Acta Montanistica Slovaca
ISSN 1335-1788
actamont.tuke.sk

Analysis of Key Establishment Techniques for Secure D2D Communication in Emerging 5G Cellular Networks

Amir Aziz BUTT[1], *Gohar Rehman CHUGHTA*[2], *Asif KABIR*[*3], *Zahid MAHMOOD*[4], *Zain ul Abidin JAFFRI*[5], *and* *Judit OLÁH*[6]

Authors' affiliations and addresses:
[1] Department of Computer Science & IT, Women University of Azad Jammu and Kashmir Bagh, Pakistan
e-mail:amirbutt12@gmail.com

[2] Department of Computer Science & IT, Women University of Azad Jammu and Kashmir Bagh, Pakistan
e-mail: goharehman@wuajk.edu.pk, goharrehman25@yahoo.com

[3] Department of CS & IT University of Kotli,11100, Azad Jammu & Kashmir, Pakistan
e-mail: asif.kabir@uokajk.edu.pk

[4] Department of CS & IT University of Kotli,11100, Azad Jammu & Kashmir, Pakistan
e-mail: zahidmahmood75@uokajk.edu.pk

[5] College of Physics and Electronic Information Engineering, Neijiang Normal University, Neijiang, 641100, P.R. China
e-mail: zainulabidinjafri@gmail.com

[6] Faculty of Economics and Business, University of Debrecen, 4032 Debrecen, Hungary; College of Business and Economics, University of Johannesburg, Johannesburg 2006, South Africa
e-mail: olah.judit@econ.unideb.hu

***Correspondence:**
Asif Kabir, Department of CS & IT University of Kotli,11100, Azad Jammu & Kashmir, Pakistan
tel.:00923335370163
e-mail: asif.kabir@uokajk.edu.pk

Acknowledgement:
Project no. 132805 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the K_19 funding scheme.

How to cite this article:
Butt, A., A., Chughta, G. R., Kabir, A., Mahmood, Z., Jaffri, Z. A., and Oláh, J. (2021). Analysis of Key Establishment Techniques for Secure D2D Communication in Emerging 5G Cellular Networks. *Acta Montanistica Slovaca,* Volume 26 (3), 395-403

DOI:
https://doi.org/10.46544/AMS.v26i3.01

Abstract
Device-to-Device (D2D) communication as part of emerging 5G wireless networks presents a new paradigm for enhancing the performance of traditional cellular networks. The number of devices connected over the internet is dramatically increasing, and cellular operators are struggling to harness the overwhelming data traffic on their networks. D2D communication in a cellular network allows two cellular devices in close proximity to communicate directly with each other without going through the base station. D2D communication faces various challenges that include device discovery, resource allocation, interference and security; however, the security aspects of D2D are not sufficiently addressed. Due to limited computing capability and energy-constrained D2D devices, effective and lightweight security solutions are required for enabling successful D2D capability. To secure D2D communication, session key establishment is the most vital task. Public Key Cryptography (PKC) is the most widely used cryptosystem and have numerous security applications such as encryption, digital signature, and key exchange. This work analyses the performance of three PKC protocols that are commonly used for session key establishment and exchange, namely, Diffie-Hellman (DH), Rivest-Shamir-Adleman (RSA) and Elliptic Curve Diffie-Hellman (ECDH), with a focus on D2D communication. We performed extensive simulations for DH, RSA and ECDH, in D2D communication scenarios using OMNET++ simulator and explored the effect of various network factors on key establishment delays such as network size, the impact of interference between D2D pairs and the effect of interference from cellular users upon D2D users as well. The results reported in this paper can provide significant insight in assessing the suitability of DH, RSA and ECDH for the key establishment for D2D in 5G networks.

Keywords
Device to Device (D2D), Key Establishment, Diffie-Hellman (DH), Elliptic Curve (ECC)

Introduction

The 5G wireless communication systems are expected to facilitate 1000 times higher capacity as compared to that current mobile networks (Asadi et al., 2014). In addition, the forthcoming 5G systems are anticipated to befittingly cater to both the existing and forthcoming applications, including those that stipulate rigorous Quality-Of-Service (QoS) needs such as higher spectral, energy efficiency, reliability and minimum delay (Kabir et al., 2021; Kharroubi, 2021).

