Security in D2D Communication in IoT: Challenges and Future Trends

Danah A. Arrabi, Mohammad H. Aljarawrah, Wail Mardini, Mazen Khair

***Abstract*—**Internet of Things (IoT) is a network of everyday devices connected to the internet and equipped with actuators, sensors, and software that enables them to send, receive, share, store and analyze the data. Recently, the devices became the main users of the IoT. As a result, the Device to device (D2D) communication is predicted to be a main component in the IoT ecosystem. In this type of communication, the devices communicate directly with each other without the need for a base station to organize the communication and they cooperate to share, collect, analyze and take an action based on the collected data. D2D communication proved its ability in improving the spectral efficiency, energy efficiency, and system throughput. Unfortunately, the D2D communication IoT architecture has a lot of challenges such as the interference management, route discovery mechanism, the limited device's resources, security and privacy, compatibility and integration management…etc that needs to be solved to provide a good quality of service (QoS). In our paper, we discuss the security as main challenge as well as the power efficiency related issues. We present the state of art contributions in the last few years to overcome the security challenges and discussed a few of them regarding the power efficiency to create an intelligent IoT environment that meets what the user needs..

***Keywords*—**Internet of Things (IoT), D2D communication, security, power efficiency.

I. Introduction

More than 4 billion people worldwide are using the internet today to communicate, share knowledge, life experiences and entertainment through laptops, smartphones and smart devices [1]. Moreover, the number of devices connected to the internet is expected to reach 1.2 billion by the end of this year [2]. The internet of things (IoT) is simply the set of objects; the everyday objects, that are equipped with smart capabilities, used in every house in day-to-day life and connected to the internet such as smart-phones. The user here is the device itself; it gathers the data from other objects, stores it, share it with other objects, or process it to perform a specific task. The capabilities of such smart devices and the availability of the data gathered and shared makes it easy to deliver intelligent services that save time and effort and could be really profitable and beneficial in many different aspects [3][4][5].

IoT applications can be found everywhere and can be integrated with any aspect of our lives. It is applications are growing tremendously day-by-day. In industry, IoT is used for production control, remote cars monitoring systems, factories supplies tracking system, and energy management. In addition, developing smart homes that can save and control the energy consumption, manage home devices network, and maintain a safe environment is possible with the IoT. Safety and security applications using IoT includes assets tracking, monitoring infrastructures for emergency cases and monitoring dangerous chemical and electrical recourses use. Water and oil resources optimization, agriculture monitoring, Smart grids and more, are all IoT applications that are increasing in number and capabilities day-by-day [6] [7].

Each IoT system architecture consists of sensors or actuators. The second architecture component is the internet gateway that receives the data and then forwards it through the used technology like Wi-Fi or else for further processing. After this IT, edge applications process the data to make it in the required form for storing it in the data center or the cloud [8].

IoT technologies include radio frequency identification (RFID) that collects and process the data using radio waves. Wireless sensor networks (WSN) that are a collection of devices with each equipped with a sensor for monitoring a specific environment. Middleware, which is software, that acts as a bridge between an operating system or database and IoT applications. Cloud computing is also an IoT technology where you can access a set of resources that are expensive or hard to acquire locally which is needed in an IoT environment. And the last IoT technology is the applications that enable the communication between the IoT devices and humans [9]. Building an IoT system and the deployment of the pre-mentioned technologies has a lot of challenges. The absence of standardization is one of the main challenges. Security and privacy preservation is also a challenge because of the nature of devices and software used that might be untested as required to preserve the privacy of the transferred data. Managing the connections and guaranteeing the availability and reliability of connections and services provided by IoT must be studied and managed well. Another challenge is the compatibility and scalability of devices and infrastructures used. Maintaining a good level of performance and service needs to be managed as well [10] [11].

Device to device (D2D) communication in IoT has become

Danah A. Arrabi is with Jordan University of Science and Technology, Irbid Jordan 22110.

Mohammad H. Aljarawrah is with Jordan University of Science and Technology, Irbid Jordan 22110.

