

Security in device-to-device communications: a survey

ISSN 2047-4954

Received on 10th July 2017

Revised 15th September 2017

Accepted on 14th October 2017

E-First on 6th December 2017

doi: 10.1049/iet-net.2017.0119

www.ietdl.org

Othmane Nait Hamoud^{1,2} ✉, Tayeb Kenaza¹, Yacine Challal²

¹Department of Computer Science, Ecole Militaire Polytechnique, BP 17 Bordj Elbahri, Algiers, Algeria

²Ecole Nationale Supérieure d'Informatique, Oued S'mar, Algiers, Algeria

✉ E-mail: o_naithamoud@esi.dz

Abstract: Device-to-device (D2D) communication is a promising technology for the next generation mobile communication networks (5G). Indeed, it is expected to allow high throughput, reduce communication delays and reduce energy consumption and traffic load. D2D technology will enhance the capacity and the performance of traditional cellular networks. Security issues must be considered in all types of communications, especially when it comes to wireless communication between devices involved in controlling critical infrastructures and/or dealing with personal data. The authors propose taxonomy based on the review of recent works which have addressed the security issues in D2D communications. This taxonomy is more practical since it gives, on the one hand, a better readability and a good understanding of all the works that have addressed the security issues in the literature, and on the other hand, a roadmap towards a global security solution that combines the best techniques and security solutions inherent to each layer: physical, MAC, network and application.

1 Introduction

The rapid growth in the number of mobile internet subscribers has fostered the emergence of various new applications and services. This implies an exponential growth of mobile data traffic. Consequently, a huge burden is imposed on the cellular infrastructure in terms of spectrum utilisation, overall throughput, communications delays and energy consumption.

Expected to be one of the technology components of the evolving 5G architecture, device-to-device (D2D) communications are a promising solution to offload the cellular infrastructure from the traffic encumbrance. Indeed, the D2D communication approach allows devices (such as smart-phone, tablet, etc.) to establish direct communication links with each other without passing through an access point or a core network of a cellular infrastructure. The main difference between the expected 5G and the first four generations is that 5G is heading towards a device-centric network architecture contrary to the previous generations which have been network centric. In 5G, a device is expected to actively perform operations which were earlier being performed by the network such as storage, relaying and content delivery [1].

These recent years, academic, industrial, and standard institutions have paid considerable attention to the D2D communication technology. In academia, different surveys have been proposed in the literature [1–5] in which, different fields related to this technology were addressed (node discovery, interference and radio resource management, use cases and requirements, power control, system architecture and design, etc.).

In industry, Qualcomm has developed FlashLinQ [6] to implement for the first time D2D communication as sub-system underlying cellular networks to enable direct communications among proximity devices in different scenarios (content sharing, gaming, social networking, etc.). FlashLinQ was designed to work in a licensed cellular band based on time division duplexing-orthogonal frequency division multiple access technology which is the same as the long-term evolution-advanced (LTE-A) system, allowing devices to discover neighbours in a large range with high efficiency.

The standardisation of this new paradigm is underway by the third generation partnership project (3GPP) under the proposed proximity services (ProSe) [7] which allow enabling direct communication between proximate devices. ProSe combine two

types of services, proximity discovery and direct communication. In [8], a brief overview of standardisation activities of the 3GPP ProSe in LTE-A is presented.

Security issues must be considered in all types of communications, especially when it comes to wireless communication. D2D communications face many security challenges as part of the future 5G systems. The importance and dimension of these challenges are to define depending on many factors: open air nature of wireless communications, large-scale applications, use cases and scenarios, adoption of D2D technology by users at a large scale, pricing and business models, etc. Despite a very few recent works, security in D2D communication is not seriously well handled in the literature especially since these works are scattered depending on some specific security issues corresponding to different security aspects and scenarios.

We propose taxonomy based on the review of recent works which have addressed the security issues in D2D communications and shed light on the necessity to design a cross-layer security architecture to overcome efficiently these security issues.

The remainder of this paper is organised as follows. Section 2 provides an overview of D2D communications by introducing scenarios and use cases, the architecture of the core network of 3GPP's LTE wireless communication standard and the underlaid ProSe. In particular, we emphasise on the classification of D2D communications, where we propose a new one that highlights their flexibility and agility so that they will be used in an efficient manner. In Section 3, we investigate potential threats and summarise the corresponding security requirements. In Section 4, we propose a new taxonomy and review the state-of-the-art D2D communication security. Section 5 discusses the summary of the reviewed works. Finally, we conclude in the last section.

2 Overview of the D2D communication

Initially, direct communications were introduced in the third generation networks (3G) within the wireless personal area network and wireless local area network (WLAN) technologies. These technologies occurred on an unlicensed band which did not provide quality of service guarantees due to the uncontrollable interference. In spite of the role which can play D2D paradigm to enhance the performance of cellular networks, cellular operators did not pay attention to D2D communications because of the

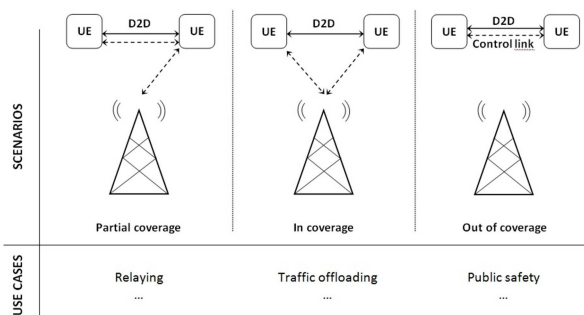


Fig. 1 Typical scenarios and use-cases in D2D communications

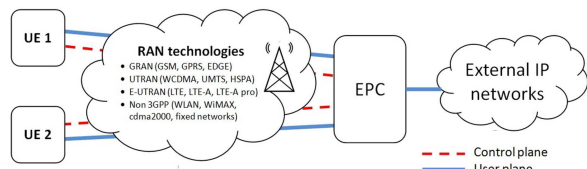


Fig. 2 Basic architecture of the EPS in 3GPP

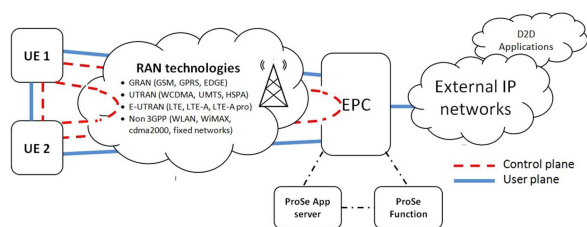


Fig. 3 Basic architecture of the ProSe underlying 3GPP's EPS

limited benefits of local communication services. However, with the growth of traffic due especially to the increasing popularity of mobile applications based on devices' proximity such as social networking, network gaming, etc., cellular operators are getting attracted towards the D2D technology until its introduction in the fourth generation (4G) through LTE-Direct and FlashLinQ [6].

