A Sidelink-Aided Approach for Secure Multicast Service Delivery: from Human-Oriented Multimedia Traffic to Machine Type Communications

A Sidelink-Aided Approach for Secure Multicast Service Delivery: From Human-Oriented Multimedia Traffic to Machine Type Communications

Sara Pizzi, Chiara Suraci, Antonio Iera, Antonella Molinaro, and Giuseppe Araniti

This is the post-print of the following article: 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, doi: 10.1109/TBC.2020.2977512. Article has been published in final form at: https://ieeexplore.ieee.org/document/9036866

***Abstract*—To date, group-oriented communications have been mainly exploited for delivering multimedia services in human-oriented communications while, in future fifth generation (5G) cellular networks, objects will be the main target. Internet of Things (IoT) will undoubtedly play a key role in 5G networks, wherein massive machine-type communications (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 device-to-device (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 work 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.**

***Index Terms*—5G, IoT, mMTC, group-oriented communications, NB-IoT, D2D, security, social trustworthiness.**

I. Introduction

FIFTH generation (5G) cellular systems will be 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 3rd Generation Partnership Project (3GPP) has specified a 5G system architecture aimed to support a wide set of use cases, typically grouped into three classes: enhanced mobile broadband (eMBB), ultra reliable and low latency communications (URLLC), and massive machine-type communications (mMTC) [1]. Focus of this work 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 Internet of Things (IoT) is expected to reach 4 billions by 2024 [2]. 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 Narrowband-IoT (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 will be 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 (IoMT), an innovative concept according to which heterogeneous multimedia things can interact and cooperate to achieve multimedia-based applications/services [3]. In fact, as also stated in [4], the target of multimedia services is shifting from traditional TV to streaming on connected devices, such as mobile devices and monitoring devices. Very recently, the feasibility of delivering less-demanding multimedia IoT applications over NB-IoT has been investigated in [5].

Actually, multicast transmissions could allow to largely weigh down latency and energy consumption of the receiving

Manuscript received October 26, 2019; revised January 20, 2020; accepted January 25, 2020. *(Corresponding author: Giuseppe Araniti.)*

Sara Pizzi, Chiara Suraci, Antonella Molinaro, and Giuseppe Araniti are with the CNIT/DIIES Department, University Mediterranea of Reggio Calabria, 89124 Reggio Calabria, Italy (e-mail: sara.pizzi@unirc.it; chiara.suraci@unirc.it; antonella.molinaro@unirc.it; araniti@unirc.it).

Antonio Iera is with the CNIT/DIMES Department, University of Calabria, 87036 Rende, Italy (e-mail: antonio.iera@dimes.unical.it).

Digital Object Identifier 10.1109/TBC.2020.2977512

IoT devices. The traditional way of serving multicast traffic is the Conventional Multicast Scheme (CMS), which assigns the group data rate based on the device that experiences the worst channel conditions. As stated in [6], 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 quality of experience (QoE), which is the quality focus of 5G networks [7]. 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 [8] 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 future 5G networks, device-to-device (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 [9]. As in [10], 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 expected for the next 5G mobile networks, mainly due to the fact that many actors will be involved in the provision of services, therefore, sensitive data will be exposed to different parties, some of which may not be trusted. Moreover, softwarization will be a key technique in the development of the 5G, hence, technologies such as Multi-Access Edge Computing (MEC), Network Function Virtualization (NFV) and Software-Defined Networking (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. Side-channel attacks, data breaches, distributed denial of service (DDoS) attacks, insecure interfaces and application programming interfaces (APIs), isolation failure, and malicious insiders are some of the most frequent attacks which focus on the vulnerabilities of 5G virtualization technologies. Many works in the literature deal with these problems and potential solutions [11], [12], [13].

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 our previous work [14], where we defined a protocol intended to secure D2D communications, in which D2D peers generate a private encryption key by using a trusted version of the Diffie-Hellman Key Exchange (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 work proposes the *Machine type Multicast Service 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 [15] *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 work are the following:

- the architecture presented in [8] 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 [14] 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 paper is organized as follows. In Section II, the research background is presented. Section III illustrates the scenario under investigation, while Section IV describes in details all MtMS-stD2D procedures. Obtained results are shown in Section V, while conclusive remarks are given in the last section.

