Security in Device-to-Device communications (D2D): a survey

Othmane Nait Hamoud, Tayeb Kenaza, Yacine Challal

Security in Device-to-Device communications (D2D): a survey

Othmane NAIT HAMOUD, Tayeb KENAZA, Yacine CHALLAL

***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 type of communication, especially when it comes to wireless communication. In this paper, we propose taxonomy based on the review of recent works which have addressed the security issues in D2D communications.**

I. 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 for the cellular infrastructure in terms of spectrum utilization, overall throughput, communications delays and energy consumption.

Expecting to be one of the technology components of the evolving 5G architecture, Device-to-Device (D2D) communications is promising solution to offload the cellular infrastructure from the traffic encumbrance. Indeed, D2D communications approach allows device users (device such Smartphone, 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 device-centric network architecture contrary to the previous generations which have been network centric. In 5G, device user is expected to actively perform operations which were earlier being performed by the network such as storage, relaying and content delivery [15].

Academicians, industrials, and standard institutions have paid considerable attention for D2D communications technology. In academia, different surveys have been proposed in the literature [1, 2, 15] in which, different fields related to this technology was 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 [3] 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 licensed cellular band based on Time Division Duplexing-Orthogonal Frequency Division Multiple Access technology (TDD-OFDMA) which is the same as LTE-A system, allowing devices to discover neighbors in a large range with high efficiency.

The work of standardizing this new paradigm is underway by the Third Generation Partnership Project (3GPP) under the proposal Proximity Services (ProSe) [8] which allows enabling direct communication between proximate devices. ProSe combines two types of services, proximity discovery and direct communication. In [4], a brief overview of standardization activities of the 3GPP ProSe in LTE-A is presented.

Security issues must be considered in all type of communication, especially when it comes to wireless communication. Despite a very rare works, security in D2D communication is not seriously and well handled in the literature. D2D communications face many security challenges when it will applied to the future 5G systems.

II. Overview of D2D communications

Initially, direct communications were introduced in the third generation networks (3G) within the wireless personal network (WPAN) and wireless local area network (WLAN) technologies. These technologies occurred on unlicensed band which didn’t provide Quality of Service (QoS) guarantees due to the uncontrollable interference. In spite of the role which can play D2D paradigm to enhance performance of cellular networks, cellular operators did not pay attention to D2D communications because of the limited benefits of local communications services. However, with the growth of traffic due especially to the increasingly 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 [3].

A. *Scenarios and use cases*

Different scenarios and use cases were proposed by 3GPP in [64]. Depending on the degree of implication of a Cellular Network Operator (CNO) in D2D communications, three typical scenarios and use cases are shown in Figure 1.

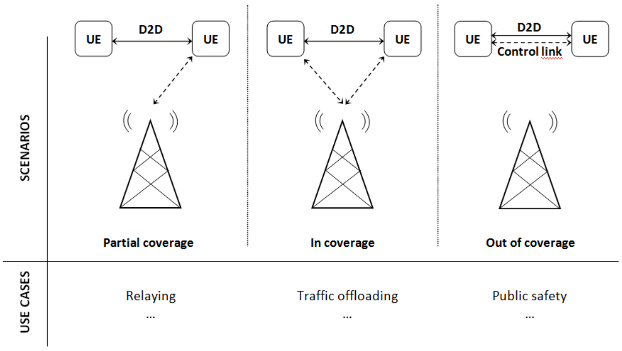

Figure1. Typical scenarios and use-cases in D2D communications.

1. *In coverage* scenario where 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 (video streaming of football match), this later will transmit the content to 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 in nowadays and allow companies to target clients in a specific geographic location with multiple and attractive services (advertising). Through D2D links, such type of networks can be more efficient.
2. *Partial coverage* scenario where 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 had previously made the facilities impossible to justify.
3. *Out of coverage* scenario where 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, terrorism attacks, etc.

In the literature, different works have investigated potential D2D use cases such as traffic offloading [23, 55], social networking [23, 46, 47], smart media sharing [25, 33, 46], intermittent cellular connectivity [26, 29, 55], extended coverage [8, 36, 10], disaster rescue [40].

B. System architecture

Before presenting the system architecture of the D2D communications, we present the basic architecture of the core network of 3GPP's LTE wireless communication standard, the Evolved Packet System (EPS). The main component of the EPS is the Evolved Packet Core (EPC). Figure 2 illustrates a basic architecture of the EPS in which, a UE is connected to the EPC over a Radio Access Network technology (RAN). In order to make the scaling independent, it was decided to separate in the EPC the user plane (data) and the control plane (signaling).

3GPP has proposed D2D communication (ProSe) as an underlay network of existing LTE-A networks [60]. 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) ProSe application server which serves UEs requesting ProSe services through a logical link. Figure 3 shows 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 [61]: (1) ProSe Discovery (ProSe-D), which identifies that ProSe-enabled UEs are in proximity using E-UTRA 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 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.

