Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6983655, 9 pages
https://doi.org/10.1155/2022/6983655

Research Article

Towards Security Mechanism in D2D Wireless Communication: A 5G Network Approach

Divya Gupta,[1] **Shalli Rani**,[2] **Aman Singh**,[3,4] **and Juan Luis Vidal Mazon**[5,6]

[1]*Department of Computer Science and Engineering, Chandigarh University, Mohali 140413, India*
[2]*Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*
[3]*Faculty of Engineering, Universidade Internacional Do Cuanza, Estrada Nacional 250, Bairro Kaluapanda, Cuito-Bié, Angola*
[4]*Department of Engineering, Universidad Internacional Iberoamericana, Arecibo 00613, Puerto Rico, USA*
[5]*Higher Polytechnic School, Universidad Europea del Atlántico, C/Isabel Torres 21, 39011 Santander, Spain*
[6]*Department of Project Management, Universidad Internacional Iberoamericana, Campeche 24560, Mexico*

Correspondence should be addressed to Aman Singh; aman.singh@unic.co.ao

Received 4 April 2022; Revised 23 May 2022; Accepted 12 July 2022; Published 22 July 2022

Academic Editor: Han Wang

Device-to-device (D2D) communication has attracted many researchers, cellular operators, and equipment makers as mobile traffic and bandwidth demands have increased. It supports direct communication within devices with no need for any intermediate node and, therefore, offers advantage in 5G network while providing wide cell coverage range and frequency reuse. However, establishing acceptable and secure mechanism for D2D communication which ensures confidentiality, integrity, and availability is an issue encountered in this situation. Furthermore, in a resource-constrained IoT environment, these security challenges are more critical and difficult to mitigate, especially during emergence of IoT with 5G network application scenarios. To address these issues, this paper proposed a security mechanism in 5G network for D2D wireless communication dependent on lightweight modified elliptic curve cryptography (LMECC). The proposed scheme follows a proactive routing protocol to discover services, managing link setup, and for data transfer with the aim to reduce communication overhead during user authentication. The proposed approach has been compared against Diffie–Hellman (DH) and ElGamal (ELG) schemes to evaluate the protocol overhead and security enhancement at network edge. Results proved the outstanding performance of the proposed LMECC for strengthening data secrecy with approximate 13% and 22.5% lower overhead than DH and ELG schemes.

1. Introduction

1.1. Background. Device-to-device (D2D) communication eliminates the need for an intermediary node. In mobile networks, D2D communication offers several advantages [1]: Firstly, it may be used to extend the cell coverage in a cellular network while providing facilities to act as communication bridge for data transmission outside the coverage range. Secondly, by delivering data directly between devices, D2D communication helps to lower the base station's energy usage. Finally, the effectiveness of reusing the same radio frequency has been improved. The distance between devices in D2D communication is very less. This means that in a D2D communication scenario, radio frequency interference is reduced, allowing numerous data to be transmitted on the same radio frequency. Due to these benefits, the D2D communication feature is adopted by long term evolution (LTE) advanced 4G networks. [2].

However, on a mobile network, D2D communication based on proactive routing protocol has certain security

concerns [3]. Device discovery, link setup, and data transfer are the three operations that make up the proactive D2D communication mechanism [4]. There is no authentication method for confirming device identification in this process. Another node responds to a request for a setup link using an acknowledgement message. Furthermore, throughout the communication process, D2D communication does not employ any kind of encryption to provide confidentiality and message authentication for integrity. This implies the attacker can use DoS attacks, eavesdropping, and network spoofing to carry out assaults [5, 6] .

1.2. Motivation. Recently, IoT is coupled with the 5G to meet its service expectations which corresponds to massive machine type communication (mMTC) and ultrareliable low latency communication (URLLC) [7]. IoT applications, on the other hand, deal with a lot of sensitive data, yet IoT devices have restricted performance, memory, and power consumption. Because traditional security solutions cannot be applied or processed effectively, these properties of IoT make the above-mentioned security concerns crucial to get handle. We need a secure system with an appropriate authentication mechanism between devices to tackle the security problems of D2D communication. Furthermore, given the limited resources available, it must be made light.

For resource-constrained devices, lightweight cryptography may be an appropriate option. Elliptic curve cryptography (ECC) is the most common lightweight asymmetric key method. It provides 128-bit cryptographic security with a 256-bit key, which is relatively smaller than the 3072-bit key being used in public key encryption scheme RSA [8].