2.1 Scenarios and use cases

Different scenarios and use cases were proposed by 3GPP in [7]. Depending on the degree of implication of a cellular network operator (CNO) in D2D communications, three typical scenarios and use cases are shown in Fig. 1.

- **In coverage scenario:** the control link is totally ensured by the CNO. The main use case in this scenario is traffic offloading. For example, if the same content is requested by different UEs from the same eNB (evolved node B; video streaming of football match), the later will transmit the content to user equipments (UEs) as cluster heads, which in turn multicast the content through D2D links to the rest of UEs belonging to the corresponding cluster. Local social networks (NextDoor, Topix, Foursquare, etc.) are emerging nowadays and allow companies to target clients in a specific geographic location with multiple and attractive services (advertising). Through D2D links, such types of networks can be more efficient.
- **In partial coverage scenario:** the control link is partially ensured by the CNO. The main use case in such a scenario is the extension of cellular network coverage in areas (refugee camp, rural areas, etc.) where the cost of traditional infrastructure facilities is impossible to justify.
- **In out of coverage scenario:** the control link is ensured by the devices themselves. The typical use case in this scenario is the emergence and critical public safety communications where the cellular infrastructure is absent due to natural disaster, terrorist attacks, etc.

In the literature, different works have investigated potential D2D use cases such as traffic offloading [9, 10], social networking [9, 11, 12], smart media sharing [11, 13, 14], intermittent cellular connectivity [10, 15, 16], extended coverage [7, 17], and disaster rescue [18]. However, security issues in most of these works were slightly considered or the underlying environment was assumed secure.

2.2 System architecture

In this section, we present the basic architecture of the core network of 3GPP's LTE wireless communication standard, namely the evolved packet system (EPS). The main components of the EPS are: (1) the UE, (2) the radio access network (RAN) and (3) the evolved packet core (EPC). Fig. 2 illustrates a basic architecture of the EPS in which, a UE is connected to the EPC over a RAN technology. To make the scaling independent, it was decided to separate in the EPC the user plane (data) and the control plane (signalling). Besides that, 3GPP had specified support of multiple access technologies [evolved-universal terrestrial radio access network (E-UTRAN) for LTE and LTE-A, global system for mobile communication (GSM) edge radio access network (GERAN) for GSM/general packet radio service (GPRS) and UTRAN for the Universal Mobile Telecommunication System based technologies: wideband code division multiple access (WCDMA) and high speed packet access (HSPA)] and also the handover between these accesses to ensure convergence by using a single core network. The EPS also allows non-3GPP technologies (WiMAX, cdma2000, WLAN or fixed networks) to interconnect the UE and the EPC.

The 3GPP has proposed the D2D communication (ProSe) as an underlying network of the existing LTE-A networks [19]. They integrated two new entities: (1) ProSe function which may provide connections between application servers and UEs and handle ProSe-related functions (UE registration, UEs' discovery, security, etc.) and (2) a ProSe application server which serves UEs requesting ProSe through a logical link. Fig. 3 shows a simplified network architecture for the ProSe, where the control plane can be ensured in three different levels: UE, RAN and EPC.

In the EPS of the 3GPP, ProSe features consists of [20]: (1) ProSe Discovery (ProSe-D), which identifies that ProSe-enabled UEs are in proximity using evolved-universal terrestrial radio access technology (with or without E-UTRAN) or EPC; and (2) ProSe Direct communication (ProSe-DC), which enables establishment of communication paths (using E-UTRAN or WLAN) between two or more ProSe-enabled UEs that are in the direct communication range. In the context of public safety usage, UEs can establish the communication path directly, regardless of whether they are served by E-UTRAN; and ProSe-DC is facilitated by the use of a ProSe UE-to-network relay, acting as a relay between E-UTRAN and UEs.

2.3 Classification

D2D communications can be considered as the bridge between ad hoc networks and centralised networks. On the one hand, it can be integrated into the ad-hoc mode other promising techniques such as cooperative communications [12, 21–23] and cognitive radio [3, 24] in order to enhance spectrum efficiency. On the other hand, the centralised mode of cellular networks can resolve interference issues.

The D2D communication can occur either on an operator's licensed spectrum (underlying LTE-A networks) or an unlicensed spectrum (Bluetooth, WiFi-Direct). Gandotra and Jah [4] have proposed taxonomy based on the D2D communication spectrum and have reviewed several works in the field.

In the licensed band, D2D communications cohabit with cellular communications and gain advantages in terms of spectral efficiency and interference control and management. In this category, D2D links are further divided into underlay and overlay subcategories, where D2D and cellular links share the same radio resources in the first subcategory and are given dedicated radio resources in the second one. The main advantage in underlay D2D communications is the spectral efficiency. However, power control

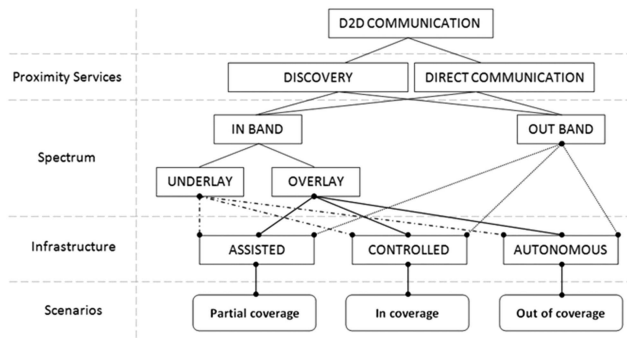


Fig. 4 Classification of D2D communications

and resource allocation solutions have to be more complex; and a user cannot perform simultaneously cellular and D2D communications. In contrast, overlay D2D eliminates the interference issue between cellular and D2D communications, but it wastes radio resources.

In the unlicensed band, there is no interference between cellular and D2D communications, but an extra interface which uses other wireless technologies (WiFi-Direct, Bluetooth, etc.) is required. D2D communications in this category are further divided into subcategories: controlled and autonomous communication. In controlled unlicensed D2D communication, the cellular operator controls both cellular and wireless technology interfaces. In contrast, the user's device controls the D2D communication interface in autonomous unlicensed D2D communication. Simultaneous cellular and D2D communications can be made by a user's device in this category.

