Security in D2D Communications: A Review

Mingjun Wang
The State Key Lab of ISN
Xidian University
Xi'an, China
wangmingjun1987@hotmail.com

Zheng Yan
The State Key Lab of ISN
Xidian University, Xi'an, China
Department of Comnet, Aalto University, Espoo, Finland
zyan@xidian.edu.cn

***Abstract*—Device-to-Device (D2D) communications have emerged as a promising technology for the next generation mobile communication networks and wireless systems (5G). As an underlay network of a conventional cellular network (LTE or LTE-Advanced), D2D communications have shown great potential in improving communication capability, reducing communication delay and power dissipation, and fostering multifarious new applications and services. However, security in D2D communications, which is essential for the success of D2D services, hasn't yet drawn special attention in the literature. In this paper, we analyze security architecture of D2D communications under the framework of 3GPP LTE and identify the security requirements in D2D communications. We survey existing security solutions in D2D communications and evaluate their comprehensiveness and effectivity based on security requirements and D2D security architecture. Finally, we discuss the open research issues for securing D2D communications based on aforementioned security requirements and architecture.**

Keywords—Device-to-Device (D2D) Communications, LTE-Advanced Network, Security, Privacy, 5G.

I. INTRODUCTION

Recent demands on wireless and mobile communications motivate exploring new technologies to improve network performance in terms of overall throughput, spectrum utilization, and energy consumption as a whole. Meanwhile, the appearance of new commercial services such as location-based social networking and content distribution services encourage us to explore new paradigms to meet user demands. Device-to-Device (D2D) communications were proposed as one of the promising technologies for communications in vicinity, which will play a key role in the next generation mobile communication networks and wireless systems (i.e., 5G).

Device-to-Device (D2D) communications refer to a type of technology that enables devices to communicate directly with each other without the involvement of fixed networking infrastructures such as Access Points (APs), Base Stations (BSs), Bluetooth and WiFi-Direct [1]. They occur on the unlicensed Industrial, Scientific and Medical (ISM) spectrum and work in a pure autonomous means. In the past, mobile operators and vendors excluded D2D communications out of universal cellular networks (e.g., Global System for Mobile Communications - GSM, Universal Mobile Telecommunications System - UMTS and Long Term Evolution - LTE) since D2D communications were only envisioned as a technology to reduce the cost of local service provision. On the other hand, appropriate use cases and business models in which mobile operators and vendors can make profits were scarce before. However, the opinion on the usage of D2D communications was changed recently. One typical argument is the D2D communications can play as a controlled or constrained underlay network of LTE-Advanced Networks by operating on the same cellular spectrum [2]. Meanwhile, in order to meet market demands on new services, such as context-aware and proximity services and Machine Type Communication (MTC), mobile operators are exploiting new usage scenarios and new business models based on D2D communications, e.g., pervasive social networking, urgent rescue and location-based services.

As a promising technology, D2D communications have drawn considerable attentions in academia, industry and also in standard organizations in recent years. In academia, D2D communications were regarded as an underlay of LTE-Advanced network from the beginning [2]. Many researchers have paid their attentions on application scenarios, communication mode selection [3][4], resource allocation [5], power control and interference control [6]. In industry, development on D2D communications is active. For example, Qualcomm developed a D2D communication sub-system in cellular networks, known as FlashLinQ [7][8] to make the communications among proximity devices possible. It is expected to complement traditional cellular based networking services and serve as a scalable platform for new types of applications, such as advertising, content sharing, and secure mobile payments. At the same time, the standardization work on D2D communications in the Third Generation Partnership Project (3GPP) is on-going. Different from the general term of D2D communications, 3GPP defined it as Proximity-Based Services (ProSe). Its technical reports [9][10] studied the feasibility of the ProSe in LTE-A and defined its system architecture and the functions of network entities with a number of use cases. The above issues will be further standardized. Moreover, the studies on radio, service and other aspects are underway and will appear in future standardization.