1.3. Contribution. The following are the key contributions of this study:

(i) This paper presents a secure D2D communication system based on lightweight modified ECC (LMECC) for a 5G IoT network

(ii) The D2D communication system has been established in three phases: service discovery, link setup, and data transfer using a proactive routing protocol

(iii) The proposed security mechanism based on LMECC has been evaluated and compared against Diffie–Hellman and ElGamal security enhancement techniques

(iv) The experiments conducted using MATLAB for overhead analysis and security enhancement proved that LMECC can better manage the 5G IoT devices

The remaining paper is structured as mentioned below: The related work done for security in D2D communication has been discussed in Section 2. Section 3 presents the proposed system model. The D2D communication process with its three operations is presented in Section 4. The existing security enhancement mechanism along with proposed security enhancement in D2D communication has been further explained in Sections 5 and 6. The Section 7 presents the results obtained after performing experimentation on proposed approach. Finally, the summary of the study is presented in the form of conclusion in Section 8.

2. Related Work

One of the most significant data transmission concerns is security. Nowadays, with the emergence of variety of smartphone apps to manage the Internet of things, mobile phone usage has increased. The extensive usage of cell phones in the industry, on the other hand, drew academics' attention to the need of protecting consumers and customers. Many models for encrypting and decrypting data outsourcing have been developed to address these difficulties. However, new dangers continue to emerge as a result of new attack tactics and hostile behavior by adversaries.

The protection of D2D communication data is critical in the face of harmful assaults [14]. Secure D2D connections between mobile devices, on the other hand, remained a problem. The work in [10] suggested a lightweight authentication technique based on ElGamal encryption. This work provides a public key infrastructure (PKI)-based authentication technique that uses a mix of ECC for key pair selection and ElGamal encryption for secret key exchange. Over public key infrastructure, another lightweight cryptography scheme considering both ECC and ElGamal has been presented in [9]. This scheme utilizes ECC for key generation and ElGamal for encryption/decryption of messages. Using smartphone sensor behavior analysis, authors in [11] suggested a D2D authentication technique. For group authentication, their authentication technique uses certificateless cryptography, and for continuous authentication, they use user behavior analysis retrieved from smartphone sensors. Further, authors in [15] designed another key exchange mechanism mainly suitable for LTE-based D2D communication which is extendable for use in 5G network. ECC-based symmetric keys are used to create their method. Similar to this, the work in [12] designed an authentication mechanism along with device detection and privacy protection with use of identity-based encryption. Another work in [13] proposed lightweight multilayer authentication scheme suitable for wireless body area networks (WBAN). To support lightweight authentication with group key design algorithm, this work again used ECC algorithm. The computation performed using Foci calculations ensures low computation cost while providing high security.

The majority of these investigations employ ECC-based cryptographic methods to enable authentication and data confidentiality/integrity. However, they have certain drawbacks, such as the inability of some of the results to give anonymity, or the fact that the studies did not discuss in detail on the data transmission stage of D2D communication (refer Table 1). Furthermore, the majority of current systems rely solely on lightweight public key techniques, rather than lightweight symmetric encryption algorithms. Our suggested system can increase the efficiency and security of D2D communication because it employs the lightweight encryption to handle all of our security concerns and all of the phases in D2D communication.

Table 1: Description of existing work.

Ref	Year	Proposed scheme	Strength	Weakness
[9]	2017	Lightweight cryptography scheme considering both ECC and ElGamal	ECC for key generation and ElGamal for encryption/ decryption of messages	High overhead
[10]	2019	Lightweight authentication technique based on ElGamal encryption	Use a mix of ECC for key pair selection and ElGamal encryption for secret key exchange	No lightweight symmetric encryption
[11]	2019	Authentication technique uses certificateless cryptography	D2D authentication technique	Asymmetric encryption with high overhead
[12]	2020	Authentication mechanism along with device detection and privacy protection with the use of identity-based encryption	Authentication, privacy protection	Weak encryption mechanism
[13]	2021	Lightweight multilayer authentication scheme	ECC algorithm with low computation cost	No lightweight symmetric encryption
Proposed work	2022	Security mechanism in 5G network for D2D wireless communication dependent on lightweight modified elliptic curve cryptography (LMECC)	Lightweight symmetric encryption with low protocol overhead	More focused on 5G D2D communication with/without various security challenges