Further, the Internet of Things (IoT) is expected to gather momentum that envisions a huge mesh of billions of interconnected devices such as sensors, actuators, home and business appliances necessitating advanced innovative wireless communication systems (Kurar, 2021; Lampropoulos et al., 2019). Device-to-Device (D2D) communication for 5G wireless systems is an emerging concept that allows two cellular devices in close proximity to communicate directly with each other without going through the base station (BS) or evolved node B (eNB) (Mach et al., 2015; Oláh et al., 2021 or Mittal, 2020). In the traditional cellular system, all the communication takes place through the base station and direct communication between the devices is not permitted even if the devices are in range of each other. In contrast, D2D communication allows the devices to establish the direct link and send data directly without traversing the base station (BS). D2D communication provides numerous benefits over traditional two-hop cellular communication. The D2D communication increases the spectral efficiency, reduces power consumption, improves throughput and cell coverage (Wei et al., 2014). However, realising these benefits of D2D communication requires overcoming several challenges. Primary challenges to D2D communication include device discovery, resource allocation, interference and security. The significant research effort is focused on device discovery, resource allocation and interference, while the security issue is relatively not that well addressed (Belas et al., 2018; Fedorko et al., 2018). Employing effective security practices to address security issues is critical for the successful deployment and acceptance of the D2D paradigm.

The secure D2D communication must meet the security requirement of confidentiality, integrity, availability and authentication (CIAA). In order to ensure the security of D2D communication, establishment, exchange and management of cryptographic keys is highly critical (Wang et al., 2015). Public Key Cryptographic (PKC) techniques are widely employed for this purpose, and one of the major concerns is the overhead associated with these methods. The focus of this works is to analyse the performance of PKC based key establishment/exchange protocols in order to assess their efficacy and associated overhead for D2D communication scenarios.

The rest of the paper is organised as follows: In section 2, the general concept of D2D communication and associated security issues are reported. It also describes key establishment/exchange methods based on PKC, along with a brief review of related work. Section 3 includes the system model, simulation scenarios, performance results, and analysis. Finally, Section 4 concludes the paper.

Secure Device-to-Device (D2D) Communication

D2D Communication Framework

In traditional cellular systems, the BS relays the packet between the cellular devices and does not permit direct communication between the devices even if the devices are in each other's range. In contrast, D2D communication allows the devices to establish the direct link with their proximity device and allows devices to send data directly without traversing the BS. Direct communication allows the devices to use lower transmission power than that used in cellular transmissions, which is essential to prolong the battery lifetime of devices. Additionally, the direct transmission between devices improves throughput, cell coverage and reduces transmission delays. Fig. 1 illustrates cellular and D2D communication.

The D2D communication in the cellular network can be classified into two major categories based on spectrum utilisation, namely out-band and in-band D2D communication (Haus et al., 2017; Barskar et al., 2016). The out-band D2D communication uses an unlicensed spectrum for the communication and is generally used by ad-hoc technologies like ZigBee, Bluetooth, WIFI and WIFI-direct. On the other hand, in-band D2D communication employs the same licensed spectrum for D2D communication that is used for cellular communication. There are two modes to use cellular spectrum for in-band D2D communication: underlay where the same frequency band is assigned to both cellular and D2D users, and overlay wherein a separate frequency band is designated for D2D users. Studies have shown that the underlay D2D provides higher performance gains than an overlay if proper interference management techniques are used. Furthermore, the underlay D2D improves the power and spectrum efficiency of the cellular network.

Security issues in D2D Communication

The wireless communication systems are susceptible to security threats given their broadcast nature. The D2D communication must meet the security requirement of confidentiality, integrity, availability, and authentication to provide resistance against attacks such as Eavesdropping, Masquerading, Denial of Service (DOS), Non-repudiation, and Replay Attacks.