II. Background

In this section, we will provide the basics of NB-IoT, the cellular technology which is the reference of our work. Then, we will discuss how multicast transmissions are managed in NB-IoT. Afterwards, research works related to security are surveyed.

A. The Narrowband-Internet of Things (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. In fact, it can extend device battery lifetime by up to 10 years, improve coverage by 20 dBm compared to Long Term Evolution (LTE), and manage the massive capacity of IoT scenarios [16].

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 GSM (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 radio access network 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 Orthogonal Frequency-Division Multiple Access (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 Single Carrier Frequency Division Multiple Access (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 [17].

B. Multicast Support in NB-IoT

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

The main nodes of the MBMS architecture are: the *broadcast multicast-service center (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-gateway (MBMS-GW)*, which is in charge of forwarding MBMS packets to the base station (BS) involved in service delivery; the *multicell/multicast coordination entity (MCE)*, which has to manage admission control and radio resource allocation to the BS [18].

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 [19], 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 [20].

C. Securing Communications

In [1], 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 [21]. Many works in the literature deal with the security problem in the next generation mobile networks, the most significant of which are collected in [22]. 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 control, authentication, communication, and encryption areas, the same targeted by the protocol proposed in this paper.

In the 5G network, D2D communications are a widely accepted technology for enhancing spectrum efficiency, improving network resource utilization, and extending battery lifetime [9]. However, as also stated in [24], 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 misbehavior.

Among proposals for securing D2D communication, an interesting solution is presented in [25]. This is the work that inspires the protocol presented in [14], 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:

$$K_{ij} = Y_j^{Xi} \bmod q = \left(\alpha^{X_j}\right)^{X_i} \bmod q = \alpha^{X_i X_j} \bmod q \qquad (1)$$

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:

$$K_{ij} = Y_i^{X_j} \bmod q = \left(\alpha^{X_i}\right)^{X_j} \bmod q = \alpha^{X_i X_j} \bmod q \qquad (2)$$

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 paper. In fact, many research works assume the intervention of a trusted third party in the key generation mechanism between resource-constrained devices [26] or of a centralized security framework to detect incoming attacks [27]. In [28], 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 eNodeB (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 [29] and [30] 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 [14] have been illustrated in order to legitimize whether this algorithm is partly used also in the protocol presented in this work. In fact, similarly to [14], we exploit 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 our 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 [14], 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 [14], this work 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.

III. System Model

This work considers an IoT scenario, wherein the MTC multicast traffic is managed through the proposed algorithm, named *MtMS with secure and trust D2D (MtMS-stD2D)*. D2D communications are established between devices directly served by the BS and those 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 Social IoT (SIoT) paradigm [31]. Social relationships that can be established among nodes are: parental object relationship (POR), among objects created by the same producer in the same period; co-location object relationship (C-LOR), that affects smart things that always work in the same place; co-work object relationship (C-WOR), between objects that collaborate to achieve a common goal; ownership object relationship (OOR), that binds objects owned by the same holder; social object relationship (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 [32]. 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 [33]. For this reason, we consider a femtocell, 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 we want 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 we want to utilize a low-power technology for reducing energy consumption of the devices, even if we must obviate to the lack of support of D2D communication in NB-IoT. Thus, we assume that 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.

Our MtMS-stD2D architecture, depicted in Fig. 1, derives from the MtMS architecture (defined in [8]) and properly enhances it to support secure D2D communications. It is composed of the following nodes: the *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.

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 we are considering femtocells. In addition, not all devices in the cell must implement the security protocol. In fact, only D2D communications, that 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, we put a keen attention to the overhead introduced by the proposed security mechanism, which is then evaluated through an energy consumption analysis.

IV. Machine-Type Multicast Service With Secure and Trust D2D

In our 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 paper focuses on procedures for *efficient* and *secure* DL service delivery.