In spite of the significant benefits of D2D communications, new application scenarios expose D2D services into unique security threats. Comparing with conventional connections between devices to a Base Station (BS), the direct connections between proximity devices are more vulnerable due to (1) the limited computational capacity of mobile devices for security related computations; (2) semi- or fully- autonomous security

978-1-4673-7952-6/15 $31.00 © 2015 IEEE
DOI 10.1109/Trustcom.2015.505

management, such as mutual authentication, key arrangement and so on; and (3) a relay transmission structure. These may severely hinder successful deployment of D2D communications in practice. However, neither the academia nor standardization communities have studied the security of D2D communications seriously. In this paper, we perform an extensive review on security in D2D communications. Based on application scenarios and use cases, we explore D2D security architecture and further analysis security issues and requirements based on it. By reviewing exiting work, we analyze open research issues and further propose future research directions in order to highlight the significance of security studies in D2D communications.

The rest of this paper is organized as follows. Section 2 describes a number of typical application scenarios and use cases of D2D communications. In Section 3, we present security architecture of D2D communications and identify security requirements in D2D communications. In Section 4, we further review the state-of-arts of security in D2D communications using the security requirements as a measure to compare existing solutions and analyze their effectivity for D2D communications based on D2D security architecture. Furthermore, we discuss open research issues and propose future research directions in Section 5 and conclude our paper in the last section.

II. Application Scenarios and Use Cases

The application scenarios and use cases of D2D communications have been explored as an underlay of a cellular network or a national security and public safety network. We categorize them into three representative types according to the involvement of various network entities (i.e., cellular base stations and core networks) and the type of utilized spectrum resources, as illustrated in Figure 1.

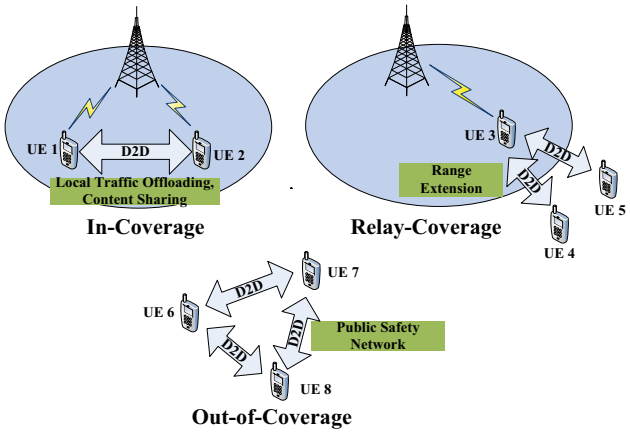

Fig. 1. D2D communication application scenarios and use cases

In-Coverage: in this scenario, user devices (e.g. UE1 and UE2) are located in the coverage of cellular BSs, D2D communications between two user devices are fully controlled by network entities, such as base stations or core networks. The operator controls over user access authentication of D2D communications, connection establishment, resource allocation and security management. This kind of D2D link shares the cellular licensed spectrum with the normal cellular connections (Device-to-Base Station) under the coordination of an operator. Typical use cases of this scenario are local traffic offloading from the core networks and operator controlled local data services, such as local content sharing, machine to machine (M2M) communications.

Relay-Coverage: when a user device (e.g. UE4 and UE5) is at the edge of BS coverage or in a poor coverage area, it can communicate with the BS through relaying its information via other covered devices (e.g. UE3). The introduction of D2D communications can greatly extend the coverage of cellular networks and improve the Quality of Services at a cellular edge. We define this type of D2D communications as "Relay-Coverage" scenario. In this case, like the "In-Coverage" scenario, the operator is fully in charge of link establishment for both BS-to-device link and D2D link, resource allocation (especially for the D2D link) and security management. The band used in the D2D link in this scenario is also the cellular licensed spectrum shared with conventional communications.