In the following, we propose a revised classification which highlights the hybridisation and flexibility of D2D communication techniques, compared with other available techniques. The classification we propose here (Fig. 4) is more practical to understand the existing solutions and to apprehend new ones related to D2D communication since it is based on the proximity services (discovery or direct communication), on the spectrum (in band or out band) and on the involvement level of the cellular infrastructure (assisted, controlled or autonomous). The assistance of cellular infrastructure refers to controlling D2D communication links at the RAN level (i.e. eNB).

Nowadays, mobile devices support simultaneously multiple radio access technologies (2G, 3G, 4G, WiFi-Direct, Bluetooth, NFC, etc.), and are given more and more processing and storage capacity. Besides, with a variety of radio access technologies, multiple formats of cells (micro-, pico- and femto-cells) with different power levels are deployed in the same geographical area. Thus, D2D communication can benefit, on the one hand, from this diversity from the point of view of signal control, energy efficiency, resource allocation, throughput, and new services and applications, and on the other hand, from the point of view of context and scenario in which they are applied.

Through this classification, we can imagine a branch of solutions, depending on the context and the situation in which, D2D communications will be used. For example, in order to offload cellular traffic through D2D links, DataSpotting [25] adopted a hybrid mode of spectrum allocation (in band and out band). The system uses the licensed band to control channel for all the setup procedures until activating both the content requester and provider in WiFi ad-hoc mode. A cellular operator assists UEs only in neighbourhood discovery. Under the assistance of an eNB, FlashLinQ works over the dedicated licensed band to enable UEs to discover proximity devices in a large range with high efficiency and to communicate directly in a distributed and autonomous manner over the licensed band. Relay-by-smartphone is a multi-hop D2D communication system which was developed for disaster relief application [26]. According to the situation (neighbour node density, mobility pattern, remaining battery power, etc.), a smartphone could switch between mobile ad hoc networks (MANET) operation mode and delay/disruption tolerant networks (DTN) operation mode in the message delivery process in such a way that the overall message delivery performance is improved.

In a centralised system, network performance is guaranteed due to resource control and interference coordination provided by the operator. However, the system will cost larger overhead and will result in a limitation of privacy and scalability. Furthermore, in a distributed system, EUs are autonomous entities, each with its own objective, and its own actions, independently and in a self-directed manner. The system will, therefore, be more flexible, autonomous and scalable.

3 Security in D2D communications

In this section, we present security threats and requirements in D2D communications.

3.1 Security threats

The radio nature of D2D communications introduces various security threats [14, 27]. The main threats are as follows:

- *Eavesdropping attack*: an attacker passively listens to the radio channel between UE devices in order to get sensitive data. Encryption can be used to defeat this threat.
- *Impersonate attack*: an attacker can pretend to be a legitimate UE device or eNB to get access to the traffic data. Authentication should be considered to parry this threat.
- *Forge attack*: an attacker may forge a specific content and send fake data to UEs, which can make prejudice to the system. Integrity control using hash functions and digital signatures should be considered to defeat this kind of attack.
- *Free-riding attack*: to reduce system availability in D2D communications, an attacker may encourage the selfish behaviour of some UEs to preserve energy consumption so they may not be willing to send contents to others while receiving its demanding data from their peers. Such vulnerability may affect the quality of experience and therefore irritates user experiences and hinders the adoption of D2D communications. To resist to such an attack, it is necessary to develop cooperative stimulation mechanisms such as works done in [12, 21–23, 28].
- *Active attack on control data*: an attacker tries to change the control data. Authentication, confidentiality and integrity using cryptography approaches can parry this threat.
- *Privacy violation*: some privacy-sensitive data such as identity, location, etc. are more concerned with D2D services, so this personal information must be concealed to non-authorised parties.
- *Denial-of-service (DoS) attack*: it consists of rendering unavailable a service in D2D communications. In [29], authors have shown via an experimental study, by exploring characteristics of DoS attacks on Android devices in D2D underlying the network environment that malicious devices can stealthily impair or even totally block the connection of legitimate devices in the underlying network.

3.2 Security requirements

Due to the aforementioned threats, a secure D2D communication system should fulfil the following security requirements [14, 27, 30], whether they are assisted, controlled or autonomous:

- *Authentication*: identification of communicating parties must be checked.
- *Data confidentiality*: transmitted data between devices must be secret using encryption mechanisms.
- *Data integrity*: data transferred by authorised devices should be verified that they are not altered.
- *Privacy*: privacy information such identity, SIM card number, geographical position, etc. must be preserved.
- *Traceability*: it is necessary to track the source of security violation attempts. However, some conflicting situations between privacy and traceability must be considered as highlighted in [31].
- *Anonymity*: communicating UEs may be anonymous to each other and from an adversary.

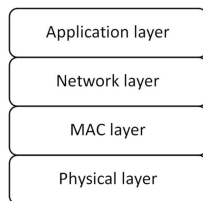


Fig. 5 Layered approach

- *Non-repudiation*: refers to the ability to prevent UEs from denying transmission or reception of a message. In the cryptography approach, digital signature is an efficient tool to prevent from transmission non-repudiation, while an additional mechanism is required to ensure reception non-repudiation.
- *Availability*: D2D services should be accessible anytime and anywhere even under DoS or free-riding attacks, lest users be discouraged to use this technology.
- *Revocability*: refers to ability to reprove user privilege of a D2D service if it is detected as malicious.
- *Fine-grained access control*: takes into account small granularity of an access rule specified to a UE when accessing in its service. It is seen as an effective solution to overcome privacy and data transmission security issues.

4 Taxonomy of D2D security solutions

An intuitive approach to address security issues in D2D communications can be based on network layers on which security is concerned. Following this approach, a complete security solution can be designed to provide the required protection for the devices involved in D2D communications. Such a solution must be based on security protocols built on each layer which has to co-operate together (Fig. 5). Besides, this approach can enable an agile defensive response for a system under attack by shifting D2D communication to a new combination of encryption implementation, routing protocol, and media access technique and frequency band [32].

This layer-based approach of security can provide a clear understanding of D2D communications security and help towards better protocol design. Based on this approach, we provide in this section an extended taxonomy of security solutions depending on which layer a solution belongs.

4.1 Application layer

In this layer, a key management scheme is considered as the foundation of any solution based on cryptography. Various solutions have been proposed in the literature [9, 13, 14, 18, 31, 33–37] (Table 1).