Wail Mardini is with Jordan University of Science and Technology, Irbid Jordan 22110.

Mazen Khair is with University of Ottawa, Ottawa, ON Canada.

an area of interest in the last few years. This is because of the tremendous growth of smart devices connected to the internet. In such systems; two devices can connect fully with each other, gather, process and take an action based on the collected data without centralized control or human intervention. This can increase network efficiency, decrease power consumption, enable good traffic monitoring and a lot more. Accomplishing such connection has a lot of challenges regarding devices management, security and privacy management, routing management and other challenges that will be discussed later in details [12]. Our objective in this paper is to represent and discuss scientist's latest contributions to enhance the security and power efficiency in device-to-device (D2D) communication in the IoT.

This paper will be structured as follows: section 2 will clarify the concept of D2D communication in IoT, section 3 will represent the challenges that arise in D2D communication, section 4 will present the contributions in the literature in the latest few years to overcome the security and power efficiency problems, section 5 will present a discussion section about the study's results and our opinion about it, section 6 will conclude the subject of the survey, and section 7 will include future work.

II. D2D Communication And Challenges In IOT

Device to device communication concept which means that two device in the network can communicate directly without the need for a base station to monitor the connection; when used in IoT ecosystem can enhance the spectrum use and energy consumption in the wireless networks. In addition to this, communication with a base station is no longer needed so this means less delay, which leads to a better quality of service [13]. Adapting a D2D communication in IoT has a lot of difficulties and challenges that need to be addressed before developing this network, those challenges will be discussed in details in the next section.

In order to build a functional and successful IoT D2D communication infrastructure, a group of issues and challenges must be solved in order to achieve that. Those will be represented next.

A. Interference Management

The interference happens when there are many communicating devices at the same time using the same frequency band so one device is affected by the nearby devices and the signals interfere with each other inside the network, and this will affect the received power and it may distort the signals, which will eventually decrease the quality of service and degrade the network performance. A good communication mechanism should be developed to solve the interference problem [14] [15] [16].

B. Devices Integration Management

The regulations and protocols that are used to establish the connection between the various devices need to be carefully chosen to guarantee a good and reliable connection and a good quality of service in the network [14].

C. Route Discovery

The link established between the devices to communicate needs to be established in an efficient way or the connection will not be done correctly which will lead to performance degradation [15] [17].

D. Security

The information shared and transferred through the network may be hacked, distorted or missed which means that the need for privacy preservation and authentication management algorithms is a must in D2D communication. If the developer wants to deliver a good level of quality of service (QoS), his network must keep the user information safe, correct, and confidential [15] [18]. The types of attacks that may happen in D2D communication are the denial of service attack (DoS), Man in the middle, and a lot of other possible attacks [19] [20]. We decided as authors to make the security as the first class to discuss in our literature review.

E. Resource Optimization

Devices in the IoT network are of limited resources regarding power, energy, CPU, bandwidth, and memory. In the common design of IoT network where there is a base station and a limited spectrum in the network; the quality of service may degrade as the load on the BS increases, latency, and low coverage may happen also. The D2D design comes as a suggestion to solve this problem because the communication happens directly between the devices, but the limited resources of such devices is an issue and those resources need to be optimized in order to deliver a good QoS yet with an optimized recourses use [15]. In our study, we chose to talk slightly about the power efficiency as a second class.

III. Literature Review

Jaehyu Kim et al. [21] proposed a new scheme that provides a secure connection between two devices in a long-range wide area network (LoRaWAN). For a long time, LoRaWan provided node-server communication links in the shape of a star topology. The authors exploited a late study that introduced the ability to create a device-to-device communication in such network with improved power use because of the direct D2D connection. They proposed a key-based approach with two new MAC request and answer messages. The secure request is sent from the base node to the network server, which in turn generates a connection channel and security parameters including a key, and sends it back to the base node. Again, the node generates a secure encryption key for the connection also. The destination node does the same, the four keys eventually are shared between the two nodes, and the secure encryption-decryption process begins. This method succeeds at securing a D2D connection in LoRaWAN but with a 5% increase in power use compared with the common used LoRaWAN connection technology.