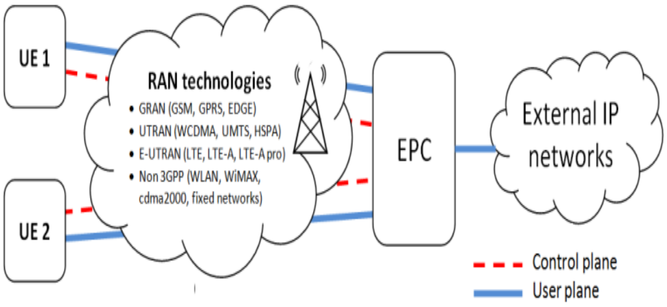
UE 1
UE 2
RAN technologies
• GRAN (GSM, GPRS, EDGE)
• UTRAN (WCDMA, UMTS, HSPA)
• E-UTRAN (LTE, LTE-A, LTE-A pro)
• Non 3GPP (WLAN, WiMAX, cdma2000, fixed networks)
EPC
External IP networks
Control plane
User plane

Figure 2. The basic architecture of the EPS in 3GPP.

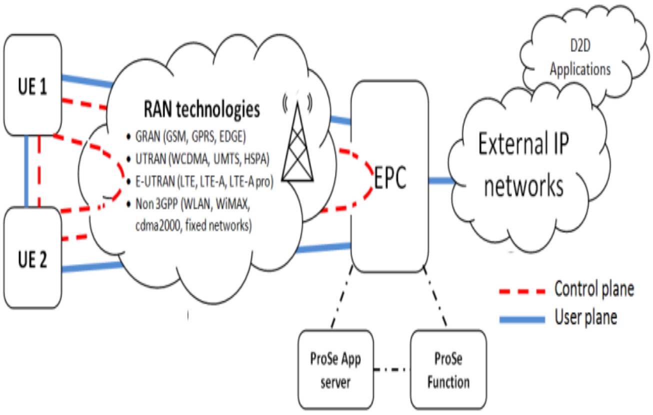

Figure 3. The basic architecture of the ProSe underlaying 3GPP's EPS.

C. Classification

D2D communications may be the bridge between ad hoc networks and centralized networks. On one hand, they may integrate into their ad-hoc aspect other promising techniques such as cooperative communication [10, 11, 38, 47] and cognitive radio [16, 17] in order to enhance spectrum efficiency. On another hand, the centralized aspect of cellular networks may resolve interference issues.

The D2D communication can occur either on operator's licensed spectrum (underlying LTE-A networks) or unlicensed spectrum (Bluetooth, WiFi-Direct). Authors in [1] proposed taxonomy based on the D2D communication spectrum and reviewed the available literature under the proposed taxonomy.

In the licensed band, D2D communications cohabit with cellular ones 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 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 device user controls the D2D communication interface in autonomous unlicensed D2D communication. Simultaneous cellular and D2D communications can be made by a device user in this category.

In the following we propose a revised classification which highlights the hybridization and flexibility of D2D communication techniques, compared to available other techniques. The classification we proposed (Fig 4) is more practical to understand 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 the 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 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 another hand, from the point of view of context and scenario in which they are applied.

Through this classification, we can imagine a brunch of solutions, depending on the context and the situation in which, D2D communication will be utilize. For example, in order to offload cellular traffic through D2D links, DataSpotting [62] adopted a hybrid mode of spectrum allocation (in band and out band). The system uses licensed band to control channel for all the setup procedures until activating both the content requester and provider into WiFi ad-hoc mode. Cellular operator assists UE only in neighborhood discovery. Under the assistance of an eNB, FlashLinQ works over 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 [63]. According to the situation (neighbor node density, mobility pattern, remaining battery power, etc.), a smartphone could switch between MANT operation mode and DTN operation mode in the message delivery process in such a way that the overall message delivery performance is improved.

In a centralized 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. By comparison, 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.

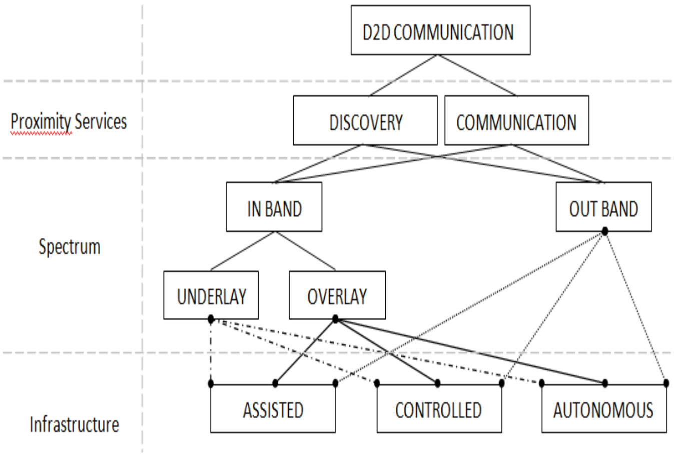

Figure 4. Classification of D2D communications.

III. Security in D2D communications

This section treats security threats and requirements in D2D communications.

A. Security threats

The radio nature of D2D communications introduces various security threats [33] [6]. The main threats are:

- *Eavesdropping attack*: an attacker passively listens to the radio channel between UE devices in order to get sensitive data. Data confidentiality in the cryptography approach can parry this threat.
- *Impersonate attack*: an attacker can pretend to be a legitimate UE device or eNB to get access to the traffic data. Authentication in the cryptography approach can parry this threat.
- *Forge attack*: an attacker may forge the content and send the fake data to the rest of UEs, which prejudices the system. Data integrity (digital signature) in the cryptography approach can parry this threat.
- *Free-riding attack:* in order to reduce system availability in D2D communications, an attacker may encourage selfish behavior 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 Quality of Experience (QoE) thus irritates user experiences and hinders the adoption of D2D communications. To resist such an attack, it is necessary to develop a cooperation stimulation mechanism [10, 11, 38, 47, 59].
- *Active attack on control data*: an attacker tries to change the control data. Authentication, confidentiality and integrity in the cryptography approach can parry this threat.
- *Privacy violation*: some privacy-sensitive data such as identity, location, etc. are more concerned by D2D services functionalities, so this personal information must be concealed to non-authorized parties.
- *Denial-of-Service (DoS) attack*: it consists of rendering up unavailable a service in D2D

communications. In [42], authors has shown via experimental study about exploration on characteristics of DoS attacks on Android devices in D2D underlaying network environment that malicious devices can stealthily impair or even totally block the connection of legitimate devices in the underlaying network.