Recently, Abd-Elrahman *et al.* [31] proposed a solution based on the identity-based encryption (IBE) and elliptic curve cryptography (ECC) mechanisms for key generation to secure exchanged messages during the discovery and communication phases. The proposed solution is discussed under two D2D use cases (single operator and multi-operators) and is further used to introduce an efficient key management system for group communication. Besides, authors designed a protocol based on the modified IBE system to ensure privacy support and legal interception for D2D clients. For this aim, authors have validated this protocol in a platform for a social network scenario using the D2D aspect in single and multi-operators' use cases. Authors proposed also in [33] a Group Key Management mechanism for the same purpose as in [31]. In this work, they used multiple Private Key Generators which are more suitable for different operators' use case than a single one as proposed previously.

In [9], three key exchange protocols for a secure network-assisted D2D communication in a cellular network are proposed. These protocols are based on Diffie–Hellman (DH) key exchange, but they differ in the role of the eNB in the authentication process. Authors have considered traffic offload and social networking use cases.

Zhang *et al.* have proposed a secure data sharing protocol for D2D communications in LTE-A network based on symmetric and asymmetric encryption [14]. Authors have considered a media-sharing scenario because of the ease of use, but the model can be extended to be more general scenarios. The involvement of EPC is assured by a gateway which serves as the gate from the local subsystem to the core network. To completely offload the cellular network, authors have proposed an interesting idea in [27] but it has not been investigated in their work. The idea introduces certificate less public key cryptography [40] to secure D2D communications.

To enable two UEs to establish a secret key to secure D2D communications without prior knowledge or involvement of EPC, Shen *et al.* [34, 39] have proposed a key agreement protocol based on the DH key exchange and a commitment scheme.

In [35], a probabilistic key management scheme was derived from wireless sensor networks (WSNs) and employed to secure D2D communications for a public safety scenario. In [36], a novel authentication protocol is proposed in a non-network assisted mode with a secure initial key establishment using cipher-policy attribute-based encryption (CP-ABE). This protocol allows the communicating parties to mutually authenticate and derive the link key in a secure manner in a multi-hop scenario.

Alam *et al.* [18] have reused the existing security solutions of LTE-A technology in order to secure D2D communication for three types of scenarios: network offloading, social networking and disaster rescue. The proposed mechanisms are based on the involvement of a cellular network as a trustworthy third party and the presence of a user application. An authentication system for D2D communication under LTE is proposed by Wang *et al.* [37], in which a shared master key is sent by the core network to UEs in order to derive a session key.

Besides, since social networking is considered as the main scenario for D2D communications, security and privacy in the mobile social network are a challenging work to construct social trust and social ties promoting efficient cooperation with privacy preservation among users. Many works have focused on the security aspect of social networking [11, 12, 15, 16, 38]. Ometov *et al.* have proposed in the context of a network-assisted D2D communication two solutions to maintain and extend the secure D2D communications in the case of unreliable cellular connectivity [15, 38]. In these solutions, authors consider all of the involved devices to be at least equipped with an LTE and WiFi interfaces and have been connected to the cellular network which is assumed to be their trusted authority. In [15], authors' target scenario consists of the assisted offloading of devices' cellular data flows onto their WiFi-Direct sessions. Cellular links are used by devices only for transferring signalling information and to communicate with the public key infrastructure (PKI) and establish a logical group of securely-communicating devices named a coalition. Based on a mathematical model, the algorithm allows adding new users to secure coalition as well as excluding existing ones from it, even in the case of an unreliable cellular network. To trial this theoretical solution, an implementation of the secure network-assisted D2D framework in live 3GPP LTE deployment was proposed in [16].

In [38], authors target a scenario consisting of providing additional coverage for users who are facing intermittent cellular connectivity and thus helping disseminate content to a larger number of user devices. Coalition formation (clustering) in this work is based on a game theoretical framework where social proximity (relationships among users) and spatial proximity (effect of cellular transmissions) are considered explicitly. Orsino *et al.* [10] adopted a game-theoretic optimisation approach to secure throughput optimised communications in the D2D-assisted cellular system.

Chen *et al.* [12] studied cooperative D2D communications based on social trust and social reciprocity. Authors target a multi-hop D2D communication scenario for relaying purpose and develop a novel coalitional game-theoretical framework. They prove the existence of a core solution and propose a mechanism to implement it by identifying reciprocal cycles, each of which contains the nodes motivated to act as a relay for others in the same

cycle. In [11], authors proposed a novel social-aware approach for optimising D2D communications based on a social network and physical wireless network layers.

Hadiks *et al.* [29] studied the impacts of DoS attacks on a D2D underlying network. Authors' experiments have shown how attacks can force UE to lose the WiFi connection with the access point without being detected by the access point (AP) or the cellular network. The goal of this work was to inspire deeper studies and more efforts in this field.

To offload cellular traffic without increasing the infrastructure cost, Ramasubramanian *et al.* [13] have considered only the network assisted mode to propose a D2D business model and to

implement an application level security framework for devices involved in D2D communications.

4.2 Network layer

D2D communications can be used in a disaster rescue (earthquake) when a network infrastructure becomes absent [14]. In this scenario, devices can play an important role in relaying D2D communications over a public safety network which requires secure communications. Moreover, secure multi-hop D2D communications can contribute to anonymity against cellular operators [17, 41–44] (Table 2).

Table 1 Application layer

	Works	Network assisted mode	Ad-hoc	Scenario or application	Techniques based	Resis. attacks	Implem.	Simul.
	In cov.	Relay	EPC	mode				
[31]	yes	no	yes	no	key management: • same operator • different operators	IBE–ECC elliptic curve Diffie-Hellman (ECDH)	reply imperson. man in the middle (MITM)	no Miracl
[33]	yes	no	yes	no	key management: • same operator • different operators • hierarchical groups	IBE–ECC elliptic curve digital signature algorithm (ECDSA)	key escrow ident. disclos.	no Miracl
[9]	yes	no	no	no	key management: • traffic offload • social network	DH	MITM brute force	no Matlab
[13]	yes	no	yes	no	media sharing business model	PKI	—	yes no
[15]	yes	yes	yes	yes	traffic offload	PKI	—	no no
[38]	yes	yes	yes	yes	intern. cel. connec. extended coverage dessiminat. content	constr. sec. coal. PKI GT clust.	—	open secure socket layer (Open SLL)
[16]	yes	yes	yes	yes	intern. cel. connec.	Shamir sec. sch. constr. sec. coal.	—	yes TestBed
[10]	yes	yes	yes	yes	traffic offload Intern. cel. connec.	PKI game theoretic (GT) clust.	—	no yes
[11]	yes	no	yes	no	social network traffic offload media sharing	social ties Indian buffet process	—	no yes
[12]	yes	yes	yes	no	social network extended coverage enhance coop. D2D	social trust social reciprocity coali. game	—	no yes
[14]	yes	no	yes	no	media sharing traffic offload	PKI bilinear pairing Diffie-Hellman key exchange	—	no yes
[34]	no	no	no	yes	authentication	DH	MITM	yes no
[39]					key agreement	commit. scheme		
[35]	no	no	no	yes	public safety	probabilistic key management scheme (Prob. KMS)	—	no no
[36]	no	no	no	yes	multi-hop	DH	MITM reply	No Matlab
[18]	yes	yes	yes	yes	traffic offload social network public safety	PKI predistributed shared key	—	no —
[37]	yes	no	yes	no	authentication key agreement	PKI shared master key	—	— no
[29]	yes	no	no	yes	studying impact of DoS attack	—	—	yes no