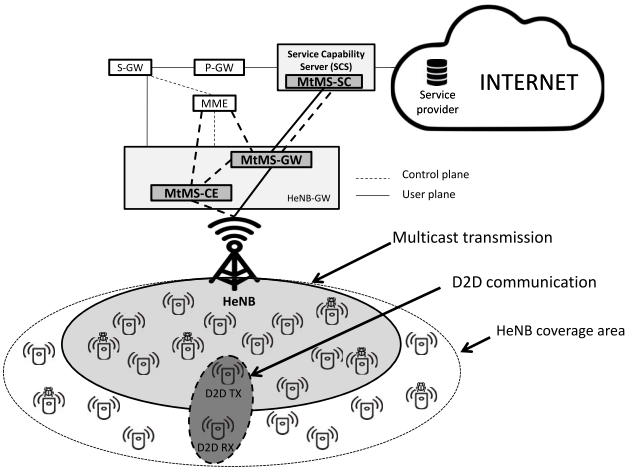

Fig. 1. Reference architecture.

TABLE I
Procedures and Sub-Procedures

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	

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

A. 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.

B. 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.

C. Joining

1) 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.

2) 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., channel quality indicator (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.

3) D2D Pairs Selection: This phase represents the heart of our proposal, 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 [34], 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:

$$NRV_k^t = \begin{cases} SRF_k^t, & MDC_k^{t-1} = 0 \\ MDC_k^{t-1}, & MDC_k^{t-1} \neq 0 \end{cases} \quad (3)$$

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 [35], a value $\in [0, 1]$ is assigned to each type of the five social relationships discussed in Section III. 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.

4) 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 [25]. 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.

5) 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.

D. Data Transfer

1) 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.

2) 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.

3) 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.

4) 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.

5) 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 IV-C3.

E. Session Stop

The MtMS session is completed when data are sent to all devices initially subscribed by the service provider.

V. Performance Evaluation

A. 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 [36]. Our work aims at optimizing the encryption key generation procedures also making them eavesdroppers proof. Hence, we first list the security requirements for reliable D2D communications and, then, we highlight which of these requirements are met by our MtMS-stD2D protocol.

- *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 identifying credentials with the entity that owns them.
- *Privacy.* The protection of information relating to network users concerns the privacy assurance. In the age of General Data Protection Regulation (GDPR), this is a fundamental requirement in some 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 our 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 implementation, *non-repudiation* is accomplished. This is particularly important in the sD2D communication step (see Section IV-D2), 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 our 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.

B. Simulation Results

We tested the performance of the proposed protocol 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 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 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 [25]. Finally, for purely simulation purposes, we consider the almost ideal situation in which devices send to the HeNB accurate values of trustworthiness, computed as in [37]. In particular, values in the range [0,0.4] and [0,1] are respectively assigned to malicious and non-malicious nodes. The ultimate goal is 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 resources wastage of the devices.

In Fig. 2 and 3 we compare three possible implementations of the D2D communication: 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. We set the dimension of the file to download to 500 kb.

Fig. 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. Fig. 3 confirms this claim. In fact, it shows that the proposed protocol allows to download practically the whole file of dimension 500 kb even with 60% of malicious devices. This happens

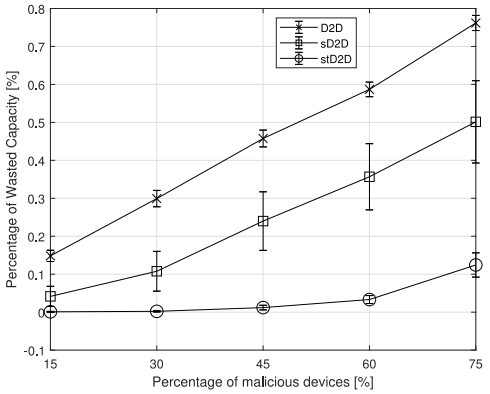

Fig. 2. % of wasted capacity vs. % of malicious devices.