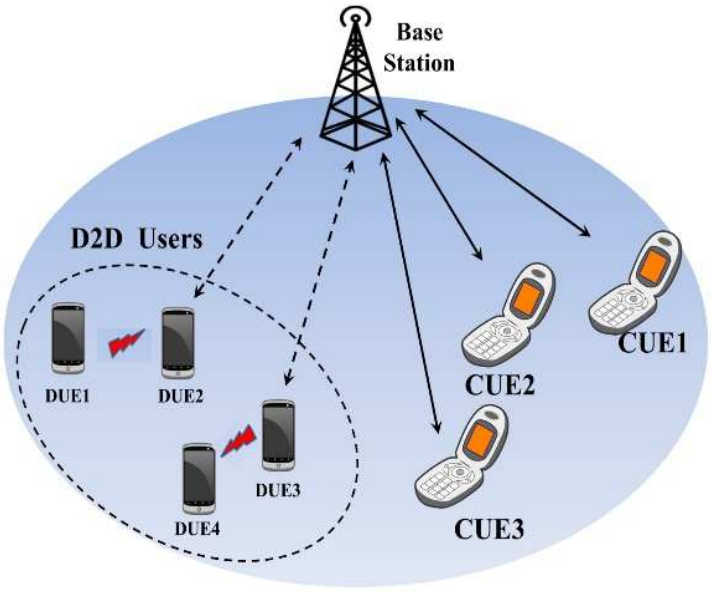

Fig. 1. D2D communication in the cellular system

Key Establishment and Management

To secure the communication among the D2D devices, secure key establishment is a vital task. The key management is concerned with the generation, storage and exchange of the keys. The authentication allows the devices to identify each other and allow only legitimate users to use the D2D services. The public-key cryptographic (PKC) algorithms are commonly used for key establishment and digital certificates. Because of PKC computational overhead, they are rarely used for usual encryption; rather, symmetric-key cryptographic (SKC) algorithms (AES/DES) are used commonly. PKC techniques are often used to exchange/create keys for SKC algorithms. Key management is also a very crucial issue in group communication in D2D. The D2D requires key updating dynamically because devices enter and leave the group frequently. Further, for emerging peer-to-peer D2D applications running over resource-constrained mobile devices, PKC techniques with lower overhead become critical.

Related Work

Several approaches have been suggested in the literature for authentication and key establishment in the D2D context. These can be categorised on the basis of a limited number of recognised PKC algorithms such as RSA, Diffie-Hellman (DH) and Elliptic Curve Cryptography (ECC). The Rivest-Shamir-Adleman (RSA) scheme was the first used public-key cryptosystem published in 1978 by Ron Rivest, Adi Shamir, and Len Adleman at MIT. The RSA cryptographic system is based on the practical difficulty of factorising the product of two large prime numbers. RSA is computationally intense and hardly used for general encryption; however, RSA has other applications like Key Exchange and Digital Signatures. RSA requires a larger key size; the normal key size being used for the encryption is 1024 bits.

The authors (Fouda et al., 2011) provide a broad overview of smart grid communication and implement a lightweight message authentication mechanism tailored for smart grid communication. This scheme is based on DH, HMAC and RSA cryptographic functions. The simulation results show that the scheme has less communication overhead and low latency compared to Elliptic Curve Digital Signature Algorithm (ECDSA). However, the scheme has more computation overhead due to RSA encryption.

The DH key exchange algorithm is the most simple and commonly used key exchange algorithm. The security and effectiveness of DH key exchange depend on the difficulty of computing discrete logarithms. A secure key establishment based on Diffie-Hellman (DH) key exchange and commitment scheme for D2D communication is presented by Shen et al. (2014). The authors in the proposed network (Sedidi et al., 2016) assisted key exchange protocols for cellular D2D communication in 5G, based on DH key exchange and HMAC cryptographic function. Elliptic curve cryptography (ECC) is a competing scheme used in resource-constrained environments like ad-hoc networks. The strength of ECC relies on the complexity of elliptic curve discrete logarithms.

Tab. 1. Bench-mark results for ECC, RSA, DH

Algorithm Family	Crypto Systems	Key Size	Key Pair Generation Time (sec)	Secret Exchange Time(sec)
Discrete Logarithm	DH	3072	0.05	0.018
Integer Factorization	RSA	3072	0.90	0.001
Elliptic Curves	ECDH	256	0.0005	0.00008

The principal attraction towards the ECC is that it provides an equal level of security for smaller key sizes as compared to RSA and DH. For instance, to protect a 128-bit AES key, it would take a 3072-bit key for RSA and DH, whereas ECC can provide an equal level of security with a 256-bit key (Sedidi et al., 2006). The length of the key is directly proportional to the computational complexity of the protocol that results in larger overhead. In proposed mutual authentication and anonymous key distribution (AKD) scheme for smart grid has been proposed (He et al., 2016). The authors adopt ID-based PKC and Schnorr's signature for AKD. Simulation results show that AKD has less computation overhead and small verification delays. The authors (Pereira et al., 2014) use Role-Based Access control (RBAC) for authorisation and ECC (Elliptic Curve Cryptography) for the key establishment. The object has to be pre-registered with the RA (Registration Authority). The RA is responsible for generating and storing the public key for the network devices. The theoretical analysis shows its resilience against MITM attack and replay attack.

System Model, Results and Analysis

We have considered three PKC based protocols, namely RSA, Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH), for key establishment (in terms of key pair generation, key exchange and key agreement) in D2D underlay communication. The performance analysis of key establishment/exchange algorithms is based on the overhead associated with the use of computing and communication resources. The two operations, i.e., computation and communication, form the basis of most of the protocols that involve the transport of information over insecure channels. We have taken the bench-marks results of these two operations performed on an Intel Core i7-5930k CPU with 32 GB of RAM running Windows 10 Enterprise 64-bit (Liu et al., 2014). The bench-mark results for key size RSA (3072), DH (3072) and ECC (256) are shown in Table 1.

To implement the public key exchange protocol, the key size is taken as the payload length of the packet, and the computation time is implemented using self-timer delays (Amin and Biswas, 2015). We also introduced a new performance measure called key establishment delay, which is the time taken by the D2D pair to establish the symmetric key.