Tata *et al.* have proposed a secure network coding based data splitting and data shuffling algorithm to secure a routing protocol for public safety D2D communications over LTE heterogeneous networks (HetNets) without adding additional control traffic [41]. To assure confidentiality in the network, the solution consists of applying the data splitting and shuffling mechanisms for forwarding over a butterfly network symbols rather than whole packets through a network coding path. Authors have proposed another approach for secure D2D routing if it is unable to apply network coding transmissions within LTE small cells [42]. The proposed algorithm called secure load balancing selective ad hoc on demand multipath distance vector (AOMDV) is based on a multi-path coded information transmissions, data splitting, and data shuffling schemes.

In the context of internet of things (IoT) scenario, Steri *et al.* [43] have proposed a secure protocol for multi-hop D2D communications where LTE-A UEs aggregate data generated in their surroundings by IoT things and the proposed protocol connects UEs to a cellular base station, which transports the traffic to the internet. The security feature of this solution is based on the work [35] where a probabilistic key management scheme is employed. In another context where UEs are out of coverage, Panaousis *et al.* have proposed in [17] a secure message delivery protocol to choose the most secure path to deliver a message from a sender to a destination in the multi-hop D2D network. For this end, authors used game theory to model the interactions between a D2D network and attacker which aims at sending a malicious message through a D2D network.

A joint operation of routing control and group key management for 5G ad hoc D2D networks is proposed in [44]. To offload the cellular network from the local traffic, the UE is assumed acting in a way that it can response to either infrastructure or ad hoc D2D communication requirements. So, authors' idea is based on the fact that the dual operation of the infrastructure and ad hoc D2D mode communications in the same UE requires the ad hoc node to rely on the network layer function as small as possible. The proposed protocol controls the ad hoc D2D network and manages the group key in the self-managed group of ad hoc nodes based on their home internet protocol address wherever they move. The authentication process is based on the PKI of the cellular network.

4.3 MAC layer

Access control is an important component in D2D communication security (Table 3). In out of coverage network extension or public safety scenarios, UEs have to become eligible to replace the role of the base station in terms of resource allocation and controlling signal [57]. On the other side, since cellular and D2D communications occur on the shared spectrum (licensed band), mutual interference appears to be harmful. However, D2D communications can be introduced as interference against eavesdroppers [53]. Thus, the secrecy capacity which quantifies the security of transmission of both D2D and cellular communications

can be preserved and even improved which consequently increases the corresponding throughput [46].

Other works considered an access control issue under the framework of a multi-priority model which assigns the highest priority to cellular users and multiple levels of priority for D2D ones [45, 47], where network calculus theory was employed to model and analyse the access control for D2D communications underlying cellular networks. Besides, access control can be used as a solution to preserve location and identity privacy in D2D communications [30].

4.4 Physical layer

Developing security features at the physical layer leads to enforcing the security of upper layers and thus improves overall D2D communications. Channel State Information (CSI) which refers to known channel properties of a wireless link can serve to extract secret keys from the measurement of the physical layer (Table 3). Recently, various CSI-based key extraction works have been proposed to secure D2D communications [23, 32, 48–56]. Xi *et al.* [48] proposed a fast secret key extraction protocol for D2D communication (KEEP), in which a validation–recombination mechanism is used to obtain symmetric secret keys from the CSI measurements of all orthogonal frequency division multiple subcarriers. The protocol achieves a high security level against eavesdropping and predictable channel attacks. Sun *et al.* [23] studied a secret key establishment between two devices in D2D communications and proposed SYNERGY, a game-theoretical approach in order to stimulate cooperative key generation and to face the attitude of self-interested nodes which are reticent to act as relays.

To emphasise the enforcement security that D2D paradigm can achieve via the physical layer, Zhu *et al.* [49] have derived the secrecy outage probability of the D2D and cellular networks and have compared performance for D2D scenarios in the presence of multi-antenna eavesdroppers. Zhang *et al.* [50] considered physical-layer security in D2D underlying cellular networks and shown that D2D communications can lift the system secrecy capacity to a higher level.

In [51], a novel resource allocation based on the physical layer security has been proposed, in which a power and subcarrier allocation scheme maximises the D2D security capacity without influencing the cellular user's basic capacity. Jayasinghe *et al.* have designed a secure beamforming technique to prevent eavesdropping on multiple-input multiple-output D2D communications via a trusted relay which performs physical layer network coding [52].

Ma *et al.* [53] have considered a large-scale D2D-enabled cellular network with the presence of eavesdroppers overhearing cellular communications which were modelled using stochastic geometry. To guarantee performances of secure cellular communications, authors have proposed strong and weak performance guarantee criteria. In [54], a security-embedded

Table 2 Network layer

Works	Network assisted mode In cov.	Relay	EPC	Ad-hoc mode	Scenario or application	Techniques based	Resis. attacks	Implem.	Simul.
[41]	no	no	no	yes	public safety routing over butterfly network	network coding coded matrix data split. mecan.	eavesdrop.	no	Matlab
[42]	no	no	no	yes	public safety over LTE HetNet	network coding data shuffling data split. mecan.	eavesdrop.	no	Matlab
[43]	yes	yes	yes	yes	multi-hop IoT relying coverage ext.	prob. KMS direct beacon	—	no	yes
[17]	no	no	no	yes	routing	game theory confusion matrices	malware	no	yes
[44]	yes	yes	yes	yes	traffic offload routing	PKI	—	no	yes

interference avoidance scheme has been proposed based on the concept of constellation-rotation which provides an inherent secrecy protection at the physical layer for both D2D and cellular users. Zhang *et al.* [55] have investigated the physical layer security issue in D2D communications underlying cellular networks from a joint optimisation perspective. They have proposed a secrecy-based joint power and access control scheme with an optimum D2D pair selection mechanism for cellular communication links and D2D pairs. Zhang *et al.* [56] proposed a radio resource allocation solution which improves the secure capacity of D2D users underlying heterogeneous networks.