B. *Security requirements*

Due to the aforementioned threats, a secure D2D communications system should fulfill the following security requirements [20] [33] [6], whether they are assisted, controlled or autonomous:

- *Authentication*: identification of communicating parties must to be checked.
- *Data confidentiality*: transmitted data between devices must be secret using encryption mechanisms.
- *Data integrity*: data transferred by authorized 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 be able to identify the source identity of false messages. In [21], authors consider the given conflicting goals between privacy and traceability.
- *Anonymity:* communicating UEs may be anonymous to each other and from an adversary.
- *Non-repudiation*: refers to the ability to prevent UEs from denying transmission or reception of a message. In cryptography approach, digital signature is an efficient tool to prevent from transmission non-repudiation, while 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 reprieve user privilege of a D2D service if it is detected as malicious.
- *Fine-grained Access Control (FAC)*: takes into account small granularity of an access rule specified to a UE when accessing in its service. It's seen as an effective solution to overcome privacy and data transmission security issues.

IV. TAXONOMY ON D2D SECURITY SOLUTIONS

A general approach to address security issues in D2D communications can be based on network layers on which security is concerned. From this point of view, a complete security solution can be designed to provide a complete protection for the devices involved in D2D communications. Such a solution must be based on security protocols built on each layer which will be called upon to cooperate together. 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.

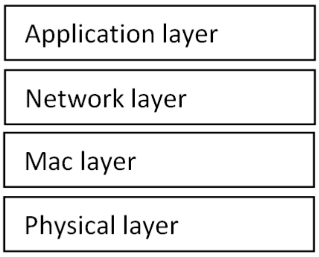

Figure 5. Classification of D2D communications.

A. *Application layer*

In this layer, key management scheme is considered as the foundation of any solution based on cryptography. Various solutions have been proposed in literature [21-23, 25, 33-25, 39, 40, 48] (Table.1).

Recently, Abd-Elrahman et al. [21] proposed a solution based on the Identity-Based Encryption (IBE) and Elliptic Curve Cryptography (ECC) mechanisms for key generation to secure the exchanged messages during the discovery and communication phases. The proposed solution is discussed under two D2D use cases (same operator and different 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 D2D aspect in same and different operators' use cases. Authors proposed also in [22] a Group Key Management (GKM) mechanism for the same purpose as in [21]. In this work, they used multiple Private Key Generators (PKGs) which is more suitable for different operators' use case than a single one as proposed in [21].

In [23], three key exchange protocols for secure network assisted D2D communication in a cellular network are proposed. These protocols are based on the standard Diffie-Hellman based key exchange, but they differ in the role of 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 (SeDS) for D2D communications in LTE-A network based on symmetric and asymmetric encryption [33]. Authors consider media sharing scenario for the ease of the understanding which can be extended to be more general ones. The involvement of EPC is assured by a gateway which serves as the gate from the local subsystem to the core network. In order to completely offload the cellular network, authors proposed an interesting idea in [6] but which has not been investigated yet. The idea introduces Certificate Less Public Key Cryptography (CL-PKC) [9] to secure D2D communications.

In order to enable two UEs to establish a secret key to secure D2D communications without prior knowledge or involvement of EPC, Shen et al. proposed in [34, 53] a key agreement protocol based on the Diffie-Hellman (DH) key exchange and a commitment schemes.