Out-of-Coverage: another representative application scenario of D2D communications occurs when the network coverage is absent. A typical use case of "Out-of-Coverage" is Emergence Communication Networks. For example, in an emergent situation where the cellular infrastructure has been partially or completely damaged due to natural disaster (e.g., earthquake or flood), D2D devices (e.g. UE6, UE7 and UE8) can setup connections and start D2D communications autonomously with others in proximity without the control of any operators. As studied in [11][12], this D2D communication scenario can serve as a technical component for providing services such as public protection, disaster relief, national security and public safety. This D2D communication scenario looks similar to Mobile Ad-hoc Networks (MANET). However, their key difference lies in D2D link works on a reserved cellular licensed spectrum for an LTE-based public safety network, while MANET works on unlicensed Industrial, Scientific and Medical (ISM) spectrum, which make it under more severe interference comparing with D2D communications.

III. Security Requirements

In this section, we propose a security architecture in the framework of D2D communications proposed in [10]. Under this security architecture, we discuss the main security requirements that should be fulfilled by D2D communications.

A. Security Architecture

As shown in Figure 2, the 3GPP Committee has defined and introduced two functional entities (ProSe Function and ProSe App Server) and five reference points (PC1, PC2, PC3, PC4, PC5) in an LTE system in order to provide D2D services [10]. ProSe Function has a set of functional modules deployed in the core network. It interacts with Evolved Packet Core (EPC) via reference point PC4, with the ProSe application server via PC2, and with D2D devices (UE) via PC3. The main functionalities of ProSe Function include service configurations for UE, UE discovery, security and trust management and so on. ProSe App Server is an application

server, which provides D2D related application service for users. It can communicate with ProSe Apps (i.e., a mobile app installed in user devices for service provision.) via PC1. D2D devices (UE) can communicate directly with each other via reference point PC5, which is a completely new radio interface introduced by D2D communications.

3GPP has defined five LTE system security levels: (I) Network access security, (II) Network domain security, (III) User domain security, (IV) Application domain security and (V) Visibility and configurability of security. According to these security levels, we propose a high-level security architecture for D2D communications based on LTE system. It includes three different security domains as shown in Fig. 2.

(A) D2D security between 3GPP networks and the ProSe Function/ProSe App Server: it can be divided into two aspects: (A1) Security for D2D between the 3GPP networks and the ProSe Function server that handles PC4 security; (A2) Security for D2D between the 3GPP networks and the D2D ProSe App Server that cooperatively handles the security related to PC2 and PC4.

(B) D2D security between D2D devices and the ProSe Function/App Server: it can be divided into two aspects: (B1) Security for D2D between D2D devices and the ProSe Function server that handles PC3 security; (B2) Security for D2D between D2D devices and ProSe App Server that cooperatively handles the security issues related to PC3 and PC2.

(C) D2D security between D2D devices: herein, we mainly concern the security related to reference point PC5.

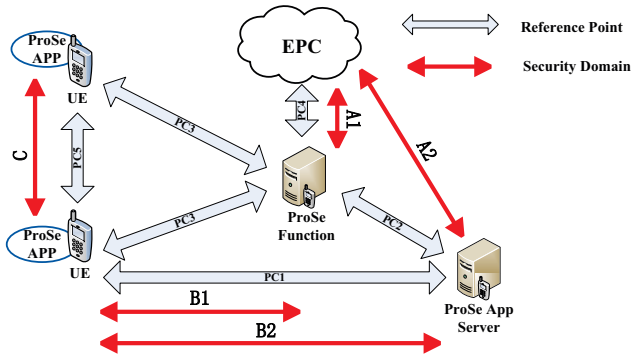

Fig. 2. D2D communication security architecture

B. Requirements of D2D Communication Security

In order to mitigate the potential threats and attacks, we summarize the security requirements that a D2D communication system should fulfill.

