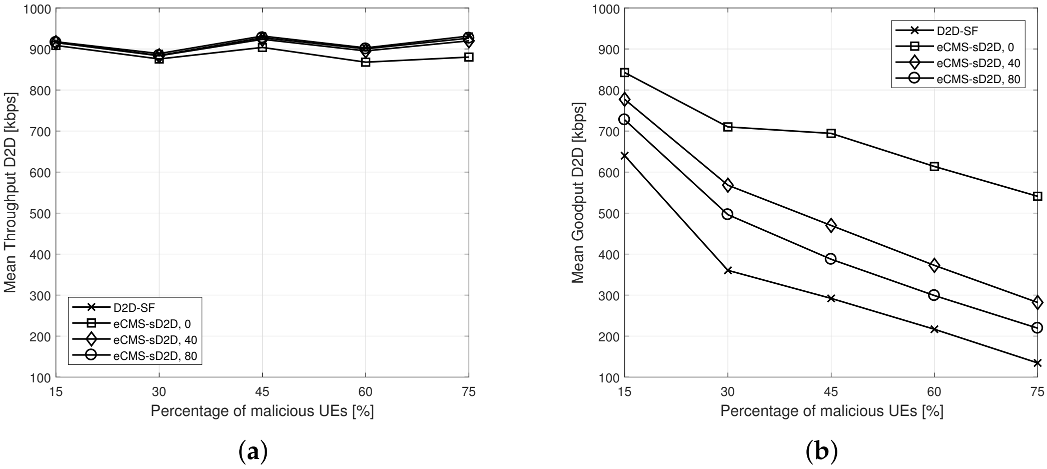

Figure 3. Mean (**a**) throughput D2D and (**b**) goodput D2D for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, under increasing percentage of malicious nodes.

A similar reasoning holds for the ADR metric. In fact, we can appreciate in Figure 4 that, 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, we highlight that the increment of the maliciousness threshold causes a performance degradation since security mechanisms are less stringent.

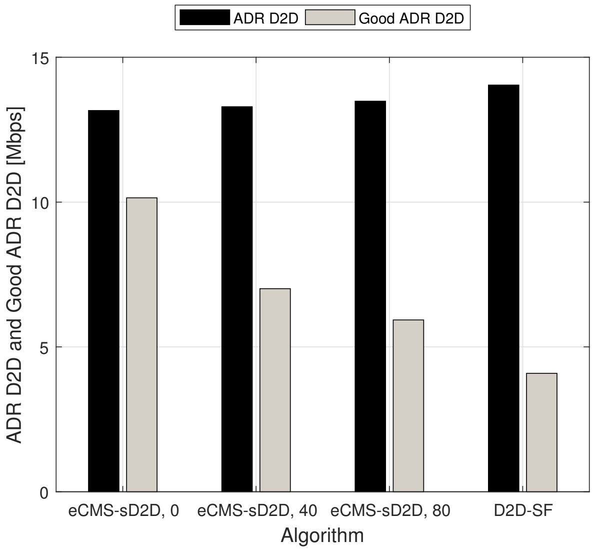

Figure 4. Comparison between ADR D2D and Good ADR D2D for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, with 75% of malicious nodes.

This significant degradation of the goodput/good ADR is due to the high amount of data loss, as confirmed by Figure 5. Thanks to the implementation of the security mechanisms foreseen in eCMS-sD2D, data loss can be reduced by 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 that malicious RN can be identified only after the eNodeB 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.

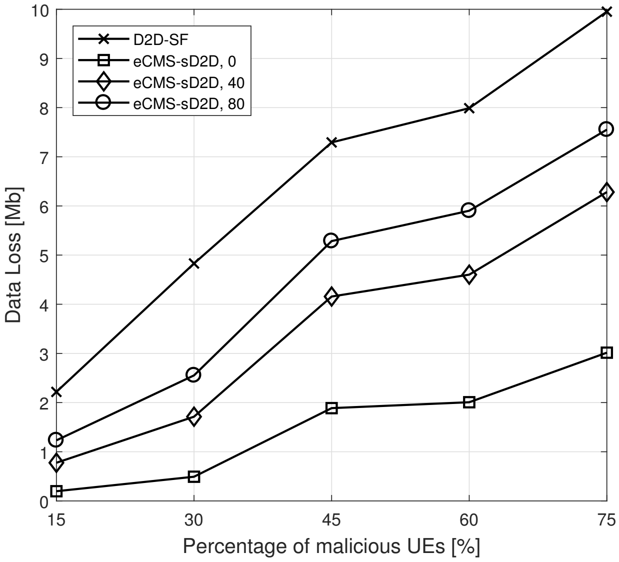

Figure 5. Data loss for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, under increasing percentage of malicious nodes.