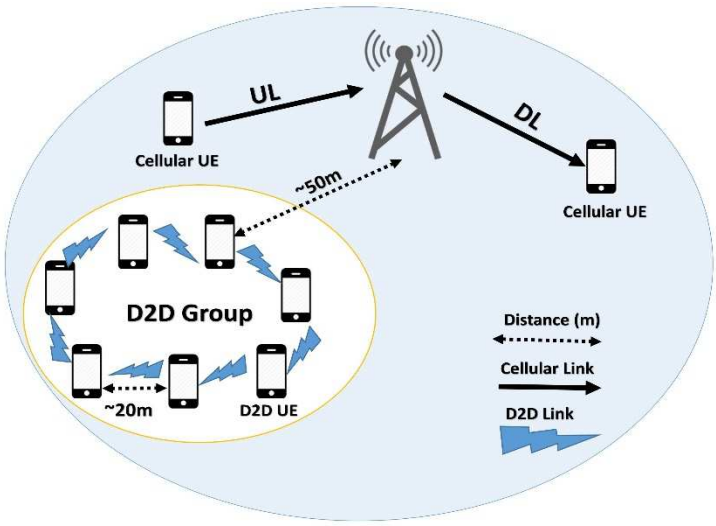

Fig. 2. Simulation model

Simulation Setup and Scenarios

The performance of key establishment and exchange methods has been evaluated using SimuLTE in OMNET++ (El-Hamawi et al., 2014). Fig. 2 shows the simulation model for this study that depicts a network with a number of cellular and D2D users. The network consists of a single cell with each UE associated with eNB. The UE are far (50m) from eNB and close (20m) to each other. Each UE has one to one correspondence with other UE, this form a unicast D2D pair. Both UEs in D2D pair have the capability to send and receive data over the D2D link. The UEs are using UDP as their transport layer protocol. This model is representative of a network-assisted

D2D communication scenario underlying cellular networks (Nardini et al., 2016). In network-assisted D2D communication, the UE-A sends a packet to UE-B without traversing eNB in contrast to traditional two-hop communications. In spite that the eNB instructs the UE-B to listen on the same RBs (Resource Blocks) on which the UE-A is transmitting data, in network-assisted D2D communication, the eNB is involved in control information exchange but never involved in data exchange 22. The link between the D2D users is also called side link (SL) and should be distinct from uplink (UL) and downlink (DL). The SL is carved out from the UL frequency resources, where the interference is expected to be less severe.

Fig. 3 shows the sequence chart for Diffie-Hellman's (DH) key exchange protocol. Alice initiates a session by sending a request to Bob. Bob accepts the request and acknowledges back. Alice generates public and private key pair of length 3072 bits using DH. The computation time required for key pair generation is 0.05 (Sedidi and Kumar, 2016) seconds and subsequently sends its public key to Bob. After receiving Alice's public key, Bob generates his own key pairs and sends his public key back to Alice. Once the public key is exchanged by both parties, the session key is established after a computation time of 0.018 seconds.