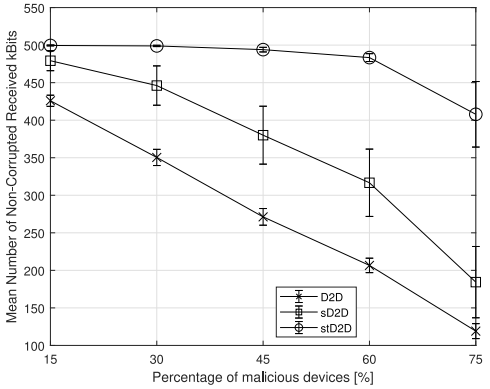

Fig. 3. Amount of data correctly transmitted in D2D (i.e., by non-malicious relays) vs. % of malicious devices.

because almost only non-malicious relays are selected as forwarding nodes towards D2D receivers.

Fig. 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 [38]. 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:

$$E_{\text{wasted, D2D}} = \frac{E_{\text{malicious}}}{E_{\text{total}}}. \tag{4}$$

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

$$E_{\text{wasted, stD2D}} = \frac{E_{\text{malicious}} + E_{\text{security}}}{E_{\text{total}}}. \tag{5}$$

As shown in Fig. 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.

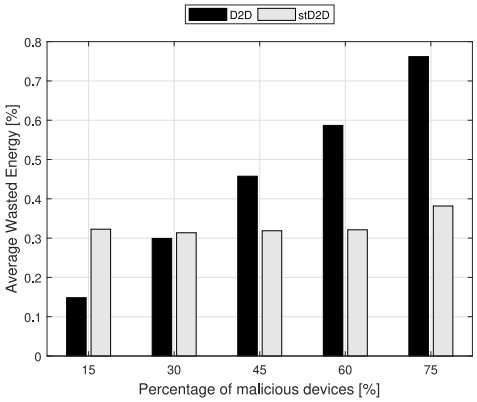

Fig. 4. Avg. wasted energy by D2D receivers vs. % of malicious devices.

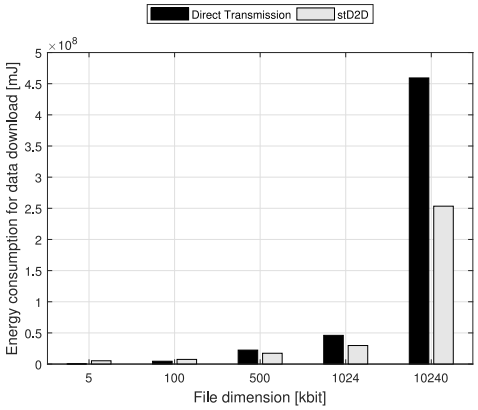

Fig. 6. Energy used to download data under increasing file dimension.

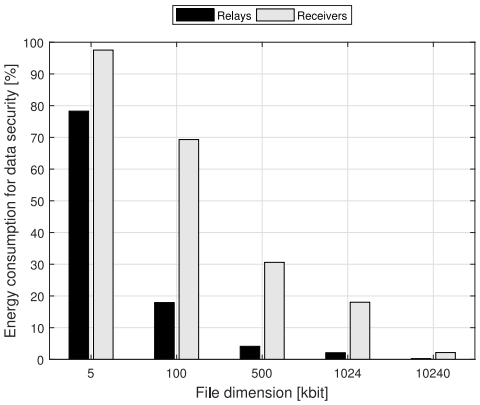

Fig. 5. % of energy consumed for data security vs. file dimension.

Fig. 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 Fig. 4. D2D receivers must handle more security data with respect to relays because our proposed protocol mainly requires the receivers to exchange information with the HeNB. Hence, the total energy consumption is greater for D2D receivers than for relays.

Fig. 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, Figs. 4, 5 and 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 our 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. We can affirm that the proposed protocol is 100% effective in the detection of malicious relays 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.

VI. Conclusion

The Machine-Type Multicast Service with secure and trust D2D (MtMS-stD2D) protocol, proposed in this paper, 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 Diffie-Hellman Key Exchange (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.

Since the introduction of a trustworthiness model showed to be a significant complement to security, because of the meaningful performance improvement it can bring, future research work will be tailored to the definition of a more accurate and realistic model for evaluating nodes' reliability.