QianXu et al. [22] introduced a new secure relay transmission protocol in an IoT network where neither the number nor locations of eavesdroppers are known. The relay transmission

architecture is used. In addition to the sender and receiver devices, there is a relay device that is responsible for retransmitting the message in its way to the receiver. Their protocol is the first one to assume that the eavesdroppers are not known, and thus; the simulation mainly distributed the eavesdroppers randomly. The authors used randomize-and-forward exiting approach as an additional step to enhance the security; both the relay and the sender use two different codes to send the same message. The proposed approach achieved optimal power use and secrecy probability.

Aleksandr Ometov et al. [23] introduced a trustworthy framework for the device-to-device communication in the IoT environment based on the social relationships between those devices or the relationships among their users. The proposed scheme suggests establishing a direct connection between the network devices when the service of connection is not available. The devices distributed over the network are divided into clusters based on the similarity properties between them, and each new device joins a specific cluster based on the degree of friendship it has with the different available clusters. The higher the value, the stronger the relationship of that device with the cluster. By comparing the performance of the simple D2D and the proposed social-aware proposed D2D connection; the percentage of served users increased by 20%, 30%, and 40% when the network coverage was 90%, 70%, and 50% respectively.

Zhaoyue Zhang et al. [24] proposed a new algorithm to ensure trusted D2D communication based on RF fingerprint. The distributed nature of D2D connections and the absence of control increase the probability of attacks, while the limited computational abilities of connected devices, make it difficult to use advanced encryption schemes. For all of these reasons, the authors thought of a way that builds a trusted D2D connection based on a fingerprint for each device. Once the two devices are authorized after the detection of their fingerprints, a trusted connection starts between them. The simulation shows that when the signal to noise ratio is larger than 8, the FR fingerprint recognition is 100% which provides more secure D2D connection.

Kecheng Liu et al. [25] studied the security of mobile device-to-device connection in the Android operating system. The authors stated the security issues in such networks and suggested a set of solutions to overcome these issues. They found that the majority of information shared across the mobile D2D network is not encrypted and can be hacked and eavesdropped. The other issue is that the structure of Android suffers from the problem of over-privileged apps that can access the Wi-Fi hotspot information including the password, which leads to an unsafe network. Lastly, the absence of a configuration that ensures the network is safe. The authors suggest that additional permission should be required from devices to access the mobile network. The other suggestion is to monitor the number of devices connected to the network to deal with undesired devices quickly. They also state that the main information of the mobile network should be encrypted to make it harder for the intruders to access the network.

Mingjun Wang et al. [26] introduced two new protocols for secure device-to-device group communication. Most of the previous studies have introduced secure communication protocols between two devices only. The D2D group communication that is established for attaining a specific service connecting the devices together like chatting groups; introduces more complicated security threats. The first privacy-preserving protocol is called PPAKA-HMAC where a session connection key is established and combined with HMAC message and shared secretly between the devices of the group so the network is protected against external attacks. In addition to this, the user identification and authentication processes are anonymously done by the protocol; making it very hard to access the key information of the network. The reason for establishing the other protocol PPAKA-IBS is that the first one only protects from the external attacks and cannot deal with the internal attacks. This protocol is able to reveal the device that does not follow the rules of the protocol and analysis of its behavior because it is suspected to cause an internal attack. The communication overhead of the PPAKA-HMAC was (97*n^2+189n) while the PPAKA-IBS was (97*n^2+229n).

Hui-Ming Wang et al. [27] proposed a new physical layer security scheme for the device-to-device (D2D) communication in random networks. The reason behind this study is that the available physical layer security approaches such as the multiple-antenna, for example, are not applicable in a D2D communication because the majority of devices in such cases are equipped with a single antenna. Another example is the cooperative approaches that are computationally demanding and cannot be applied in D2D environment where the devices are of limited resources such as memory and power. For the pre-mentioned reasons, there is a chance of attacks on the transmitted data. Latest studies introduced a full-duplex jamming receiver approach. The core idea of this approach is that the receiver of a specific message in the network transmits a jamming signal at the moment it receives the message. This signal is able to arouse the eavesdropper and prevents it from accessing the transmitted data. The researchers proposed a scheme of two receivers' switched full-duplex and half-duplex modes. The switching between the two modes is based on a threshold and the resources optimization is studied in both modes. The two modes proposed approach achieved a higher secrecy throughput than the single full-duplex mode or the single half-duplex mode.