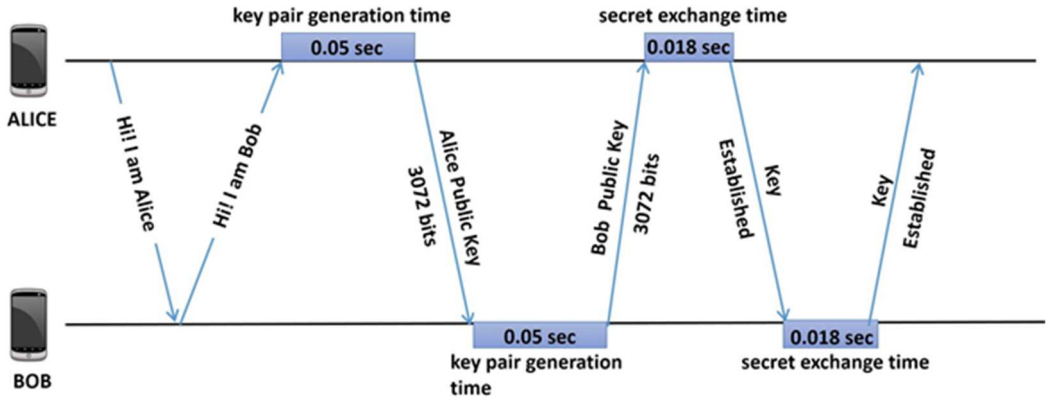

Fig. 3. Sequence chart Diffie-Hellman key exchange protocols in simuLTE

Impact of increasing D2D pairs

We have performed extensive simulations for ECC, DH and RSA in underlay D2D communication scenarios by considering no cellular equipment in the network. To ascertain the impact of an increasing number of devices on key establishment delay, we increased the number of D2D pairs from 1 to 16. As shown in Fig. 4, key establishment delays for ECC, DH, and RSA generally increase for the increasing number of pairs. For a smaller number of pairs, we observed that delay for DH and ECC exhibits the minimum difference. However, for a larger number of devices, the difference between ECC and DH increases significantly. More specifically, the difference between ECC and RSA increases from 0.131s to 0.902s when D2D pairs are increased from 1 to 16 (Alvarez et al., 2017). Interestingly, we have also observed that the difference between RSA and DH is reduced significantly for a larger number of D2D pairs. For instance, the difference between RSA and DH is reduced from 1.666s to 0.8574s as D2D pairs increase from 1 to 16 (Virdis et al., 2016). This shows that for a higher number of D2D pairs, DH key establishment delay starts approaching that of RSA. In general, we note that ECC outperforms the DH and RSA in terms of having the least key establishment delay.

Impact of Cellular Users on Key Establishment Delay

To comprehend the effect of cellular users in the given scenario, we now present the results of average key establishment delay and the number of transmitted packets. For this analysis, the number of D2D pairs is fixed at eight while the number of cellular users is increased gradually. Fig. 5 and Fig. 6 depict the results for the increasing number of cellular users for the three key exchange protocols. The number of cellular users that communicate in the cell via eNodeB is increased from 0 to 20. The cellular users are assumed to be running VoIP applications, while D2D pairs are running key exchange algorithms for session key establishment. It can be seen from the figure that for key establishment, the average number of packets sent for DH is the largest among the three protocols, while the least number of packets has been sent for RSA. One can observe that the number of transmitted packets generally increases with an increase in the number of cellular users in the network. In terms of key establishment delay, the impact of the increased number of cellular users is shown in Fig. 6. The DH incurs the largest key establishment delay due to the higher number of packets sent by the D2D pairs