REFERENCES

[1] I. F. Akyildiz, S. Nie, S.-C. Lin, and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," *Comput. Netw.*, vol. 106, pp. 17–48, Sep. 2016.

[2] (Jun. 2019). *Ericsson Mobility Report*. [Online]. Available: https://www.ericsson.com/en/mobility-report/reports

[3] S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood, "Internet of Multimedia Things: Vision and challenges," *Ad Hoc Netw.*, vol. 33, pp. 87–111, Oct. 2015.

[4] A. Martin *et al.*, "Network resource allocation system for QoE-aware delivery of media services in 5G networks," *IEEE Trans. Broadcast.*, vol. 64, no. 2, pp. 561–574, Jun. 2018.

[5] A. Karaagac, E. Dalipi, P. Crombez, E. De Poorter, and J. Hoebeke, "Light-weight streaming protocol for the Internet of Multimedia Things: Voice streaming over NB-IoT," *Pervasive Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101044.

[6] J. Bukhari and W. Yoon, "Multicasting in next-generation software-defined heterogeneous wireless networks," *IEEE Trans. Broadcast.*, vol. 64, no. 4, pp. 915–921, Dec. 2018.

[7] J. Nightingale, P. Salva-Garcia, J. M. A. Calero, and Q. Wang, "5G-QoE: QoE modeling for ultra-HD video streaming in 5G networks," *IEEE Trans. Broadcast.*, vol. 64, no. 2, pp. 621–634, Jun. 2018.

[8] 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," *IEEE Access*, vol. 4, pp. 5555–5569, 2016.

[9] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communications in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, 4th Quart., 2014.

[10] A. Moubayed, A. Shami, and H. Lutfiyya, "Wireless resource virtualization with device-to-device communication underlaying LTE network," *IEEE Trans. Broadcast.*, vol. 61, no. 4, pp. 734–740, Dec. 2015.

[11] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Jun. 2019.

[12] A. Shaghaghi, M. A. Kaafar, R. Buyya, and S. Jha, "Software-defined network (SDN) data plane security: Issues, solutions and future directions," in *Handbook of Computer Networks and Cyber Security*. Cham, Switzerland: Springer, Jan. 2020, pp. 341–387.

[13] S. Lal, T. Taleb, and A. Dutta, "NFV: Security threats and best practices," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 211–217, May 2017.

[14] C. Suraci, S. Pizzi, A. Iera, A. Molinaro, and G. Araniti, "Delivering multicast content through secure D2D communications in the Internet of Things," in *Proc. Wired/Wireless Internet Commun.*, Sep. 2019, pp. 182–193.

[15] *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2 (Release 15)*, 3GPP Standard TS 36.300, Sep. 2019.

[16] L. Feltrin *et al.*, "NarrowBand-IoT: A survey on downlink and uplink perspectives," *IEEE Wireless Commun. Mag.*, vol. 26, no. 1, pp. 78–86, Feb. 2019.

[17] Y.-P. E. Wang *et al.*, "A primer on 3GPP narrowband Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 117–123, Mar. 2017.

[18] G. Araniti, M. Condoluci, P. Scopelliti, A. Molinaro, and A. Iera, "Multicasting over emerging 5G networks: Challenges and perspectives," *IEEE Netw.*, vol. 31, no. 2, pp. 80–89, Mar./Apr. 2017.

[19] 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," *IEEE Trans. Broadcast.*, vol. 64, no. 4, pp. 791–802, Dec. 2018.

[20] G. Tsoukaneri, M. Condoluci, T. Mahmoodi, M. Dohler, and M. K. Marina, "Group communications in narrowband-IoT: Architecture, procedures, and evaluation," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1539–1549, Jun. 2018.

[21] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[22] 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," *IEEE Commun. Surveys Tuts.*, early access, doi: 10.1109/COMST.2019.2933899.

[23] *Security Architecture and Procedures for 5G System*, 3GPP Standard TS 33.501, Jun. 2019.

[24] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mobile Netw. Appl. J.*, vol. 22, no. 2, pp. 195–208, Apr. 2017.

[25] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-advanced networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659–2672, Apr. 2016.