Confidentiality and Integrity (C\I): In order to prevent control signaling and user data from maliciously modifying and leaking during transmission, the data needs to be always kept confidential and integrated. For example, in the Relay-Coverage scenario, a receiver can detect any accidental or malicious data alteration by a relay device. All the security domains in D2D communications should support the confidentiality and integrity of data transmission, especially for control signaling.

Authentication (Au): Authentication is the cornerstone of correct functioning of the whole D2D communication system. It is the key to resist the impersonate attack. It must be possible to verify the eligibility of a device or an application to use a D2D service, which is performed on PC1, PC2 or PC3. Meanwhile, the D2D user should be able to verify the identity of D2D service provider. In order to guarantee the security of data transmission, it should be also possible to verify the identity of the sender of any message exchanged in the D2D network, which may happen on PC5. Since the D2D communications relate to relay communications and fully distributed communications, user identity authentication are totally different from common authentication schemes. New authentication schemes for D2D communications are needed, especially a uniform scheme that is applicable in D2D communication scenarios. *Fine-grained Access Control (FAC):* Fine-grained refers to the small granularity of an access policy, which could take into account a user's personal profile and other factors. For example, the D2D application servers always perform access control to D2D devices on their services and data based on fine-grained policies. Moreover, FAC is also expected for group communications, which is an application scenario in D2D communications. Fine-grained data access control needs to be enforced for data delivery in D2D communications so that unauthorized users cannot obtain private information.

Privacy (Pr): User identity, location and other personal information must be concealed to non-authorized parties. Comparing with data confidentiality, user data privacy concerns more about the D2D service functionalities in order to control data leakage to any other parties except the data owner.

Non-Repudiation (NR): To be able to find and separate compromised devices, it must be impossible for a sender or a receiver of a message to successfully deny the authorship or reception of that message.

Revocability (Re): It is indispensable to revoke the user privilege of a D2D service if a user is detected as malicious or harmful or out of service.

Availability and Dependability (A\D): The D2D services should be always available even under attacks such as DoS or DDoS attacks. Intermittent unavailability of the D2D services may irritate user experiences thus hinders the adoption of D2D communications.

IV. Solutions of D2D Security

In this section, we investigate security schemes that have been developed for D2D communications since year 2000. We organize the section by reviewing existing related work, discussing whether they can satisfy the aforementioned requirements and analyzing whether they address related security issues based on the D2D security architecture. TABLE I compares comprehensiveness of existing work based on the security requirements. TABLE II compares existing work for addressing related practical issues based on the D2D security

architecture. We classify our review based on 4 main design purposes about security.

TABLE I. COMPARISON OF EXISTING WORK BASED ON D2D SECURITY REQUIREMENTS

Ref	C\I	Au	FAC	Pr	NR	Re	A\D
[14]	DHKE\HMAC	HMAC	N	N	HMAC	N	Y
[15]	DHKE\N	Commitment Scheme	N	N	N	N	N
[16]	Probabilistic Key Sharing\N	Probabilistic Key Sharing	N	N	N	Y	N
[17]	N\Y	Device Confusion Matrix	N	N	Route Confusion Matrix	N	N
[18]	GKA\Y	Certificate	N	N	N	Y	Y
[19]	N\N	Y	Multi-Priority	N	N	N	Y
[20]	N\N	Y	Secrecy Capacity	N	N	N	Y
[21]	CSI-based key extraction\Y	N	N	N	N	N	N
[22]	PHY-based Cooperative Key Generation\Y	N	N	N	N	N	N

Y: Yes with support; N: No without considerations.