Works	Network Assisted Mode			Ad-Hoc Mode	Purpose, scenario or application	Techniques Based	Security Require.	Resisted Attacks	Imple.	Simul.
	In Cover.	Relay	EPC Involve.							
[21]	**Yes**	No	**Yes**	No	**Key Management:** - Same operator - Different operator	IBE-ECC ECDH	N.-repud + C-I Privacy Anonymity PFS-PBS	Reply Imperson. Man in the middle	No	MIRACL
[22]	**Yes**	No	**Yes**	No	**Key Management:** - Same operator - Different operator - Hierarchical groups	IBE-ECC ECDSA	N.-repud + C-I Privacy Anonymity PFS-PBS Key revoc.	Key escrow Identity disclosure	No	MIRACL
[23]	**Yes**	No	No	No	**Key Management:** - Traffic offload - Social network	- Diffie Hellman	-	Man in the middle Brute Force	No	Matlab
[25]	**Yes**	No	**Yes**	No	Smart media sharing Business model	-	-	-	No	No
[26]	**Yes**	**Yes**	**Yes**	**Yes**	Scenario: assisted offloading traffic Intermittent cellular connectivity Construct secure coalition	PKI	-	-	No	No
[27]	**Yes**	**Yes**	**Yes**	**Yes**	Scenario: extended coverage and disseminate content Game theoretic clustering	PKI	-	-	OpenSSL	Matlab WINTERsim
[29]	**Yes**	**Yes**	**Yes**	**Yes**	Intermittent cellular connectivity Construct secure coalition	Shamir Secret Scheme	-	-	Yes Testbed	No
[55]	**Yes**	**Yes**	**Yes**	**Yes**	Scenario: assisted offloading traffic Intermittent cellular connectivity Game theoretic clustering	PKI			No	Yes
[46]	-	-	-	-	Social networking Media sharing (traffic offload)	- Exploiting the social ties and influence among individuals - Indian Buffet Process	Privacy	-	No	Yes
[47]	-	-	-	-	Application : Social networking Scenario : relaying and coverage extension Purpose: Enhance cooperative D2D communications	Social trust based relay selection Social reciprocity based relay	-	-	No	Yes
[33]	**Yes**	No	**Yes**	No	Scenario: Media sharing (traffic offload)	PKI + Symmetric encryption Bilinear Pairing DHKE	Confidentiality Intergerity Authentication Privacy Non-repu. Availability	Eavesdropping Alteration Privacy DoS attack Free-riding	No	Yes
[34] [53]	No	No	No	**Yes**	Authentication and key agreement	- Diffie Hellman - Commit. scheme	-	Man in the middle	WiFi-D Android	No
[35]	No	No	No	**Yes**	Public Safety	Probabilistic Key Management scheme	-	-	No	No
[39]	No	No	No	**Yes**	Multi hop D2AribtraryDevice and D2GroupD D2SpecificD_in_Group	Cipher text Policy-ABE Bluetooth auth. protocol	Man in the middle Replay Alteration	**Yes**	No	-
[40]	**Yes**	**Yes**	**Yes**	**Yes**	Scenario 1: Traffic offload (key distribution) Scenario 2: Social networking (auth. & k.d.) Scenario 3: Disaster rescue (node disc.& k.d)	-	-	No	No	More complicated scenarios
[48]	**Yes**	No	**Yes**	No	Authentication and key agreement	PKI Shared Master key	-	-	-	-
[42]	**Yes**	-	-	**Yes**	Studying impacts of Denial-of-Service (DoS) attacks in a D2D underlaying network	-	-	Yes	-	Testing speed impact and developing detection/counterm easure schemes.

Table 1. Application layer.

In [35], a probabilistic key management scheme was derived from wireless sensor networks (WSN) and employed to secure D2D communications for a public safety scenario. In [39], 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. in [40] have reused existing security solutions of LTE-A technology in order to secure D2D communication for three types of scenario: 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. [48], 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 mobile social network is a challenging work to construct social trust and social ties promoting efficient cooperation with privacy preservation among users. Many works have focused on security aspect of social networking [26, 27, 29, 46, 47]. Ometov et al. proposed in the context of a network-assisted D2D communication two solutions to maintain and extend the secure D2D operation in case of unreliable cellular connectivity [26, 27]. 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 [26], authors' target scenario consists on the assisted offloading of devices' cellular data flows onto their WiFi-Direct sessions. Cellular links are used by devices only for transferring signaling information and to communicate with the PKI functions and establish a logical group of securely-commutating 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 unreliable cellular network. In order to trial this theoretical solution, an implementation of secure network-assisted D2D framework in live 3GPP LTE deployment was proposed in [29].

In [27], authors' target scenario consists on providing additional coverage for users that are facing intermittent cellular connectivity and thus helping disseminate content to larger numbers of device users. Coalition formation (clustering) in this work is based on game theoretical framework where social proximity (relationships among users) and spatial proximity (effect of cellular transmissions) are considered explicitly. Orsino et al. [55] adopted a game-theoretic optimization approach to secure throughput optimized communications in D2D-assisted cellular system.

Works	Network Assisted Mode			Ad-Hoc Mode	Purpose, scenario or application	Techniques Based	Resisted Attacks	Imple.	Simul.
	In Cover.	Relay	EPC Involve.						
[24] [31]	No	No	No	**Yes**	Public safety D2D Com. over LTE HetNets Routing over butterfly network	-Network coding -Coded matrix -Data splitting mechanism	Eavesdropping	No	Matlab
	No	No	No	**Yes**	Routing for public safety over LTE HetNet	- Multipath coded inform. Trans. - Data splitting scheme - Data shuffling scheme	Eavesdropping	No	Matlab
[28]	**Yes**	**Yes**	**Yes**	**Yes**	Multihop D2D com. between LTE-A UEs as enabler of IoT scenarios. Scenario : relaying and coverage extension	- Probabilistic scheme - Direct beacon	-	No	Yes
[36]	No	No	No	**Yes**	Routing	Game theory Confusion matrices	Malware	No	Yes
[43]	**Yes**	**Yes**	**Yes**	**Yes**	Scenario: Deal with local traffic = traffic offload Purpose: secure joint operation (Routing)	PKI Group key agreement	-	No	Yes

Table 2. Network layer.

Chen et al. studied in [47] 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 relay for others in the same cycle. In [46], authors proposed a novel social-aware approach for optimizing D2D communication based on social network and physical wireless network layers.

Authors in [42] studied the impacts of Denial of Service (DoS) attacks in a D2D underlaying network. Authors' experiments have shown how attacks can force UE to lose the WiFi connection with the access point without being detected by the AP or the cellular network. The goal of this work was to inspire deeper study and more efforts in this field.

In order to offload cellular traffic without increasing the infrastructure cost, the work in [25] 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.