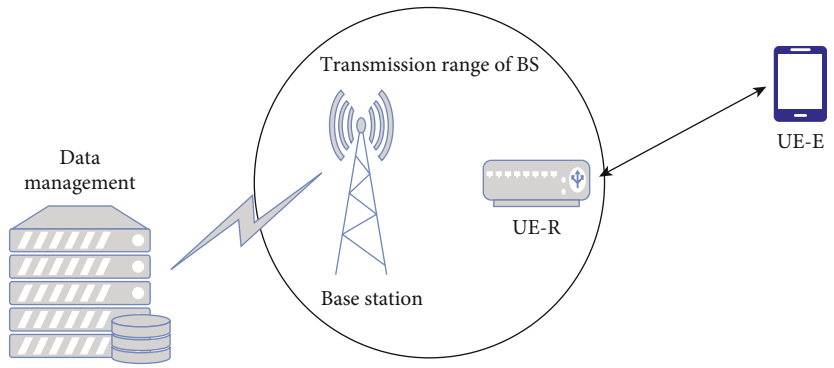

Figure 1: System model scenario.

Table 2: Abbreviation list.

Notations	Definition
DM	Data management
UE	User equipment
BS	Base station
D2D	Device to device
ECC	Elliptic curve cryptography
Non	A random value
*D*sig	Digital signature
PU_k	Public key
PR_k	Private key
key_{sec}	Secret key

3. Proposed System Model

For a 5G IoT network, this section presents a secure D2D communication system model. Figure 1 depicts the suggested secure D2D communication paradigm. 5G network components such as user equipment (UE), base station (BS), and user data management (DM) participate in D2D communication (refer Table 2). A user equipment (UE) is a physical mobile device in direct connection with other devices in proposed model. The base station (BS) connects UE to cellular networks. Within the service region, BS can work with UE-Relay (UE-R). UE-R, like other UEs, must respect the cellular network's function.

Furthermore, before the discovery process can begin, UEs must first register for proximity service discovery and D2D services. In this study, we execute procedures such as registration and authentication for all UEs. Following registration, the proximity service application on each device may begin initiating requests or monitoring the proximity services of other UEs. The BS may help in advertisement so that it is available to all D2D-enabled UEs. We further assume that in the envisioned situation, all UEs and the BS support both open proximity service and network proximity service.

4. D2D Communication Process

This section explains the complete D2D communication establishment process by providing details about service discovery, link setup, and data transfer as these are the three

operations that make up the D2D communication mechanism.

4.1. Service Discovery. The initial phase of secure D2D communication, i.e., service discovery, follows a proactive approach where BS advertises the available service information. Proactive protocol is particularly important for commercial businesses that wish to market themselves and deliver information to their clients [16]. In our approach, just one BS is taken into account for simplicity [3]. UE-R receives service advertisement information from BS and transmits it to UE-E. Any UE-E(s) that are interested should respond to this message. The communication during the device discovery phase is multicast. They do, however, exchange unicast messages after completing the D2D discovery phase. Furthermore, even though UE-E does not require special service information, a D2D connection is established between UE-R and UE-E. The PUSH mechanism is an example of this kind.

The steps involved in discovery of services have been shown in Figure 2 and are explained below:

(i) Service advertisement: Through broadcast messages, BS offers "Service advertisement" to UEs throughout its coverage

(ii) Service invitation: Being a relay device, the UE-R delivers a "Multicast D2D service invitation" to the UE-E in its close vicinity(s)

(iii) Request initialization: UE-E accepts the service invitation by sending a unicast "D2D request initialization" message to UE-R

(iv) Request for approval: UE-R requests D2D approval from BS by transmitting information about UE-E

(v) Checking operations: D2D checking operations for UE-E are represented by steps 5, 6, and 7. In step 5, "Forwards D2D request" is sent by BS to the DM. Following that, DM saves UE-E's information in its database and verifies channel capacity for it. Following this, DM responds to UE-R by sending a "D2D request admission" message via BS

4.2. Link Setup and Data Transfer. After the successful discovery of services and device for D2D communication, the next operation is to setup links and to transfer data. The complete process of link setup and data transfer has been divided in to several steps which have been illustrated in Figure 3.

(i) Step 1: UE-E sends "D2D service selection" to UE-R and, therefore, selects the exact service in which it is interested

(ii) Step 2: The request for service is passed from UE-R to the BS

(iii) The allocation of service from BS to UE-R is represented by steps 3, 4, and 5. It mandates service confirmation from DM, as well as the processing and distribution of the desired service data

(iv) Step 6: UE-R uses unicast messages to transmit information about the "Relay D2D request"

5. Existing Security Enhancement Mechanisms

This section provides knowledge on the existing authentication schemes for security enhancement based on Diffie–Hellman (DH) and ELG schemes. Both the schemes are then compared against proposed proactive service discovery protocol for security enhancement in D2D communication environment in Section 7.