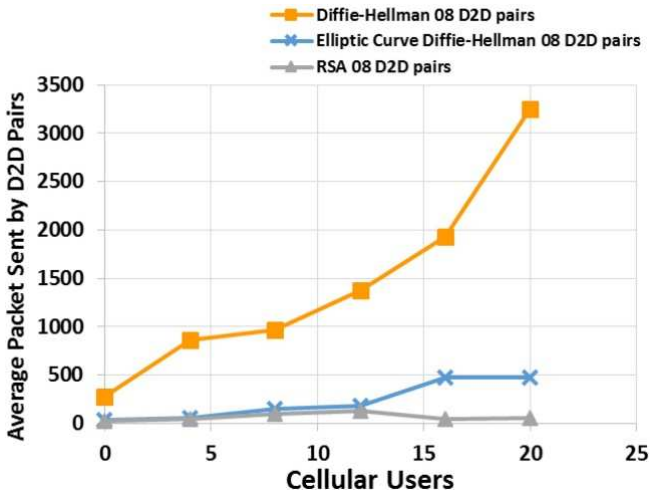

Fig. 4. Average key establishment delay for ECC, DH, and RSA

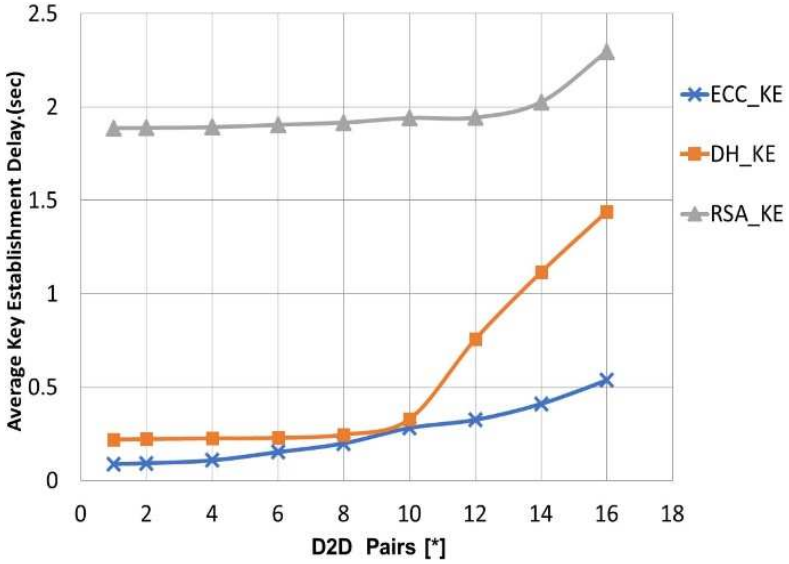

Fig. 5. Average packet Sent by D2D users

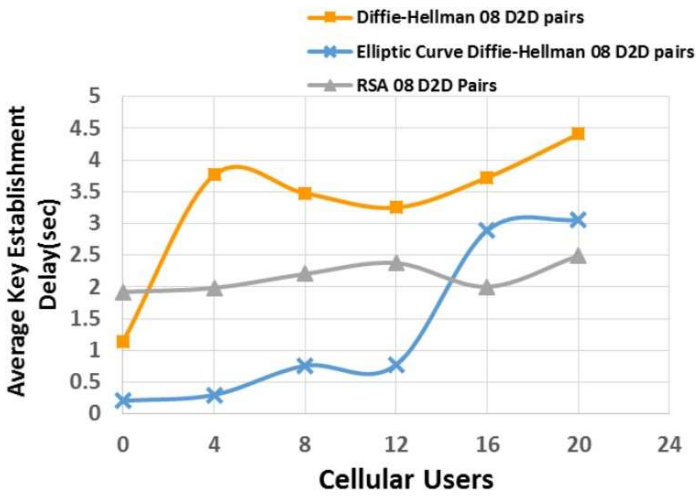

Fig. 6. Average key establishment delay

Impact of interference on average key establishment delay in a single cell

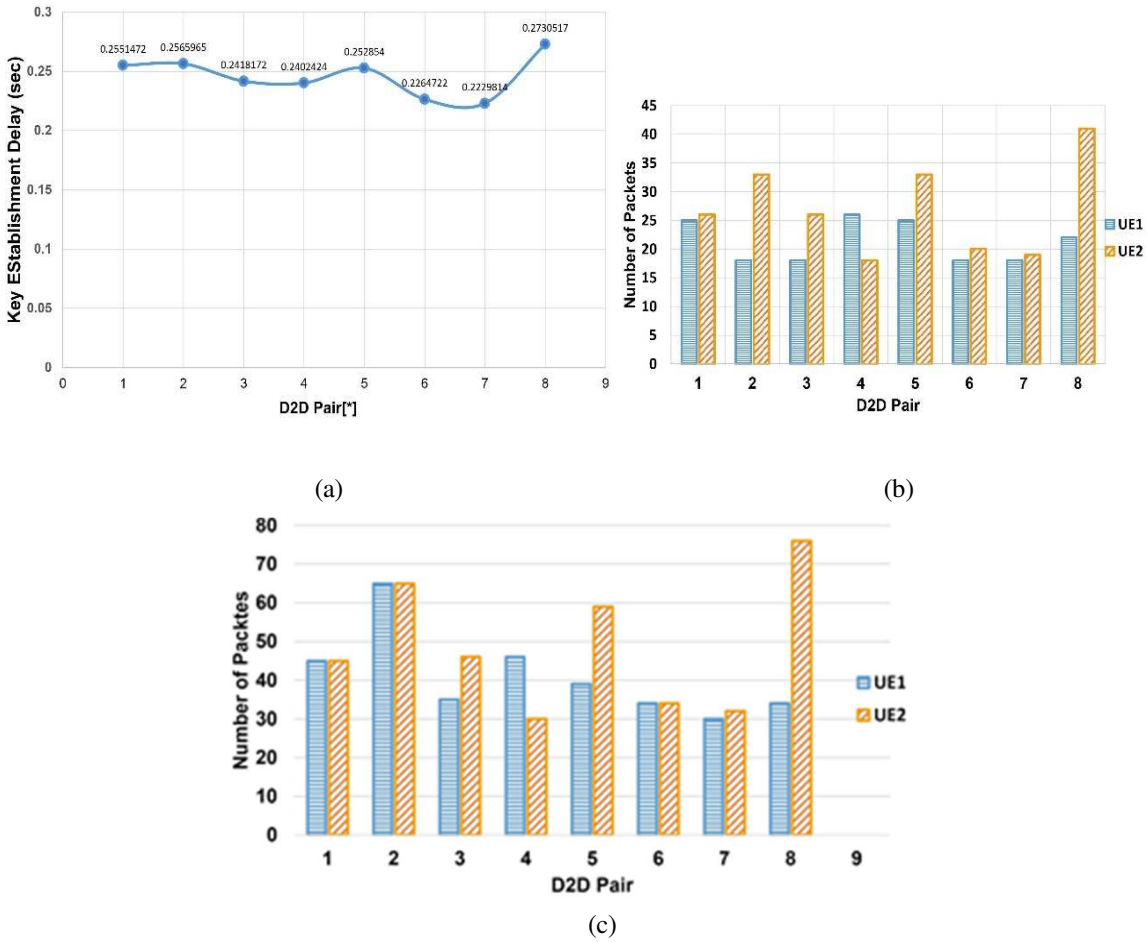

Fig. 7. (a). Impact of interference on average key establishment delay, Fig. 7. (b). Sent packet to lower layer, Fig. 7. (c). Received packet from a lower layer