The work in [32] contributes to D2D security by employing the concept of continuous authenticity and proposing a security scoring system for measuring security. This solution is based on legitimacy patterns which are sent continuously to confirm and maintain the legitimacy of the involved devices in D2D communications.

5 Discussion

By reviewing many recent works related to security in D2D communications, we notice that these works are scattered depending on some specific security issues in different security aspects and contexts. The majority of works within the application layer deals with cryptographic key management issues in order to apply them in a specific context. From the cryptographic point of view, key management schemes are important to find efficient cryptographic solutions in order to satisfy requirements in terms of authentication, confidentiality, integrity and many other security issues. The proposed solutions in the literature did not assume all scenarios related to the involvement of the cellular infrastructure (i.e. assisted, controlled or autonomous), the most important difficulties concern keys' distribution and revocation problems. It is judicious to reuse security solutions ensured by a cellular infrastructure, but in the same time these solutions have to work in the case of an out-of-coverage scenario.

In the out of coverage scenario, techniques used in the proposed key management schemes are inspired from those used in the context of WSNs and mobile ad-hoc networks, such as DH-based

key exchange, IBE-ECC, CP-ABE and probabilistic key management schemes. However, D2D communications may gain advantage from the control and the assistance of a cellular infrastructure by getting necessary credentials to be employed in the case of intermittent cellular connectivity or out of coverage scenarios. On the other side, local social networks have attracted increasing attentions from researchers in recent years. To face privacy issues in this type of scenario, clustering and coalition formation are the main approaches developed for this purpose.

Generally, D2D communications rely on one hop routing; however, in different scenarios (public safety, extension of coverage, dissemination of content, etc.) they may rely on multi-hop routing. Few works in the literature have treated the routing aspect in D2D communications. From the security point of view, much work remains to be done, especially to face security threats related to the absence of trust authority and the highly dynamic topology on the one hand; and on the other hand to preserve security and privacy of users which will see their sensitive information transit different nodes without trust authority. Besides, malicious contents can be injected into the D2D network to affect UEs with viruses, malwares and many other threats. Secure D2D routing through a cryptography approach needs manipulating cryptographic keys that key management schemes must take into account. Another approach to secure routing in D2D communications relies on network coding which employs data splitting and shuffling mechanisms over butterfly networks.

Physical layer security is playing a key role in securing wireless communications in recent years. It exploits physical characteristics of the wireless channel to prevent essentially from an eavesdropping attack without utilising cryptographic approaches. Works related to this field turn around theoretic secrecy capacity, CSI-based authentication and CSI-based key agreement.

6 Conclusion

D2D is a promising technology in LTE-A networks. Taking advantage of proximity devices, it offers high throughput, lower delays and offloading cellular networks traffic. On the other side, it

Table 3 MAC and physical layers

Works	Network assisted mode			Ad-hoc mode	Scenario or application	Techniques based	Resis. attacks	Implem. Simul.	
	In cov.	Relay	EPC						
[45]	Yes	no	yes	no	access control	multi-priority model network calculus theory	—	no	yes
[46]	Yes	no	yes	no	access control	CSI secrecy outage prob.	eavesdrop.	no	yes
[47]	Yes	no	yes	no	access control	multi-priority model network calculus theory	—	no	yes
[32]	yes	no	yes	no	developing security-scoring measure	continuous authenticity	eavesdrop.	no	yes
[48]	no	no	no	yes	detecting physic. attacks establish a share secret key between two UEs	legitimacy patterns CSI validation-recombination mechanism	jamming injecting eavesdrop.	yes	no
[23]	no	no	no	yes	key management multi-hop	CSI GT approach for key generation	eavesdrop.	no	Matlab
[49]	no	no	no	yes	physical layer security secrecy outage prob.	CSI	eavesdrop.	no	yes
[50]	yes	no	yes	no	physical layer security	system secrecy capacity Kuhn–Munkres algorithm	eavesdrop.	no	yes
[51]	yes	no	no	no	physical layer security	system secrecy capacity	eavesdrop.	no	yes
[52]	yes	no	no	no	physical layer security	CSI	eavesdrop.	no	yes
[53]	yes	no	no	no	physical layer security	physical network coding stochastic geometry	eavesdrop.	no	yes
[54]	yes	no	no	no	physical layer security	constellation rotation	distrust between cellular and D2D users	no	yes
[55]	yes	no	no	no	physical layer security	system secrecy capacity	eavesdrop.	no	yes
[56]	yes	no	no	no	physical layer security	system secrecy capacity	eavesdrop.	no	yes

offers a variety of practical services (advertising and commercial services, public safety services, etc.). There are many design challenges in D2D so that much research effort is still needed. Security in D2D communication is still in an embryonic state. Few works have handled security issues in this novel technology. Furthermore, these works address security in a scattered way as each solution is defined in a well-defined scenario and faces well-defined threats and does not attempt to solve security problems in their entirety. Generally, the existing security solutions work on a specific layer (application, network, MAC or physical layer), while the few solutions which consider the corresponding security aspects of more than one layer do so only independently. We are interested in emphasising the necessity to develop a security solution which fulfils all security requirements, faces all security threats and supports all D2D communication scenarios. The approach we advocate is based on a joint framework which involves each layer security technology to work in a cooperative way to overcome efficiently security issues. Thus, significant efforts must be provided in order to overcome seriously D2D security problems.