Aleksandr Ometov et al. [28] introduced a new security approach in a socially-aware device to device communications. The main idea behind this approach is that the devices connected to a network, socially connected based on specific criteria and in the case of an unavailable cellular network; the devices still can manage their secret network and accept a new trusted device to the network or rejecting an existing device when the cellular connection that manages the network is not available. This feature was not available before this study. In order to establish this approach, they used 3GPP LTE (release

10) with some modifications regarding configurations and security parameters. On the other hand, the mobile device-to-device connection policies were modified in terms of firewalls and protection to allow the device's connection when the cellular connection is out of reach. As an initial step, each device in the network receives a number of secret and public keys as a certificate. At the devices group configuration step; the server of the network operates a series of steps to establish the group based on the secret IDs of the devices. A direct connection and information sharing can happen fully directly between devices without the server help, which reduces the latency in the proposed approach. This research introduces new chances for building secure social-aware networks with improved performance and computational efficiency.

Aleksandr Ometov et al. [29] proposed a secure protocol for the delivery of secure data between the user and its wearable devices in the case of cellular connection absence. The connectivity between devices in this approach depends on the cluster the device resides in; which in the first place was constructed based on the social and spatial similarities of users and devices. After the clusters are formed and devices are distributed among them based on the social and spatial proximity; the secure connection can begin between the same cluster devices. Every device should request to join a group of devices, and after that, all the devices should reply with acceptance before a set of certificates are generated and distributed so that a direct link is created to transfer the data. The proposed protocol enhanced many performance measurements related to D2D communications and can be used efficiently in other D2D areas in the future.

Mingjun Wang et al. [30] reviewed the device-to-device (D2D) application scenarios in terms of network equipment presence such as the base station; to an in-coverage scenario in which all the devices are located in the cellular network range and controlled by the network equipment and operators. The operator here is in charge of authenticating the devices and regularizing the connections. The other scenario is the relay-coverage where the devices that are outside the cellular network coverage rely on a device that is in the range to communicate with the network. The last scenario is the out-of-coverage in which there is no network coverage and the devices communicate directly with each other. In most of the cases, this scenario is used for emergency connections when the cellular network coverage is down. They also discussed the security threats that arise in D2D networks such as Impersonation, fabrication and data distortion. The authors stated also the security requirements when establishing a D2D network, the available security schemes and their problems and suggested some research areas that have not been addressed until that moment regarding network roaming security issues and the absence of universal security D2D frameworks. Table (1) presents a comparison between the D2D security solutions presented in this survey.

Zhenyu Zhou et al. [31] proposed a hybrid algorithm for resource allocation in D2D communications underlaying C-RAN based LTE-A networks to improve energy efficiency (EE) and ensure the quality of service (QoS) through joint channel selection and power allocation design. The hybrid algorithm consisting of distributed remote radio heads (RRHs) and centralized baseband unit (BBU) pool. The results appear in the simulation show that the algorithm achieved the proportion of the futility of "zero" almost and achieved better performance in energy efficiency and QoS requirement.

Lingjun Puet al. [32] Proposed D2D Fogging novel network assisted D2D collaboration framework. The proposed D2D fogging can perform energy-efficient tasks for users at the network level through the sharing of computation resources and communications. The results show that the algorithm not only achieves excellent performance but also adapts to different situations.

Antonino Orsino et al. [33] present data collector scheme for the IoT in a Smart City scenario for energy efficient, based on network-assisted D2D communications under LTE-A networks. The author covers a lot of study cases and the comprehensive assessment of the performance evaluation in many scenarios Will testify the gains that can be achieved in terms of energy efficiency and resource utilization. Radio resource utilization and of energy efficiency used to evaluate the performance. Table (2) presents a comparison between D2D power efficiency solutions presented in this survey.