Because of security, as shown in Figure 6, the mean number of malicious D2D UE that gains service is reduced (see the first bar with respect to the fourth bar). However, despite this metric showing 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 eCMS-D2D is limited. Going more in depth in the analysis, we show in Figure 7 the mean number of selected malicious RNs under increasing percentage of malicious users. We can appreciate that 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).

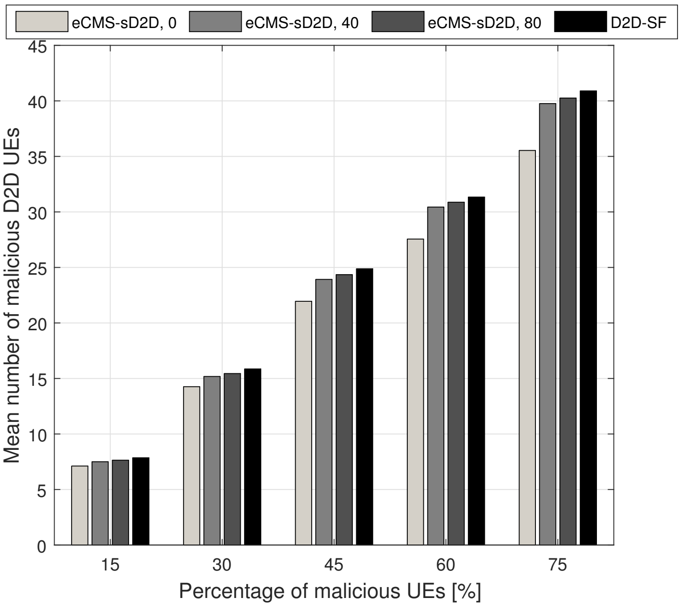

Figure 6. Mean number of malicious D2D nodes for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, under increasing percentage of malicious nodes.

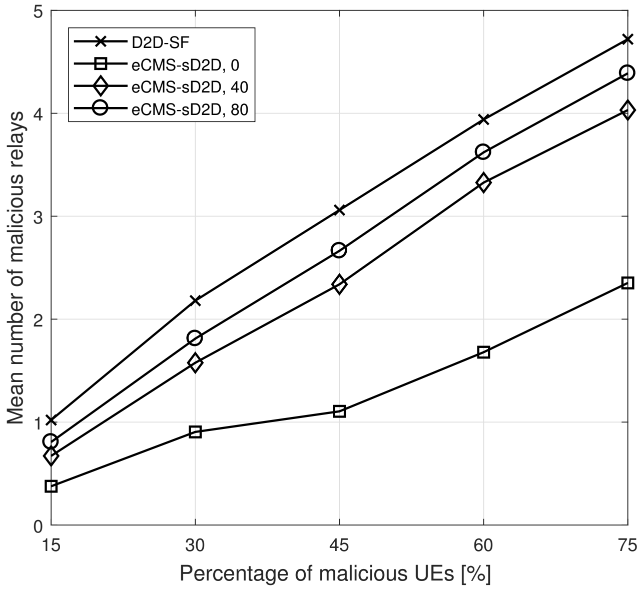

Figure 7. Mean number of malicious relays for eCMS-sD2D, with three different settings of the maliciousness threshold, and D2D-SF, under increasing percentage of malicious nodes.

6. Conclusions

In this paper, we have proposed a protocol, called eCMS-SD2D (enhanced CMS with secure D2D communications), to perform a secure transmission of a multicast service while also efficiently utilizing network resources of the forthcoming 5G network. In doing this, we use mechanisms as signature and encryption in order to increase the data protection and the privacy when nearby devices aim at transmitting each other through proximity-based links (e.g., D2D). The outcome of our 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, a reasonable data-rate to the users within the multicast group during a radio transmission.

Author Contributions: Conceptualization, S.P., C.S. and G.A.; Investigation, S.P. and C.S.; Software, C.S.; Validation, S.P. and G.A.; Writing—original draft, S.P. and C.S.; Writing—review & editing, G.A., L.M., A.O., A.M. and A.I.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fodor, G.; Dahlman, E.; Mildh, G.; Parkvall, S.; Reider, N.; Miklós, G.; Turányi, Z. Design aspects of network assisted device-to-device communications. *IEEE Commun. Mag.* **2012**, *50*, 170–177. [CrossRef]
2. CISCO. Cisco Visual Networking Index: Forecast and Methodology, 2016–2021. Available online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html (accessed on 9 July 2018).
3. 3GPP. Evolved Universal Terrestrial Radio Access Network (E-UTRAN); General Aspects and Principles for Interfaces Supporting Multimedia Broadcast Multicast Service (MBMS) within E-UTRAN. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2455 (accessed on 9 July 2018).
4. Liu, J.; Chen, W.; Cao, Z.; Letaief, K. Dynamic power and sub- carrier allocation for OFDMA-based wireless multicast systems. In Proceedings of the 2008 IEEE International Conference on Communications (ICC), Beijing, China, 19–23 May 2008.