To assess the impact of interference and retransmissions on key establishment delay, we consider statistics of individual D2D pairs as depicted in Fig.7(a), Fig.7 (b), and Fig.7 (c). It can be observed from Fig.7(a) that the key establishment delays for the 2nd, 5th, and 8th pair are considerably higher than those of other pairs. This phenomenon can be explained by observing Fig.7 (b) and Fig.7 (c), which show the number of the MAC layer packets sent and received for all eight D2D pairs. It is evident that the number of MAC packets is much higher for the 2nd, 5th, and 8th pairs, primarily retransmissions due to increased interference. The packet size significantly affects the network performance; a larger packet size will take a longer transmission time, resulting in more chance of collision at the physical layer. The key size was used as the length of the payload of the packet during our simulation. RSA and DH use 50% longer keys than ECC. When the performance of ECC, RSA and DH was analysed in a highly contended environment, we observed that the interference influenced RSA and DH more than ECC. Consequently, this resulted in ECC in minimal communication overhead and key establishment delay.

Conclusions

This work has presented the analysis of key establishment and exchange mechanisms in D2D communication scenarios based on three public-key cryptographic (PKC) techniques: RSA, DH, and ECC. The key size is directly tied to computation power; ECC uses significantly smaller keys than those required by RSA or DH yet delivers equivalent cryptographic strength. The key pair generation and agreement time of ECC are much faster than RSA and DH. Thus, ECC can save roughly 10% of computational overhead than DH and RSA. The results gathered through extensive simulations demonstrate that ECC affords minimal communication overhead and key establishment delay compared to DH and RSA. This performance is considered even more critical when the network size significantly increases, and the delay requirements need to be kept to a minimum to ensure end-users' quality of service (QoS) requirements. The results also show that the RSA has an advantage over DH in terms of

communication overhead for larger network sizes. More specifically, as the number of D2D pairs in the network increases to twelve or more, the communication overhead for DH becomes higher than that for RSA and ECC. This is critical for future ultra-dense networks where hundreds of devices may simultaneously communicate with each other. The analysis conducted in this work in terms of key establishment delays and communication overhead for ECC, DH and RSA can be of critical importance for assessing the suitability of these techniques in the forthcoming 5G network incorporating the D2D communication framework. This work has focused on the key establishment in a unicast scenario. However, in a dense multiuser network, cooperative schemes can be used to minimise the delay in the key establishment procedure. Motivated by this, we intend to extend our work to exploit group key establishment in a multicast scenario. This exciting approach in a cooperative D2D environment can open new avenues for the provisioning of robust and flexible key establishment protocols in D2D networks.

References

Amin, R., & Biswas, G. P. (2015). An improved rsa based user authentication and session key agreement protocol usable in tmis. *Journal of Medical Systems*, 39(8), 1-14. https://doi.org/10.1007/s10916-015-0262

Asadi, A., Wang, Q., & Mancuso, V. (2014). A survey on device-to-device communication in cellular networks. *IEEE Communications Surveys & Tutorials*, 16(4), 1801-1819 https://doi.org/10.1109/COMST.2014.2319555

Alvarez, R., Caballero-Gil, C., Santonja, J., & Zamora, A. (2017). Algorithms for lightweight key exchange. *Sensors*, 17(7), 1517. https://doi.org/10.3390/s17071517

Belas, J., Gavurova, B., & Toth, P. (2018). Impact of selected characteristics of SMEs on the capital structure. *Journal of Business Economics and Management*, 19(4), 592-608. https://doi.org/10.3846/jbem.2018.6583

Barskar, R., & Chawla, M. (2016). A survey on efficient group key management schemes in wireless networks. *Indian J. Sci. Technol*, 9(14), 1-16. https://doi.org 10.17485/ijst/2016/v9i14/87972

El-Hamawi, E., Bakhache, B., & Rostom, R. (2014, April). An improved authenticated key agreement protocol for low power networks. In MELECON 2014-2014 17th IEEE Mediterranean Electrotechnical Conference (pp. 426-431). IEEE. https://doi.org/10.1109/MELCON.2014.6820572

Fedorko, I., Bacik, R., & Gavurova, B. (2018). Technology acceptance model in e-commerce segment. Technology acceptance model in e-commerce segment. *Management & Marketing – Challenges for the Knowledge Society*, 13(4), 1242-1256. Doi: 10.2478/mmcks-2018-0034

Fouda, M. M., Fadlullah, Z. M., Kato, N., Lu, R., & Shen, X. (2011). Towards a lightweight message authentication mechanism tailored for smart grid communications. In 2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS) (pp. 1018-1023). IEEE. https://doi.org/10.1109/INFCOMW.2011.5928776

Haus, M., Waqas, M., Ding, A. Y., Li, Y., Tarkoma, S., & Ott, J. (2017). Security and privacy in device-to-device (D2D) communication: A review. *IEEE Communications Surveys & Tutorials*, 19(2), 1054-1079. https://doi.org/10.1109/COMST.2017.2649687