TABLE II. COMPARISON OF EXISTING WORK BASED ON D2D SECURITY ARCHITECTURE

Ref	A		B		C
	A1	A2	B1	B2	
[14]	N	C\I; Au	C\I; Au	C\I; Au	C\I; Au; NR;
[15]	N	N	N	N	C\I; Au
[16]	N	N	N	N	C\I; Au
[17]	N	N	N	N	I; Au; NR;
[18]	N	N	N	N	C\I; Au; Re; A\D
[19]	FAC	FAC	FAC	FAC	N
[20]	FAC	FAC	FAC	FAC	N
[21]	N	N	N	N	C\I
[22]	N	N	N	N	C\I

A. Authentication and Key Management

Zhang et al. proposed a secure data sharing protocol for D2D communications in LTE-Advanced (LTE-A) networks [14]. They leveraged Diffle-Hellman Key Exchange (DHKE) to realize session key distribution between two D2D devices in order to protect confidentiality of distributed data based on a symmetric encryption algorithm. Meanwhile, they took advantage of an HMAC digital signature algorithm to guarantee authentication, data authority and integrity, as well as transmission non-repudiation. Furthermore, by keeping a status record, malicious node detection was realized. However, the application scenario of this protocol is specific and time deterministic. For the purpose of data sharing, a content providing server need to be installed and pre-register into the cellular network and is assumed fully honest. However, the content providing server is exposed under attacks and easily compromised in its insecure domain. Thus, more universal security schemes are expected to support general scenarios. By evaluating this work with the security requirements, we find that this protocol didn't consider or support FAC, Pr and Re. Dependability and availability were not well enhanced. It was not effective in A1 security domain although it concerned other security domains in D2D communications.

Sheng et al. established a shared secret key for D2D communications between two D2D devices based on Diffle-Hellman Key Exchange (DHKE) [15]. In order to overcome Man-in-the-Middle Attack (MITMA), the authors used a commitment scheme to realize mutual authentication between two devices. Nevertheless, its authentication scheme using the commitment scheme is impractical. The authentication process should be accomplished with a visual or verbal comparison in the end, which makes the scheme unrealistic. Furthermore, the scheme only deals with two-device communication scenarios without cellular coverage. Thus, it cannot be applied into all three D2D application scenarios. Obviously, I, FAC, Pr, NR, Re and A\D cannot be supported by this work. It only focused on supporting C\I and Au in the D2D security domain C.

Goratti et al. proposed a security communication protocol to establish direct links among D2D devices [16]. The author first presented a D2D establishment protocol that broadcasts beacon to nearby devices to set up D2D communications. Then, they borrowed a random encryption key pre-distribution scheme from sensor network [24] to help D2D devices selecting encryption keys from a common large pool of keys. The information of key exchange protocol was embedded into a sub-field of the beacon, thus this protocol addressed the compatibility issue with LTE specifications. C, Au and Re were supported by this protocol in the security domain C, while other security requirements were not considered.

B. Secure Routing

In the Out-of-Coverage scenario, routing from a source device to a destination device should be chosen securely. In order to protect the message relayed, a Secure Message Delivery (SMD) protocol was proposed to determine the lowest risk route to delivery messages in the D2D communications [17]. The decision made for the most secure route is not only based on the ability of collaborative detection of malicious messages for each route, but also takes energy costs and Quality-of-Service (QoS) into account. A device confusion matrix and a route confusion matrix were applied respectively to support Au and NR only in security domain C. Route availability and dependability were supported through risk management and by considering QoS and energy costs.

In [18], the authors proposed a D2D group communication protocol by integrating routing control and group key arrangement together. They didn't design the protocol based on Optimized Link State Routing protocol (OLSR) and Secure

OLSR (SOLSR) in order to reduce dependency on network layer functions. The proposed joint scheme controls the routing through link and node state detection. Meanwhile, a Group Key Agreement (GKA) procedure is triggered to produce keys periodically or when networks merged or separated, which can deal with the revocation (Re) issue. Moreover, key renewal latency is analyzed and evaluated to show the availability of this scheme. Certainly, C\I, Au, Re and A\D were supported in the security domain C.