5. Militano, L.; Condoluci, M.; Araniti, G.; Molinaro, A.; Iera, A.; Muntean, G.-M. Single Frequency-Based Device-to-Device-Enhanced Video Delivery for Evolved Multimedia Broadcast and Multicast Services. *IEEE Trans. Broadcast.* **2015**, *61*, 263–278. [CrossRef]
6. ERICSSON. 5G Security—Enabling a Trustworthy 5G System. AVailable online: https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system (accessed on 9 July 2018).
7. Gandotra, P.; Jha, R.K.; Jain, S. A survey on device-to-device (D2D) communication: Architecture and security issues. *J. Netw. Comput. Appl.* **2017**, *78*, 9–29. [CrossRef]
8. Haus, M.; Waqas, M.; Ding, A.Y.; Li, Y.; Tarkoma, S.; Ott, J. Security and Privacy in Device-to-Device (D2D) Communication: A Review. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1054–1079. [CrossRef]
9. Wang, M.; Yan, Z. A Survey on Security in D2D Communications. *Mob. Netw. Appl.* **2017**, *22*, 195–208. [CrossRef]
10. Zhang, A.; Chen, J.; Hu, R.Q.; Qian, Y. SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 2659–2672. [CrossRef]
11. GSMA Intelligence. Understanding 5G: Perspectives on Future Technological Advancements in Mobile. Available online: https://www.gsmaintelligence.com/research/?file=141208-5g.pdf&download (accessed on 9 July 2018).
12. Akyildiz, I.F.; Nie, S.; Lin, S.C.; Chandrasekaran, M. 5G roadmap: 10 key enabling technologies. *Comput. Netw.* **2016**, *106*, 17–48. [CrossRef]
13. Asadi, A.; Wang, Q.; Mancuso, V. A Survey on Device-to-Device Communications in Cellular Networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1801–1819. [CrossRef]
14. Boabang, F.; Nguyen, H.-H.; Pham, Q.-V.; Hwang, W.-J. Network-assisted Distributed Fairness-aware Interference Coordination for Device to Device Communication Underlaid Cellular networks. *Mob. Inf. Syst.* **2017**, *2017*, 1821084. [CrossRef]
15. Pham, Q.-V.; To, H.L.; Hwang, W.-J. A Multi-Timescale Cross-Layer Approach for Wireless Ad Hoc Networks. *Comput. Netw.* **2015**, *18*, 471–482. [CrossRef]
16. Araniti, G.; Condoluci, M.; Scopelliti, P.; Molinaro, A.; Iera, A. Multicasting over Emerging 5G Networks: Challenges and Perspectives. *IEEE Netw.* **2017**, *31*, 80–89. [CrossRef]
17. Feng, L.; Zhao, P.; Zhou, F.; Yin, M.; Yu, P.; Li, W.; Qiu, X. Resource Allocation for 5G D2D Multicast Content Sharing in Social-Aware Cellular Networks. *IEEE Commun. Mag.* **2018**, *56*, 112–118. [CrossRef]
18. Bhat, J.R.; Sheu, J.P.; Hon, W.K. Resource Allocation Schemes for Revenue Maximization in Multicast D2D Networks. *IEEE Access* **2017**, *5*, 26340–26353. [CrossRef]
19. Antonopoulos, A.; Kartsakli, E.; Verikoukis, C. Game theoretic D2D content dissemination in 4G cellular networks. *IEEE Commun. Mag.* **2014**, *52*, 125–132. [CrossRef]
20. Datsika, E.; Antonopoulos, A.; Zorba, N.; Verikoukis, C. Cross-Network Performance Analysis of Network Coding Aided Cooperative Outband D2D Communications. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3176–3188. [CrossRef]
21. Militano, L.; Araniti, G.; Condoluci, M.; Farris, I.; Iera, A. Device-to-Device Communications for 5G Internet of Things. *EAI Endorsed Trans. Internet Things* **2015**, *1*, e4. [CrossRef]
22. 3GPP. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN). Available online: https://www.etsi.org/deliver/etsi_ts/136300_136399/136300/11.05.00_60/ts_136300v110500p.pdf (accessed on 9 July 2018).
23. Diffie, W.; Hellman, M.E. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]