He, D., Wang, H., Khan, M. K., & Wang, L. (2016). Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. *IET Communications*, 10(14), 1795-1802. https://doi.org/10.1049/iet-com.2016.0091

Kabir, K., Gilani, S. M., Rehmanc, G., Sabahat, S. H. Popp, J., Shehzad Hassan, M. A., & Oláh, J. (2021). Tax aspects of mining companies in V4 countries. *Acta Montanistica Slovaca*, 26(1), 47-59. https://doi.org/10.46544/AMS.v26i1.04

Kharroubi, D. (2021). Global workforce diversity management: Challenges across the world. *Ekonomicko-manazerske spektrum*, 15(1), 28-37. https:// doi.org/10.26552/ems.2021.1.28-37.

Kurar, İ. (2021). Research on the determination of recreational experience preferences, expectations, and satisfaction levels of local people. International Journal of Entrepreneurial Knowledge, 9(1), 41-66. https://doi.org/ 10.37335/ijek.v9i1.122

Lampropoulos, G., Siakas, K., Anastasiadis, T. (2019). Internet of Things in the Context of Industry 4.0: An Overview. International Journal of Entrepreneurial Knowledge, 7(1), 4-19. https://doi.org/10.2478/ijek-2019-0001

Liu, Y., Wang, L., & Chen, H. H. (2014). Message authentication using proxy vehicles in vehicular ad hoc networks. *IEEE Transactions on vehicular technology*, 64(8), 3697-3710. https://doi.org/10.1109/TVT.2014.2358633

Mach, P., Becvar, Z., & Vanek, T. (2015). In-band device-to-device communication in OFDMA cellular networks: A survey and challenges. *IEEE Communications Surveys & Tutorials*, 17(4), 1885-1922 https://doi.org/. 10.1109/COMST.2015.2447036.

Mittal, H. (2020). How does the institutional context of an emerging economy shape the innovation trajectory of different types of firms? A case study of India. *Ekonomicko-manazerske spektrum*, 14(2), 36-51. https://doi.org/10.26552/ems.2020.2.36-51.

Niu, Q. (2014). ECDH-based Scalable Distributed Key Management Scheme for Secure Group Communication. *J. Comput*., 9(1), 153-160. https://doi.org/. 10.4304/jcp.9.1.153-160

Nardini, G., Virdis, A., & Stea, G. (2016). Simulating device-to-device communications in OMNeT++ with SimuLTE: scenarios and configurations. arXiv preprint arXiv:1609.05173. https://summit.omnetpp.org/archive/2016/index.html

Oláh, J., Hidayat, Y. A., Gavurova, B., Khan, M. A., & Popp, J. (2021). Trust levels within categories of information and communication technology companies. *Plos one*, 16(6), e0252773, 1-21. https://doi.org/10.1371/journal.pone.0252773

Pereira, P. P., Eliasson, J., & Delsing, J. (2014). An authentication and access control framework for CoAP-based Internet of Things. In IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society (pp. 5293-5299). IEEE. https://doi.org/10.1109/iecon.2014.7049308

Shen, W., Hong, W., Cao, X., Yin, B., Shila, D. M., & Cheng, Y. (2014). Secure key establishment for device-to-device communications. In 2014 IEEE Global Communications Conference (pp. 336-340). IEEE. https://doi.org/10.1109/glocom.2014.7036830

Sedidi, R., & Kumar, A. (2016). Key exchange protocols for secure device-to-device (D2D) communication in 5G. In 2016 Wireless Days (WD) (pp. 1-6). IEEE. Stallings, W. (2006). Cryptography and network security, 4/E. Pearson Education India. https://doi.org/10.1109/glocom.2014.7036830

Virdis, A., Stea, G., & Nardini, G. (2015). Simulating lte/lte-advanced networks with simulate. In Simulation and Modeling Methodologies, Technologies, and Applications (pp. 83-105). Springer, Cham. https://doi.org/10.5220/0005040000590070

Virdis, A., Nardini, G., & Stea, G. (2016, July). Modeling unicast device-to-device communications with SimuLTE. In 2016 1st International Workshop on Link-and System Level Simulations (IWSLS) (pp. 1-6). IEEE. https://doi.org/10.1109/iwsls.2016.7801579

Wei, L., Hu, R. Q., Qian, Y., & Wu, G. (2014). Enable device-to-device communications underlaying cellular networks: challenges and research aspects. *IEEE Communications Magazine*, 52(6), 90-96. https://doi.org/10.1109/mcom.2014.6829950

Wang, M., & Yan, Z. (2015). Security in D2D communications: A review. In 2015 IEEE Trustcom/BigDataSE/ISPA (Vol. 1, pp. 1199-1204). IEEE. https://doi.org/10.1109/trustcom.2015.505