7 References

- [1] Gandotra, P., Jah, R.K., Jain, S.: 'A survey on device-to-device (D2D) communication: architecture and security issues', *J. Netw. Comput. Appl.*, 2017, **78**, pp. 9–29
- [2] Asadi, A., Wang, Q., Mancuso, V.: 'A survey on device-to-device communication in cellular networks', *IEEE Commun. Surv. Tutor.*, 2014, **16**, (4), pp. 1801–1819
- [3] Liu, J., Kato, N., Ma, J., *et al.*: 'Device-to-device communication in LTE-advanced networks: a survey', *IEEE Commun. Surv. Tutor.*, 2015, **17**, (4), pp. 1923–1940
- [4] Gandotra, P., Jah, R.K.: 'Device-to-device communication in cellular networks: a survey', *J. Netw. Comput. Appl.*, 2016, **71**, (Suppl. C), pp. 99–117
- [5] Fodor, G., Dahlman, E., Mildh, G., *et al.*: 'Design aspects of network assisted device-to-device communications', *IEEE Commun. Mag.*, 2012, **50**, (3), pp. 170–177
- [6] Wu, X., Tavildar, S., Shakkottai, S., *et al.*: 'FlashLinQ: a synchronous distributed scheduler for peer-to-peer *ad hoc* networks', *IEEE/ACM Trans. Netw.*, 2013, **21**, (4), pp. 1215–1228
- [7] 3GPP TR 22.803: 'Feasibility study for proximity services (ProSe) (Rel. 12), V1.2.2.0', June 2013
- [8] Lin, X., Andrews, J.G., Ghosh, A., *et al.*: 'An overview of 3GPP device-to-device proximity services', *IEEE Commun. Mag.*, 2014, **52**, (4), pp. 40–48
- [9] Seddi, R., Kumar, A.: 'Key exchange protocols for secure device-to-device (D2D) communication in 5G'. Wireless Days 2016, Toulouse, France, March 2016, pp. 1–6
- [10] Orsino, A., Ometov, A.: 'Validation information security framework for offloading from LTE onto D2D links'. Proc. 18th Conf. of Open Innovation and Seminar on Information Technology (FRUCT-ISPIT), St. Petersburg, Russia, April 2016, pp. 241–247
- [11] Zhang, Y., Pan, E., Song, L., *et al.*: 'Social network aware device-to-device communication in wireless networks', *IEEE Trans. Wirel. Commun.*, 2015, **14**, (1), pp. 177–190
- [12] Chen, X., Proulx, B., Gong, X., *et al.*: 'Exploiting social ties for cooperative D2D communications: a mobile social networking case', *IEEE/ACM Trans. Netw.*, 2015, **23**, (5), pp. 1471–1484
- [13] Ramasubramanian, S., Chung, S., Ding, L., *et al.*: 'Secure and smart media sharing based on a novel mobile device-to-device communication framework with security and procedures'. Proc. RIIT'15, Chicago, Illinois, USA, 2015, pp. 35–40
- [14] Zhang, A., Chen, J., Hu, R., *et al.*: 'SeDS: secure data sharing strategy for D2D communication in LTE-Advanced networks', *IEEE Trans. Veh. Technol.*, 2016, **65**, (4), pp. 2659–2672
- [15] Ometov, A., Zhidanov, K., Bezzateev, S., *et al.*: 'Securing network-assisted direct communication: the case of unreliable cellular connectivity'. IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, August 2015, pp. 826–833
- [16] Ometov, A., Masek, P., Urama, J., *et al.*: 'Implementing secure network-assisted D2D framework in live 3GPP LTE deployment'. Proc. IEEE Int. Conf. on Communications (ICC) 2016-Workshops, Kuala Lumpur, Malaysia, May 2016, pp. 749–754
- [17] Panaousis, E., Alpcan, T., Fereidooni, H., *et al.*: 'Secure message delivery games for device-to-device communications'. Int. Conf. on Decision and Game Theory for Security, Los Angeles, CA, USA, November 2014 (LNCS, 8840), pp. 195–215
- [18] Alam, M., Yang, D., Rodriguez, J., *et al.*: 'Secure device-to-device communication in LTE-A', *IEEE Commun. Mag.*, 2014, **52**, (4), pp. 66–73
- [19] 3GPP TR 23.703: 'Study on architecture enhancements to support proximity services (ProSe) (Rel. 12), V12.0.0', February 2014
- [20] 3GPP TS 23.303: 'Proximity-Based services (ProSe) Stage 2 (Rel. 14), V14.1.0', December 2016
- [21] Li, Z., Shen, H.: 'Game-theoretic analysis of cooperation incentive strategies in mobile *Ad Hoc* networks', *IEEE Trans. Mob. Comput.*, 2012, **11**, (8), pp. 1287–1303
- [22] Chen, T., Zhu, L., Wu, F., *et al.*: 'Stimulating cooperation in vehicular *ad hoc* networks: a coalitional game theoretic approach', *IEEE Trans. Veh. Technol.*, 2011, **60**, (2), pp. 566–579
- [23] Sun, J., Chen, X., Zhang, J., *et al.*: 'SYNERGY: a game-theoretical approach for cooperative key generation in wireless networks'. IEEE Conf. on Computer Communications (INFOCOM), Toronto, Canada, April 2014, pp. 997–1005
- [24] Sakr, A.H., Ekram, H.: 'Cognitive and energy harvesting-based D2D communication in cellular networks: stochastic geometry modeling and analysis', *IEEE Trans. Commun.*, 2015, **63**, (5), pp. 1867–1880
- [25] Bao, X., Lin, Y., Lee, U., *et al.*: 'DataSpotting: exploiting naturally clustered mobile devices to offload cellular traffic'. IEEE Conf. on Computer Communications (INFOCOM), Turin, Italy, 2013, pp. 420–424
- [26] Nishiyama, H., Ito, M., Kato, N.: 'Relay-by-smartphone: realizing multihop device-to-device communications', *IEEE Commun. Mag.*, 2014, **52**, (4), pp. 56–65
- [27] Zhang, A., Zhou, L., Wang, L.: 'Security-aware device-to-device communications underlying cellular networks', Springer Briefs in Electrical and Computer Engineering (Springer, 2016, 1st edn.)
- [28] Jiang, L., Tian, H.: 'Secure beamforming in cooperative D2D communications with simultaneous wireless information and power transfer'. IEEE/CIC Int. Conf. on Communications in China (ICCC), Chengdu, 2016, pp. 1–6
- [29] Hadiks, A., Chen, Y., Li, F., *et al.*: 'A study of stealthy denial-of-service attacks in Wi-Fi direct device-to-device networks'. IEEE 11th Consumer Communications and Networking Conf. (CCNC 2014), Las Vegas, USA, January 2014, pp. 507–508
- [30] Haus, M., Waqas, M., Ding, A.Y., *et al.*: 'Security and privacy in device-to-device (D2D) communication: a review', *IEEE Commun. Surv. Tutor.*, 2017, **19**, (2), pp. 1054–1079
- [31] Abd-Elrahman, E., Ibn-khedher, H., Afifi, H., *et al.*: 'Fast group discovery and non-repudiation in D2D communications using IBE'. Int. Wireless Communications and Mobile Computing Conf. (IWCMC), Dubrovnik, Croatia, 2015, pp. 616–621
- [32] Abualhaol, I., Muegge, S.: 'Securing D2D wireless links by continuous authenticity with legitimacy patterns'. 49th Hawaii Int. Conf. on System Sciences (HICSS), Koloa, HI, USA, 2016, pp. 5763–5771
- [33] Abd-Elrahman, E., Ibn-khedher, H., Afifi, H.: 'D2D group communications security'. Int. Conf. on Protocol Engineering (ICPE) and Int. Conf. on New Technologies of Distributed Systems (NTDS), Paris, France, 2015, pp. 1–6
- [34] Shen, W., Hong, W., Cao, X., *et al.*: 'Secure key establishment for device-to-device communications'. IEEE Global Communications Conf. (GLOBECOM), Austin, TX, USA, December 2014, pp. 336–340
- [35] Goratti, L., Steri, G., Gomez, K., *et al.*: 'Connectivity and security in a D2D communication protocol for public safety applications'. 11th Int. Symp. on Wireless Communications Systems (ISWCS), Barcelona, Spain, August 2014, pp. 548–552
- [36] Kwon, H., Kim, D., Hahn, C., *et al.*: 'Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks'. Proc. 9th Int. Conf. on Wireless Algorithms, Systems and Application (WASA), Harbin, China, June 2014, vol. 8491, pp. 267–278
- [37] Wang, J.T., Lin, T.M.: 'Authentication system for device-to-device communication and authentication method therefore', Google Patents, EP Patent App. EP2663051A1, 6 May 2013
- [38] Ometov, A., Orsino, A., Militano, L., *et al.*: 'A novel security-centric framework for D2D connectivity based on spatial and social proximity', *Comput. Netw.*, 2016, **107**, pp. 327–338
- [39] Shen, W., Yin, B., Cao, X., *et al.*: 'Secure device-to-device communications over Wi-Fi direct', *IEEE Netw. Mag.*, 2016, **30**, (5), pp. 4–9
- [40] Al-Riyami, S., Paterson, K.: 'Certificateless public key cryptography', in Lai, C. (Ed.): 'Advances in Cryptology – ASIACRYPT 2003: 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 – December 4, 2003. Proceedings' (Springer, Berlin, Heidelberg, 2003), vol. **2894**, pp. 452–473
- [41] Tata, C., Kadoch, M.: 'Secure network coding based data splitting for public safety D2D communications over LTE heterogeneous networks'. Proc. 14th IEEE Int. Conf. on Computer and Information Technology (CIT'14), Spain, 2014, pp. 243–248
- [42] Tata, C., Kadoch, M.: 'Secure multipath routing algorithm for device-to-device communications for public safety over LTE heterogeneous networks'. 3rd Int. Conf. on Future Internet of Things and Cloud, Rome, 2015, pp. 212–217
- [43] Steri, G., Baldini, G., Fovino, I.N., *et al.*: 'A novel multi-hop secure LTE-D2D communication protocol for IoT scenarios'. 23rd Int. Conf. on Telecommunications (ICT), Thessaloniki, Greece, 2016, pp. 1–6
- [44] Jung, Y., Festijo, E., Peradilla, M.: 'Joint operation of routing control and group key management for 5G *ad hoc* D2D networks'. Int. Conf. on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, May 2014, pp. 1–8
- [45] Huang, J., Sun, Y., Xiong, Z., *et al.*: 'Modeling and analysis on access control for device-to-device communications in cellular network: a network calculus based approach', *IEEE Trans. Veh. Technol.*, 2016, **65**, (3), pp. 1615–1626
- [46] Yue, J., Ma, C., Yu, H., *et al.*: 'Secrecy-based access control for device-to-device communication underlying cellular networks', *IEEE Commun. Lett.*, 2013, **17**, (11), pp. 2068–2071
- [47] Huang, J., Xiong, Z., Li, J., *et al.*: 'A priority-based access control model for device-to-device communications underlying cellular network using network calculus'. Proc. 9th Int. Conf. on Wireless Algorithms, Systems, and Applications (WASA 2014), Harbin, China, June 2014, vol. 8491, pp. 613–623