B. *Network layer*

D2D communications can be used in a disaster rescue (earthquake) when network infrastructure becomes absent [33]. In this scenario, devices can play an important role in relaying D2D communications over public safety network which require secure communications. Moreover, secure multi-hop D2D communications can contribute to anonymity against cellular operators [24, 31, 28, 36, 43] (Table 2).

Tata et al. proposed Secure Network Coding based Data Splitting and Data Shuffling algorithm to secure routing for public safety D2D communications over LTE Heterogeneous Networks (HetNets) without adding additional control traffic [24]. In order 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 proposed another approach for secure D2D routing if unable to apply network coding transmissions within LTE small cells [31]. The proposed algorithm called Secure Load Balancing Selective AOMD (LBS-AOMDV) is based on a multipath coded information transmissions, data splitting, and data shuffling schemes.

In the context of IoT scenario, the work in [28] 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. proposed in [36] Secure Message Delivery protocol to choose the most secure path to deliver a message from a sender to a destination in 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 [43]. To offload the cellular network from the local traffic, the UE is assumed acting in a way that it cans response to either infrastructure or ad hoc D2D communications requirements. So, authors' idea is based on that the dual operation of 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 self-managed group of ad hoc nodes based on their home IP address wherever they move. The authentication process is based on the PKI of the cellular network.

C. *MAC layer*

Access control is an important component in D2D communications security. In out of coverage network extension or public safety scenarios, UEs have to become eligible to replace the role of the base station in term of resource allocation and controlling signal [14]. On another 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 [54]. 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 [45].

Other works considered an access control issue under the framework of multi-priority model which assigns highest priority to cellular users and multiple levels of priority for D2D ones [44, 49], where Network Calculus theory was employed to model and analyze the access control for D2D communications underlaying cellular networks. Besides, access control can be used as a solution to preserve location and identity privacy in D2D communications [20].

Works	Network Assisted Mode			Ad-Hoc Mode	Purpose, scenario or application	Techniques Based	Resisted Attacks	Imple.	Simul.
	In Cover.	Relay	EPC Involve.						
[44]	-	-	-	-	Access control	Multi priority model Network calculus theory	-	-	-
[45]	-	-	-	-	Access control	CSI Secrecy outage probability	Eavesdropping	-	-
[49]	-	-	-	-	Access control not dealing with security	Multi priority model Network calculus theory	-	-	-
[32]	-	-	-	-	Developing a security-scoring measure Detecting Physical layer attacks	Continuous authenticity Legitimacy patterns	-	No	Yes
[37]	No	No	No	**Yes**	Establish a share secret key between two communication entities	Extraction from CSI Validation-recombination mechanism	Eavesdropping	Yes	No
[38]	No	No	No	**Yes**	Key management Multi hop	Extraction from CSI Game theoretical approach for Cooperative Key Generation	Eavesdropping	No	Matlab
[41]	No	No	No	**Yes**	Improving security at the physical layer	CSI Secrecy outage probability	Eavesdropping		
[50]	-	-	-	-	Physical layer security	System secrecy capacity *Kuhn-Munkres* algorithm	-	-	Yes
[51]	**Yes**	No	No	No	Physical layer security	D2D resource allocation	Eavesdropping		
[54]	**Yes**	No	No	No	Physical layer security	D2D resource allocation scheme based on stochastic geometry	Eavesdropping	-	-
[56]	**Yes**	No	No	No	Physical layer security	Constellation-rotation technique	Distrust between cellular and D2D users	-	Yes
[57]	**Yes**	No	No	No	Physical layer security	System secrecy capacity	Eavesdropping	-	Yes
[58]	**Yes**	No	No	No	Physical layer security	System secrecy capacity	Eavesdropping	-	Yes

Table 3. MAC and network layer.

D. *Physical layer*

Developing security features at physical layer lead to enforce the security of upper layers and thus improve overall D2D communications. Chanel State Information (CSI) which refers to known channel properties of a wireless link can serve to extract secret keys from the measurement of physical layer. Recently, various CSI-based key extraction works have been proposed to secure D2D communications [32, 37, 38, 41, 50, 51]. Xi et al. proposed in [37] 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 OFDM subcarriers. The protocol achieves high security level against eavesdropping and predictable channel attacks. Authors in [38] studied 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-interesting nodes which are reticent to act as relays.

In order to emphasize instead the enforcement security that D2D paradigm can achieve via the physical layer, authors in [41] derived the secrecy outage probability (SOP) for the D2D and cellular networks and compare performance for D2D scenarios in the presence of multi-antenna eavesdropper. Zhang et al. considered in [50] physical-layer security in D2D underlaying 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 physical layer security was proposed, in which a power and subcarrier allocation scheme maximizes the D2D security capacity without influencing the cellular user’s basic capacity. Jayasinghe et al. designed a secure beamforming technique to prevent eavesdropping on MIMO D2D communication via trusted relay which performs physical layer network coding [52].

Authors in [54] considered a large-scale D2D-enabled cellular network with presence of eavesdroppers overhearing cellular communications which was modeled using stochastic geometry. In order to guarantee performances of secure cellular communications, they proposed strong and weak performance guarantee criteria. In [56] a security-embedded interference avoidance scheme was proposed based on the concept of constellation-rotation which provides an inherent secrecy protection at the physical layer for both D2D and cellular users. Authors in [57] investigated the physical layers security issue in D2D communications underlaying cellular networks from a joint optimization perspective. They proposed a secrecy-based joint power and access control scheme with optimum D2D pair selection mechanism for cellular communication links and D2D pairs. Zhang et al. proposed in [58] a radio resource allocation solution which improves the secure capacity of D2D users underlaying 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 involved devices in D2D communications.