IV. Discussion

After comparing and studying the various contributions that focus on solving D2D communication challenges related to security, we noticed that there is a tendency towards the social-aware solutions that focus on finding a common relation between the devices connected to the network or even the users of such devices, and exploiting this in building and maintaining a secure relationship, in addition to developing security schemes based on this relation. Additionally, in most of those contributions, there was always a tradeoff between the security and another factor such as power consumption, memory use, latency, and other factors. Regarding the power efficiency challenge, we noticed that there is a wide diversity in the proposed solutions and there is a tendency towards combining the different techniques as hybrid solutions to overcome the power efficiency challenge in D2D communication in the internet of things (IoT).

V. Conclusion

Device to device direct communication without a centralized control is a recent concept that is proving its ability in network resource's optimization, decreasing latency, and improving the level of quality of service (QoS) in the network. Yet, developing such a way of communication holds many challenges. The main objective of this survey was to present the security and power efficiency as the main challenges and presenting the contributions in the literature to overcome those challenges. The results were very promising.

TABLE I: COMPARISON OF D2D SECURITY SOLUTIONS -PART1

Ref.	Year	Objective	Technique/s Employed
[21]	2018	Secure D2D link establishment	- SecureD2DReq and SeceureD2DAns messages - Shared cryptographic keys
[22]	2016	Security enhancement with eavesdroppers with uncertain locations	- Relay (sensor node) employment to retransmit secret messages - Different code books to retransmit the same secret message (RF strategy)
[23]	2016	Secure social aware D2D connectivity	- Devices clustering based on social relationships - Direct link establishment between cluster's devices when no cellular conn.
[24]	2018	Secure D2D link establishment based on RF fingerprint	Hilbert transform and principal component analysis (PCA) used for RF fingerprint establishment
[25]	2018	Security enhancement schemes in Android mobile networks	Suggestions proposed: - Tracking the number of connected devices - Encrypting the network connection information
[26]	2018	Secure protocols for secure D2D group communication	- PPAKA-HMAC protocol - PPAKA-IBS protocol
[27]	2018	Adaptive full-duplex jamming receiver for secureD2D links establishment	- Jamming signal generation at the receiver's side to arouse the eavesdropper and prevents it from accessing the transmitted data - Two modes receiver (Full duplex and half duplex)
[28]	2016	Secure social aware D2D connectivity	- Modified 3GPP LTE (release 10) - Devices votes to accept or reject a new device in the network social group
[29]	2016	Security-centric framework for D2D connectivity based on spatial and Social relations	New Communication protocol where: - Each cluster of devices has a certificate that is generated when the cluster is formed - Every device should request to join a group of devices

TABLE II: COMPARISON OF D2D SECURITY SOLUTIONS -PART2

Ref.	Security Requirements	Results Achieved	Network Type
[21]	- Mutual Authentication - Confidentiality - Message Integrity	- Secure D2D communication - 4-5% increased power consumption compared with the basic D2D communication scheme	LoRaWan
[22]	Not Mentioned	- Enhanced secrecy throughput - Extended secure coverage area	Networks with 5G technology
[23]	Not Mentioned	- Security connection is delivered - Percentage of served users increased by 20% when the network coverage was 90%	Cellular Networks
[24]	Not Mentioned	Recognition rate of devices is more than 90% under SNR=5dB	Wireless Networks
[25]	Not Mentioned	No mathematical results	Mobile Networks/ Android OS
[26]	- Authentication - Identity privacy preservation - Group communication security	- PPAKA-IBS can establish secure D2D group communications by providing better security than PPAKA-HMAC in terms of resisting internal attacks	IoT networks
[27]	Not Mentioned	- Increased secrecy throughput with budgets of transmit power and jamming power growth - Higher secrecy throughput than the single full-duplex mode or the single half-duplex mode	Random Networks
[28]	Not Mentioned	In unreliable cellular connectivity; adding anew user takes less than 120 ms on average, whereas excluding a user may consume up to 5 s in the worst case	Cellular Networks
[29]	Not Mentioned	Average user relevant throughput increased by 2.5% compared with the standard security approach	Networks with 5G technology

REFERENCES

[1] "DIGITAL IN 2018: WORLD'S INTERNET USERS PASS THE 4 BILLION MARK", We Are Social USA, 2018. [Online]. Available: https://wearesocial.com/blog/2018/01/global-digital-report-2018.