[26] P. K. Jamshiya and D. M. Menon, "Design of a trusted third party key exchange protocol for secure Internet of Things (IoT)," in *Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, Apr. 2018, pp. 1834–1838.

[27] M. Pavloski, G. Görbil, and E. Gelenbe, "Bandwidth usage—Based detection of signaling attacks," *Inf. Sci. Syst.*, vol. 363, pp. 105–114, Aug. 2015.

[28] 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," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1037–1050, Feb. 2017.

[29] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.

[30] D. Rivera *et al.*, "Secure communications and protected data for a Internet of Things smart toy platform," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3785–3795, Apr. 2019.

[31] 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," *Comput. Netw.*, vol. 56, pp. 3594–3608, Nov. 2012.

[32] (Nov. 2018). *Ericsson Mobility Report*. [Online]. Available: https://www.ericsson.com/en/mobility-report/reports

[33] F. Al-Turjman, E. Ever, and H. Zahmatkesh, "Green femtocells in the IoT era: Traffic modeling and challenges—An overview," *IEEE Netw.*, vol. 31, no. 6, pp. 48–55 Nov./Dec. 2017.

[34] L. Militano, M. Condoluci, G. Araniti, A. Molinaro, A. Iera, and G. M. Muntean, "Single frequency-based device-to-device-enhanced video delivery for evolved multimedia broadcast and multicast services," *IEEE Trans. Broadcast.*, vol. 61, no. 2, pp. 263–278, Jun. 2015.

[35] L. Militano, A. Orsino, G. Araniti, and A. Iera, "NB-IoT for D2D-enhanced content uploading with social trustworthiness in 5G systems," *Future Internet*, vol. 9, no. 3, p. 31, Jul. 2017.

[36] *Proximity-Based Services (ProSe); Security Aspects*, 3GPP Standard TS 33.303, Jun. 2018.

[37] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the Social Internet of Things," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 18–23.

[38] 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," in *Proc. 10th MobySis*, Jun. 2012, pp. 225–238.

Sara Pizzi received the first- and second-level Laurea degrees (*cum laude*) in telecommunication engineering and the Ph.D. degree in computer, biomedical and telecommunication engineering from the University Mediterranea of Reggio Calabria, Italy, in 2002, 2005, and 2009, respectively, where she is a Research Associate of telecommunications. Her current research interests focus on QoS provisioning in wireless networks, resource allocation in multiradio wireless mesh networks, and multicast support in broadband wireless networks.

Chiara Suraci received the M.Sc. degree in telecommunications engineering from the University Mediterranea of Reggio Calabria, Italy, in 2018, where she is currently pursuing the Ph.D. degree with DIIES Department. Her current research topics include device-to-device communications in 5G cellular systems, network security, and multiaccess edge computing.

Antonio Iera received the graduation degree in computer engineering from the University of Calabria in 1991, and the master's degree in IT from the CEFRIEL/Politecnico di Milano in 1992, and the Ph.D. degree from the University of Calabria in 1996. From 1997 to 2019, he was with the University Mediterranea of Reggio Calabria, Italy. He is currently a Full Professor of telecommunications with the University of Calabria, Italy. His research interests include next generation mobile and wireless systems, and the Internet of Things.

Antonella Molinaro received the graduation degree in computer engineering from the University of Calabria in 1991, the master's degree in information technology from the CEFRIEL/Polytechnic of Milano in 1992, and the Ph.D. degree in multimedia technologies and communications systems in 1996. She is currently an Associate Professor of telecommunications with the University Mediterranea of Reggio Calabria, Italy, and also with CentraleSupelec, Paris-Saclay University, France. Her research activity mainly focuses on wireless and mobile networking, vehicular networks, and future Internet.

Giuseppe Araniti received the Laurea degree and the Ph.D. degree in electronic engineering from the University Mediterranea of Reggio Calabria, Italy, in 2000 and 2004, respectively, where he is an Assistant Professor of telecommunications. His major area of research is on 5G/6G networks and it includes personal communications, enhanced wireless and satellite systems, traffic and radio resource management, multicast and broadcast services, device-to-device, and machine-type communications (M2M/MTC).