V. Discussion

By reviewing many of 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 related to the application layer have treated cryptographic key management issues in order to apply them in 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 so on. Proposed solutions in the literature didn’t assume all scenarios related to the involvement of cellular infrastructure (i.e. assisted, controlled or autonomous), all the more difficulties concern keys distribution and revocation problems. It is judicious to reuse security solutions ensured by a cellular infrastructure, but in the same time theses solutions may work in case of out of coverage scenario.

In out of coverage scenario, techniques used in the proposed key management schemes are inspired from those used on the context of Wireless Sensor Networks (WSN) and Mobile Ad-hoc Networks (MANET), such as Diffie-Hellman based key exchange, IBE-ECC, CP-ABE and probabilistic key management schemes. However, D2D communications may gain advantage from the controlling or assistance of a cellular infrastructure by getting necessary credentials to be employed in case of intermittent cellular connectivity or out of coverage scenario. On the other side, local social networks have attracted increasing attentions from researchers in recent years. In order 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 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 of the topology on one hand; and on another hand to preserve security and privacy of users which will seen their sensitive information transit different nodes without trust authority. Besides, malicious contents can be injected into the D2D network and affect UEs with viruses, malwares and so on. Secure D2D routing through a cryptography approach needs manipulating cryptographic keys in such a way key management schemes may 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 for securing wireless communications in recent years. It exploits physical characteristics of wireless channel to prevent essentially from eavesdropping attack without utilizing cryptographic approaches. Works related to this field turn around theoretic secrecy capacity, CSI-based authentication and CSI-based key agreement.

VI. Conclusion

D2D is 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 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. We are interesting in this paper to underline the necessity to develop a security solution which fulfills all security requirements, faces all security threats and supports all D2D communication scenarios. Thus, significant efforts must be provided in order to overcome seriously D2D security problems.

References

[1] A. Asadi, Q. Wang, and V. Mancuso, “A survey on Device-to-Device communication in cellular networks,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1801-1819, April 2014.

[2] J. Liu, N. Kato, J. Ma and N. Kadowaki, “Device-to-Device communication in LTE-Advanced networks: A survey,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 1923-1940, December 2015.

[3] X. Wu, S. Tavildar, S. Shakkottai, T. Richardson, J. Li, R. Laroia, and A. Jovicic, “FlashLinQ: A synchronous distributed scheduler for peer-to-peer ad hoc networks,” IEEE/ACM Transactions on Networking, vol. 21, no. 4, pp. 1215-1228, June 2013.

[4] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, “An overview of 3GPP device-to-device proximity services,” *IEEE Communications Magazine*, December 2013.

[5] M. Wang, Z. Yan, “A survey on security in D2D communications,” in Mobile Networks and Applications, 2016. DOI10.1007/s11036-016-0741-5.

[6] A. Zhang et al., “Security-aware Device-to-Device Communications Underlaying Cellular Networks,” in SpringerBriefs in Electrical and Computer Engineering, 2016. DOI 10.1007/978-3-319-32458-6_5.

[7] FCC, Public Safety & Homeland Security Bureau, http://publicsafety.fcc.gov/pshs/public-safety-spectrum/index.htm.

[8] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study for Proximity Services (ProSe) (Rel 12), 3GPP TR 22.803 V1 2.2.0 (2013-06).

[9] Al-Riyami S, Paterson K, “Certificateless public key cryptography,” Advances in cryptology-ASIACRYPT. Lecture notes in computer science, vol 2894. Springer, New York, pp 452–473, 2003.

[10] Li Z, Shen H (2012) Game-Theoretic analysis of Cooperation incentive strategies in mobile Ad Hoc networks. IEEE Trans Mob Comput 11(8):1287–1303.

[11] Chen T, Zhu L, Wu F, Zhong S (2011) Stimulating cooperation in vehicular ad hoc networks: a coalitional game theoretic approach. IEEE Trans Veh Technol 60(2):566–579.

[12] Pimmy Gandotra and Rakesh Kumar Jha, Device-to-device communication in cellular networks: A survey, Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2016.06.004

[13] G. Fodor et al., “Design Aspects of Network Assisted Device-to-Device Communications,” IEEE Commun. Mag., vol. 50, no. 3, Mar. 2012, pp. 170–77.

[14] A. Bourrous, L. Iacobelli, “URA-MAC a new strategy for D2D communications,” in 2016 IEEE Conference on Standards for Communications and networking (CSCN). DOI: 10.1109/CSCN.2016.7785186.

[15] P. Gandotra, R. K. Jah, and S. Jain, “A survey on device-to-device (D2D) communication: architecture and security issues,” Journal of Network and Computer Applications 78 (2017), pp. 9-29.

[16] Sakr, Ahmed Hamdi, and Ekram Hossain. "Cognitive and energy harvesting-based D2D communication in cellular networks: Stochastic geometry modeling and analysis." *Communications, IEEE Transactions on* 63.5 (2015): 1867-1880.

[17] Liu, Jiangchuan, et al. "Device-to-device communication in LTE-advanced networks: a survey.", IEEE Communications Surveys and Tutorials, Volume 17, 2014.