[2] "Global connected IoT devices by type 2017 and 2018 | Statistic," Statista.[Online].Available:https://www.statista.com/statistics/789615/worldwide-connected-iot-devices-by-type/.

[3] O. Bello and S. Zeadally, "Intelligent Device-to-Device Communication in the Internet of Things," in IEEE Systems Journal, vol. 10, no. 3, pp. 1172-1182, Sept. 2016. https://doi.org/10.1109/JSYST.2014.2298837

[4] P. V. Paul and R. Saraswathi, "The Internet of Things — A comprehensive survey," 2017 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), Melmaruvathur, 2017, pp. 421-426. https://doi.org/10.1109/ICCPEIC.2017.8290405

[5] "What Is the Internet of Things?" Cloudwards, 2018. [Online]. Available:https://www.cloudwards.net/what-is-the-internet-of-things/.

[6] R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key

Challenges," 2012 10th International Conference on Frontiers of Information Technology, Islamabad, 2012, pp. 257-260. https://doi.org/10.1109/FIT.2012.53

[7] S. Chen, H. Xu, D. Liu, B. Hu and H. Wang, "A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective," in IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349-359, Aug. 2014. https://doi.org/10.1109/JIOT.2014.2337336

[8] "How to design an IoT-ready infrastructure: The 4-stage architecture", TechBeacon,2018.[Online].Available:https://techbeacon.com/4-stages-iot-architecture.

[9] I. Lee and K. Lee, "The internet of things (IoT): Applications,investments, and challenges for enterprises," ScienceDirect, vol. 58, no. 4, pp. 431-440, Aug. 2015. https://doi.org/10.1016/j.bushor.2015.03.008

[10] S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," 2016 IEEE Smart Energy Grid Engineering (SEGE), Oshawa, ON, 2016, pp. 381-385. https://doi.org/10.1109/SEGE.2016.7589556

[11] "Biggest IoT (Internet of Things) Challenges in 2018", Kualitatem, 2018.[Online]. Available: https://www.kualitatem.com/blog/internet-of-things-in-2018/.

[12] "How does device to device communication works - RF Page", RF Page, 2018. [Online]. Available: https://www.rfpage.com/how-does-device-to-device-communication-works/.

[13] A. Essameldin and K. Harras, "Device-to-Device communication in the internet of things QSIURP report," pp. 1-6. [Online]. Available: http://docplayer.net/39590069-Device-to-device-communication-in-the-internet-of-things-qsiurp-report.html

[14] M. S. M. Gismalla and M. F. L. Abdullah, "Device to device communication for internet of things ecosystem: An overview," International Journal of Integrated Engineering, vol. 9, no. 4,pp.118-123,2017.[Online].Available: http://penerbit.uthm.edu.my/ojs/index.php/ijie/article/view/2043

[15] P. Pawar and A. Trivedi, "Device-to-Device communication based IoT system: Benefits and challenges," IETE Technical Review, pp. 1-13, Jun. 2018. https://doi.org/10.1080/02564602.2018.1476191

[16] T. Peng, Q. Lu, H. Wang, S. Xu and W. Wang, "Interference avoidance mechanisms in the hybrid cellular and device-to-device systems," 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, Tokyo, 2009, pp. 617-621. https://doi.org/10.1109/PIMRC.2009.5449856

[17] X. Lin, J. G. Andrews, A. Ghosh and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," in IEEE Communications Magazine, vol. 52, no. 4, pp. 40-48, April 2014. https://doi.org/10.1109/MCOM.2014.6807945