C. Access Control

In [19], the authors addressed the issue of access control for D2D communications in cellular networks. To mitigate the interference caused by D2D communications to cellular communications, the proposed access control model assigned multiple levels of priority for cellular and D2D communication access requests. Cellular communication requests are endowed with the strictly highest priority while D2D communication requests are assigned with distinct priorities according to their types. The authors innovatively applied Network Calculus to evaluate the proposed solution.

Yue et al considered the access control issue under the framework of secrecy capacity of cellular communications [20]. Creatively, the authors introduced the D2D communications as an intentional interference into the cellular communications to prevent against eavesdroppers. With the prerequisite that the secrecy capacity of cellular communications is satisfactory, an optimal D2D pair can be selected to access the D2D network.

Although the above studies [19][20] are heuristic, they both considered improving security from the perspective of cellular communications, rather than from D2D communications. In both studies, FAC was supported in the security area A and B, not C. Meanwhile, they both considered Au and A\D.

D. Physical Layer Security

Physical layer security is under lively discussions as a novel perspective to secure D2D communications. Different from conventional security methods, physical layer security tries to establish security fundament by analyzing and applying physical characteristics of wireless channels between D2D devices.

Xi et al. proposed an improved Channel State Information (CSI) based key extraction protocol for D2D communications [21]. In this scheme, they first used an adaptive quantizer to realize bit stream generation from CIS measurements. Then, in order to prevent key information from leakage, a universal hash function was applied to elaborately validate the consistence of key generation between two users. At last, a fast key recombination method was proposed to dispose the secret key inconsistent problem.

Sun et al. introduced a cooperative key generation scheme [23] into D2D communications in order to setup shared secret keys between devices in physical layer [22]. To overcome the drawback of selfishness in an original cooperative key generation scheme, the authors innovatively modeled the cooperative key generation process as a coalitional game. In this game, all the devices involved in D2D and relay communications are strongly motivated to help other nodes to establish secret keys, and thus gain benefits consequently.

The above two works [21, 22] focused on supporting C\I in the security domain C. But how to merge or integrate them into other security domains requests additional investigation.

V. Open Research Issues and Future Research Directions

According to the above analysis and comparison from two aspects of view in Section IV, we find that a lot of security issues in D2D communications are still open without resolution. First, no work is comprehensive, thus can cover all security domains and fulfill all security requirements. Current work scattered into different aspects of D2D security. It lacks a holistic solution e.g., a generic D2D security framework to support solving all security issues in all security domains in D2D communications. Second, privacy is not considered and supported in D2D communications. Third, the possibility or applicability to merge a security solution into the generic D2D security framework hasn't yet investigated in the literature. But this study is essential for evaluating a solution's applicability and effectiveness. Forth, an integration method lacks in the literature to compose the advance of D2D studies. All above open issues will motivate future research trends.

In addition, we suggest a few promising research directions on D2D communication security based on D2D security architecture and requirements as follows:

(1) Uniform and LTE-compatible key management and authentication schemes for D2D communications are required. Although many literatures have investigated the key management and authentication issues, all of these schemes can only deal with unique application scenario, such as only for "In-Coverage" or "Out-of-Coverage" scenario. A uniform key management and authentication scheme is crucially important for providing available and seamless D2D services in a heterogeneous network environment. In addition, new key arrangement and authentication schemes should be designed compatible with current LTE network security framework as much as possible. The characters of none-repudiation and revocability of the key management scheme should also be seriously taken into consideration due to the dynamic nature of D2D communications.

(2) Fine-grained access control mechanisms need to be designed to address the data protection of D2D communications in all scenarios. The access control solutions proposed in [19][20] focused on the D2D communications with LTE network access control support. The access control problems of inner-D2D communications were not discussed and supported. Heterogeneous and fine-grained access control mechanisms that can cooperate with key management and authentication are yet to be solved in order to support all security domains and application scenarios of D2D communications.

(3) Protecting user privacy will be a significant research topic. For example, in a pervasive social networking scenario supported by D2D communications, when D2D users want to discovery and communicate with proximity users who hold

similar interests or willingness, how to find out target users and communicate with them without leaking personal information (e.g. location, user profiles and so on) is an interesting and significant research topic.