[18] Y. Meng, C. Jiang, H. Chen and Y. Ren, “Cooperative Device-to-Device communications: Social networking perspectives”, in *IEEE Network* Volume PP, Issue 99, 2017.

[19] A. S. M. Ghanem, and M. Ara, “Secure communications with D2D cooperation”, in *Communications, Signal Processing, and their applications (ICCSPA), 2015 International Conference on,* Sharjah, 2015, pp. 1-6. Doi: 10.1109/ICCSPA.2015.7081278.

[20] M. Haus, M. Waqas A. Y. Ding Y. Li, S. Tarkoma and J, Ott, “Security and privacy in Device-to-Device (D2D) communication: a review”, *IEEE Communications Surveys & Tutorials*, vol. PP, no. 99, pp. 1-1, doi: 10.1109/COMST.2017.2649687.

[21] E. Abd-Elrahman, H. Ibn-khedher, H. Afifi and T. Toukabri, “Fast Group Discovery and Non-Repudiation in D2D Communications using IBE”, in the proceeding of IWCMC 2015, Security Symposium - Wireless Communications and Mobile Computing 2015.

[22] E. Abd-Elrahman, H. Ibn-khedher and H. Afifi, “D2D Group Communications Security,” in international Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015.

[23] R. Sedidi, and A. Kumar, “Key Exchange Protocols for Secure Device-to-Device (D2D) Communication in 5G,” in Wireless Days 2016.

[24] C. Tata and M. Kadoch, “Secure Network Coding based Data Splitting for Public Safety D2D Communications over LTE Heterogeneous Networks,” (CIT '14). Spain, 2014.

[25] S. Ramasubramanian, S. Chung, L. Ding and S. Ryu, “Secure and smart media sharing based on a novel mobile Device-to-Device

communication framework with security and procedures," in Proc. RIIT'15. 2015, pp. 35-40.

[26] A. Ometov, K. Zhidanov, S. Bezzateev, R. Florea, S. Andreev, and Y. Koucheryavy, "Securing Network-Assisted Direct Communication: The Case of Unreliable Cellular Connectivity," in Proc. of IEEE 14th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2015.

[27] A. Ometov, A. Orsino, L. Militano, G. Araniti, D. Moltchanov and S. Andreev, "A Novel Security-Centric Framework for D2D Connectivity Based on Spatial and Social Proximity," in Computer Networks, 2016. DOI: 10.1016/j.comnet.2016.03.013.

[28] G. Steri, G Baldini, I. N. Fovino, R. Neisse and L. Goratti, "A Novel Multi-hop Secure LTE-D2D Communication Protocol for IoT Scenarios," in 23rd International Conference on Telecommunications (ICT) 2016.

[29] A. Ometov, P. Masek, J. Urama, J. Hosek, S. Andreev and Y. Koucheryavy, "Implementing Secure Network-Assisted D2D Framework in Live 3GPP LTE Deployment," in IEEE ICC2016-Workshops: W10-Eighth Workshop on Cooperative and Cognitive Networks (CoCoNet8).

[30] W. Aldosari and T. El Taeib, "Secure Key Establishment for Device-To-Device Communications among Mobile Devices," International Journal of Engineering Research and Reviews. Vol. 3, Issue 2, 2015, pp. 43-47.

[31] C. Tata and M. Kadoch, "Secure Multipath Routing Algorithm for Device-to-Device Communications for Public Safety over LTE Heterogeneous Networks," 3rd International Conference on Future Internet of Things and Cloud, Rome, 2015, pp. 212-217. Doi: 10.1109/FiCloud.2015.51.

[32] I. Abualhaol and S. Muegge, "Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns," 49th Hawaii International Conference on System Sciences, 2016. DOI 10.1109/HICSS.2016.713.

[33] A. Zhang, J. Chen, R. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks," IEEE Transactions on Vehicular Technology, vol. PP, no. 99, pp. 1, March, 2015.

[34] W. Shen, W. Hong, X Cao, Bo Yin; D. Shila, and Y. Cheng, "Secure key establishment for Device-to-Device communications," 2014 IEEE Global Communications Conference (GLOBECOM), pp. 336-340, December 2014.

[35] L. Goratti, G. Steri, K. Gomez, and G. Baldini, "Connectivity and security in a D2D communication protocol for public safety applications," International Symposium on Wireless Communications Systems (ISWCS), pp. 548-552, August. 2014.

[36] E. Panaousis, T. Alpcan, H. Fereidooni, and M. Conti, "Secure message delivery games for Device-to-Device communications," Decision and Game Theory for Security, Lecture Notes in Computer Science, vol. 8840, pp. 195-215, November 2014.

[37] W. Xi, X. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "KEEP: Fast secret key extraction protocol for D2D communication," IEEE 22nd International Symposium of Quality of Service (IWQoS), pp. 350- 359, May 2014.

[38] J. Sun, X. Chen, J. Zhang, Y. Zhang, and J. Zhang, "SYNERGY: A game-theoretical approach for cooperative key generation in wireless networks," IEEE Conference on Computer Communications (INFOCOM), pp. 997-1005, April 2014.

[39] H. Kwon, D. Kim, C. Hahn and J. Hur, "Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks." Proceeding of the 9th International Conference on wireless Algorithms, systems and application (WASA), vol. 8491, pp. 267-278, June 2014.