- [48] Xi, W., Li, X., Qian, C., *et al.*: 'KEEP: fast secret key extraction protocol for D2D communication'. IEEE 22nd Int. Symp. of Quality of Service (IWQoS), Hong Kong, China, May 2014, pp. 350–359
- [49] Zhu, D., Swindlehurst, A., Fakoorian, S., *et al.*: 'Device-to-device communications: the physical layer security advantage'. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), Florence, Italy, May 2014, pp. 1606–1610
- [50] Zhang, H., Wang, T., Song, L., *et al.*: 'Radio resource allocation for physical-layer security in D2D underlay communications'. IEEE Int. Conf. on Communications (ICC 2014), Sydney, NSW, June 2014, pp. 2319–2324
- [51] Wang, J., Li, C., Wu, J.: 'physical layer security of D2D communications underlying cellular networks', *Appl. Mech. Mater.*, 2014, **441**, pp. 951–954
- [52] Jayasinghe, K., Jayasinghe, P., Rajatheva, N., *et al.*: 'Physical layer security for relay assisted MIMO D2D communication'. IEEE Int. Conf. on Communication Workshop (ICCW), London, 2015, pp. 651–656
- [53] Ma, C., Liu, J., Tian, X., *et al.*: 'Interference exploitation in D2D-enabled cellular networks: a secrecy perspective', *IEEE Trans. Commun.*, 2015, **63**, (1), pp. 229–242
- [54] Sun, L., Du, Q., Ren, P., *et al.*: 'Two birds with one stone: towards secure and interference-free D2D transmissions via constellation rotation', *IEEE Trans. Veh. Technol.*, 2016, **65**, pp. 8767–8774
- [55] Zhang, R., Cheng, X., Yang, L.: 'Joint power and access control for physical layer security in D2D communications underlying cellular networks'. IEEE ICC2016 Communication and Information Systems Security Symp., Kuala Lumpur, Malaysia, 2016, pp. 1–6
- [56] Zhang, K., Peng, M., Zhang, P., *et al.*: 'Secrecy-optimized resource allocation for device-to-device communication underlying heterogeneous networks', *IEEE Trans. Veh. Technol.*, 2017, **66**, (2), pp. 1822–1834
- [57] Bourrous, A., Iacobelli, L.: 'URA-MAC a new strategy for D2D communications'. IEEE Conf. on Standards for Communications and Networking (CSCN), Berlin, Germany, 2016, pp. 1–6