[18] U. N. Kar and D. K. Sanyal, "An overview of device-to-device communication in cellular networks," ScienceDirect, vol. 4, no. 4, pp. 203-208, Oct. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959517301467 https://doi.org/10.1016/j.icte.2017.08.002

[19] O. Nait Hamoud, T. Kenaza and Y. Challal, "Security in device-to-device communications: a survey," in IET Networks, vol. 7, no. 1, pp. 14-22, 1 2018. https://doi.org/10.1049/iet-net.2017.0119

[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," in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1054-1079, Second quarter 2017. https://doi.org/10.1109/COMST.2017.2649687

[21] J. Kim and J. Song, "A secure Device-to-Device link establishment scheme for LoRaWAN," IEEE SENSORS JOURNAL, vol. 18, no. 5, pp. 2153-2160, Mar. 2018. https://doi.org/10.1109/JSEN.2017.2789121

[22] Q. Xu, P. Ren, H. Song and Q. Du, "Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations," in IEEE Access, vol. 4, pp. 2840-2853, 2016. https://doi.org/10.1109/ACCESS.2016.2575863

[23] A. Ometov et al., "Toward trusted, social-aware D2D connectivity: bridging across the technology and sociality realms," in IEEE Wireless Communications, vol. 23, no. 4, pp. 103-111, August 2016. https://doi.org/10.1109/MWC.2016.7553033

[24] Z. Zhang, X. Guo and Y. Lin, "Trust Management Method of D2D Communication Based on RF Fingerprint Identification," in IEEE Access, vol. 6, pp. 66082-66087, 2018. https://doi.org/10.1109/ACCESS.2018.2878595

[25] K. Liu et al., "Security Analysis of Mobile Device-to-Device Network Applications," in IEEE Internet of Things Journal, 2018.

[26] M. Wang and Z. Yan, "Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications," in IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3637-3647, Aug. 2018. https://doi.org/10.1109/TII.2017.2778090

[27] H. Wang, B. Zhao and T. Zheng, "Adaptive Full-Duplex Jamming Receiver for Secure D2D Links in Random Networks," in IEEE Transactions on Communications, 2018. https://doi.org/10.1109/TCOMM.2018.2880216

[28] A. Ometov et al., "Dynamic Trust Associations Over Socially-Aware D2D Technology: A Practical Implementation Perspective," in IEEE Access, vol. 4, pp. 7692-7702, 2016. https://doi.org/10.1109/ACCESS.2016.2617207

[29] A. Ometova, A. Orsinob, L. Militanob, G. Aranitib, D. Moltchanova, and S. Andreeva, "A novel security-centric framework for D2D connectivity based on spatial and social proximity - ScienceDirect," Computer Networks, vol. 107, no. 2, pp. 327-338, Oct. 2016. https://doi.org/10.1016/j.comnet.2016.03.013

[30] M. Wang and Z. Yan, "A survey on security in D2D communications - SpringerLink," Mobile Networks and Applications, vol. 22, no. 2, pp. 195-208, Apr. 2017. https://doi.org/10.1007/s11036-016-0741-5

[31] Z. Zhou, M. Dong, K. Ota, G. Wang and L. T. Yang, "Energy-Efficient Resource Allocation for D2D Communications Underlaying Cloud-RAN-Based LTE-A Networks," in IEEE Internet of Things Journal, vol. 3, no. 3, pp. 428-438, June 2016. https://doi.org/10.1109/JIOT.2015.2497712

[32] L. Pu, X. Chen, J. Xu and X. Fu, "D2D Fogging: An Energy-Efficient and Incentive-Aware Task Offloading Framework via Network-assisted D2D Collaboration," in IEEE Journal on Selected Areas in Communications, vol. 34, no. 12, pp. 3887-3901, Dec. 2016. https://doi.org/10.1109/JSAC.2016.2624118

[33] A. Orsino, G. Araniti, L. Militano, J. Alonso-Zarate, A. Molinaro, and A. Iera, "Energy efficient IoT data collection in smart cities exploiting D2D communications," Sensors, vol. 16, no. 6, pp. 1-19, Mar. 2016. https://doi.org/10.3390/s16060836