[40] M. Alam, D. Yang, J. Rodriguez, and R. Abd-Alhameed, "Secure device-to-device communication in LTE-A," IEEE Communications Magazine, vol. 52, no. 4, pp. 66-73, April 2014.

[41] D. Zhu, A. Swindlehurst, S. Fakoorian, W. Xu, and C. Zhao, "Device-todevice communications: The physical layer security advantage," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.1606-1610, May 2014.

[42] A. Hadiks, Y. Chen, F. Li, and B. Liu, "A study of stealthy denial-of-service attacks in Wi-Fi direct device-to-device networks," IEEE 11th Consumer Communications and Networking Conference (CCNC 2014), pp.507-508, January 2014.

[43] Y. Jung, E. Festijo, and M. Peradilla, "Joint operation of routing control and group key management for 5G ad hoc D2D networks," International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1-8, May 2014.

[44] J. Huang, Y. Sun, Z. Xiong, Q. Duan, Y. Zhao, X. Cao, and W. Wang, "Modeling and analysis on access control for Device-to-Device communications in cellular network: A network calculus based approach," IEEE Transactions on Vehicular Technology, vol.PP, no.99, pp.1, March 2015.

[45] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for Device-to-Device communication underlaying cellular networks," IEEE Communications Letters , vol. 17, no. 11, pp. 2068-2071, November 2013.

[46] Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy, and Z. Han, "Social Network Aware Device-to-Device Communication in Wireless Networks," IEEE Transactions on Wireless Communications, vol. 14, no. 1, pp. 177-190, January 2015.

[47] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Exploiting Social Ties for Cooperative D2D Communications: A Mobile Social Networking Case," IEEE/ACM Transactions on Networking, vol. 23, no. 5, pp. 1471-1484, October 2015.

[48] J. Wang and T. Lin, "Authentication system for device-to-device communication and authentication method therefore," EP2663051A1, 2013-05-06.

[49] J. Huang, Z. Xiong, J. Li, Q. Chen, Q. Duan, and Y. Zhao, "A Priority-Based Access Control Model for Device-to-Device Communications Underlaying Cellular Network Using Network Calculus," Wireless Algorithms, Systems, and Applications, vol. 8491, pp. 613-623, June 2014.

[50] H. Zhang, T. Wang, L. Song, and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," 2014 IEEE International Conference on Communications (ICC 2014), pp. 2319-2324, June 2014.

[51] J. Wang, C. Li and J. Wu, "physical layer security of D2D communications underlaying cellular networks," Applied Mechanics and Materials vol. 441 (2014) pp 951-954. DOI:10.4028/www.scientific.net/AMM.441.951

[52] K. Jayasinghe, P. Jayasinghe N. Rajatheva and M. Latva-aho, "Physical layer security for relay assisted MIMO D2D communication," IEEE ICC 2015 - Workshop on Device-to-Device Communication for Cellular and Wireless Networks

[53] W. Shen, Bo Yin, X Cao, L. X. Cai and Y. Cheng, "Secure Device-to-Device communications over WiFi Direct," IEEE Network Magazine, pp. 4-9, September/October 2016.

[54] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui and X. Wang, "Interference exploitation in D2D-enabled cellular networks: a secrecy perspective," IEEE Transactions on Communications. Vol. 63, NO. 1, January 2015.

[55] A. Orsino and A. Ometov, "Validation information security framework for offloading from LTE onto D2D links," in proceeding of the 18th Conference of Open Innovation and Seminar on Information Technology (FRUCT-ISPIT), pp. 241-247. DOI: 10.1109/FRUCT-ISPIT.2016.7561534.

[56] L. Sun, Q, Du, P, Ren and Y. Wang, "Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation," IEEE transactions on vehicular technology, vol. 65, pp.8767-8774 (2016).

[57] R. Zhang, X. Cheng, and L. Yang, "Joint power and access control for physical layer security in D2D communications underlaying cellular networks," in IEEE ICC2016 Communication and Information Systems Security Symposium.

[58] K. Zhang, M, Peng, P, Zhang, and X. Li, "Secrecy-optimized resource allocation for Device-to-Device communication underlaying heterogeneous networks," IEEE transactions on vehicular technology, vol 66, no.2, pp. 1822-1834, Feb. 2017. Doi: 10.1109/TVT.2016.2566298.

[59] L. Jiang, and H, Tian, "Secure beamforming in cooperative D2D communications with simultaneous wireless information and power transfer," IEEE/CIC International Conference on Communications in China (ICCC), Chengdu, 2016, pp. 1-6. Doi: 10.1109/ICCChina. 2016.7636833.

[60] 3GPP TR 23.703, "Study on architecture enhancements to support proximity services (ProSe) (Release 12)," V12.0.0, February, 2014.

[61] 3GPP TS 23.303, “Proximity-Based services (ProSe) Stage 2 (Release 14),” V14.1.0, December, 2016.

[62] X. Bao, Y. Lin, U. Lee, I. Rimac, and R. R. Choudhury, “DataSpotting: Exploiting Naturally Clustered Mobile Devices to Offload Cellular Traffic,” in *INFOCOM*, 2013.

[63] H. Nishiyama, M. Ito, and N. Kato, “Relay-by-Smartphone: Realizing Multihop Device-to-Device Communications,” IEEE Communications Magazine, April 2014.

[64] 3GPP TR 22.803, “Feasibility study for proximity services (ProSe), (Release 12),” V12.2.0, June, 2013.