VI. CONCLUSIONS

Deice-to-Device (D2D) communications have been treated as a promising technical component for 5G. In spite of impressive benefits, D2D communications encounter many security problems. However, D2D security hasn't yet been seriously investigated in both academic and standardization communities. In this paper, we introduced main D2D application scenarios and use cases. We further proposed a D2D security architecture compatible with the LTE system and suggested D2D security requirements accordingly. Based on the security architecture and security requirements, we reviewed the existing work in order to explore open research issues and propose future research directions. We found that significant efforts are needed in order to overcome D2D security problems.

ACKNOWLEDGMENT

This work is sponsored by the PhD grant (JY0300130104) of Chinese Educational Ministry, the initial grant of Chinese Educational Ministry for researchers from abroad (JY0600132901), the grant of Shaanxi Province for excellent researchers from abroad (680 F1303) and Aalto University.

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] K. Doppler, M. Rinne, C. Wijting, C. Ribeiro, and K. Hugl, "Device-to-Device communication as an underlay to LTE-Advanced networks," IEEE Communications Magazine, vol. 47, no. 12, pp. 42-49, December 2009.

[3] K. Doppler, C. Yu; C. Ribeiro, and P. Janis, "Mode selection for Device-To-Device communication underlaying an LTE-Advanced network," IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, April 2010.

[4] L. Lei; Z. Zhong; C. Lin; and X. Shen, "Operator controlled Device-to-Device communications in LTE-Advanced networks," IEEE Wireless Communications, vol. 19, no. 3, pp. 96-104, June 2012.

[5] A. Gamage, H. Liang, R. Zhang, and X. Shen, "Device-to-device communication underlaying converged heterogeneous networks," IEEE Wireless Communications, vol. 21, no. 6, pp. 98-107, December 2014.

[6] P. Janis, C. Yu, K. Doppler, C. Ribeiro, C. Wijting, K. Hugl, O. Tirkkonen and V. Koivunen, "Device-to-Device communication underlaying cellular communications systems," International Journal of Communications, Network and System Sciences, Vol. 2 No. 3, pp. 169-178, 2009.

[7] M. Corson, R. Laroia, J. Li, V. Park, T. Richardson, and G. Tsirtsis, "Toward proximity-aware internetworking," IEEE Wireless Communications, vol. 17, no. 6, pp. 26-33, December 2010.

[8] 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.

[9] 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).

[10] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on architecture enhancements to support Proximity-based Services (ProSe) (Rel 12), 3GPP TS 23.703 V12.0.0 (2014-02).

[11] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Proximity-based services (ProSe); Stage 2 (Rel 12), 3GPP TS 23.303 V12.0.0 (2014-02)

[12] G. Fodor, S. Parkvall, S. Sorrentino, P. Wallentin, Q. Lu; and N. Brahmi, "Device-to-Device communications for National Security and Public Safety," IEEE Access, vol. 2, pp. 1510-1520, Decemeber 2014.

[13] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 33GPP System Architecture Evolution (SAE) (Rel 12), 3GPP TS 33.401, V12.12.0 (2014-09).

[14] 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.

[15] 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, Decemeber 2014.

[16] L. Goratti, G. Steri, K. Gomez, and G. Baldini, "Connectivity and security in a D2D communication protocol for public safety applications," 2014 11th International Symposium on Wireless Communications Systems (ISWCS), pp. 548-552, August. 2014.

[17] 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.

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

[19] 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.

[20] 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.

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

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

[23] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," IEEE Journal on Selected Areas in Communications, vol. 30, no. 8, pp. 1578–1588, 2012.

[24] L. Eschenauer and V. L. Gligor, "A Key Management Scheme for Distributed Sensor Networks," 9th ACM Internation Conference. on Computers and Commun. Security (CCS), pp. 41–47, 2002.