5.1. Diffie–Hellman (DH) Scheme. This approach assigns responsibility to two communicating UEs to generate and use a common shared secret key for message encryption/decryption during communication process. Initially, out of all available numbers such as $1, 2, 3, \cdots, W-1$, where W is a large prime number and is known to both UEs and UE-R and UE-E generate a secret number x and y, respectively. Afterwards, a public key is computed by both UEs, UE-R computes $\mathrm{PU}_k(\mathrm{UE}-R) = h^x \bmod W$ and UE-E computes $\mathrm{PU}_k(\mathrm{UE}-E) = h^y \bmod W$. Here h is a common generator known to both UEs in advance.

Both UEs initiate the process of digital signature as listed in the following steps:

Step 1: UE-E and UE-R generate the random nonce values Non_E and Non_R, respectively.

Step 2: UE-E computes hash value of Non_E, encrypts this hash with its secret number y, and attaches to Non_E to construct digital signature of its own. Therefore, digital signature of UE-E $D_{\mathrm{sig}}(\mathrm{UE}-E)$ is represented as:

$$= [\mathrm{Encrypt}[\mathrm{hash}(\mathrm{Non}_E), y], \mathrm{Non}_E]. \quad (1)$$

Step 3: UE-R computes hash value of Non_R, encrypts this hash with its secret number x, and attaches to Non_R to construct digital signature of its own. Therefore, digital signature of UE-R $D_{\mathrm{sig}}(\mathrm{UE}-R)$ is represented as:

$$= [\mathrm{Encrypt}[\mathrm{hash}(\mathrm{Non}_R), y], \mathrm{Non}_R]. \quad (2)$$

Step 4: UE-E fetches the Non_R from D_{sig} and calculates message as:

$$\mathrm{Mes}_E = \mathrm{Encrypt}[\mathrm{hash}(\mathrm{Non}_R\mathrm{Non}_E), \mathrm{PU}_k(\mathrm{UE}-R). \quad (3)$$

Step 5: UE-R fetches the Non_E from D_{sig} and calculates message as:

$$\mathrm{Mes}_R = \mathrm{Encrypt}[\mathrm{hash}(\mathrm{Non}_E\mathrm{Non}_R), \mathrm{PU}_k(\mathrm{UE}-\mathrm{E}). \quad (4)$$

Both UEs decrypt Mes_R and Mes_E using their private key and verify the $[\mathrm{hash}(\mathrm{Non}_E\mathrm{Non}_R)]$. After successful verification, both UEs agree on formation of common secret key for encryption/decryption of rest of the messages during their communication process in network. The common

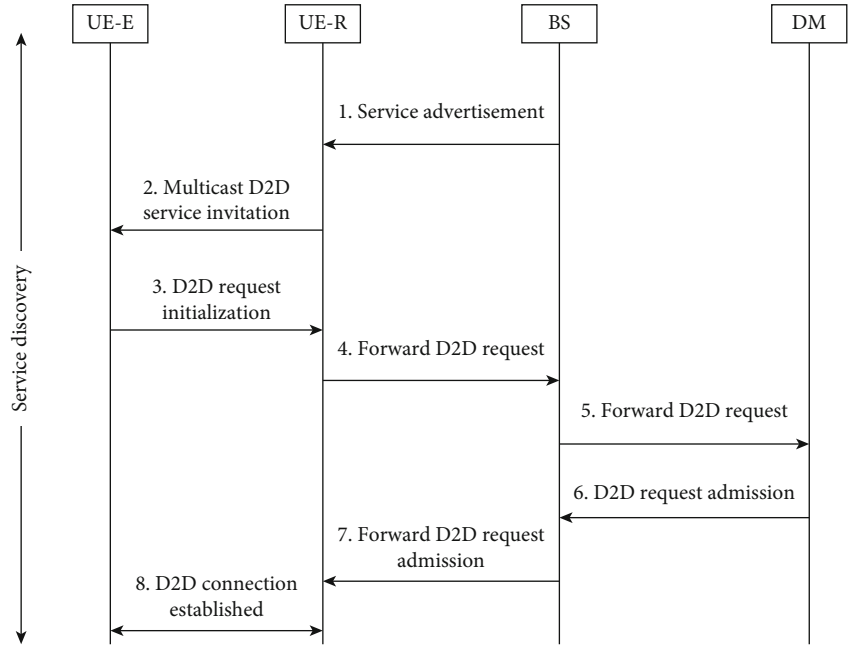

Figure 2: Service discovery process.

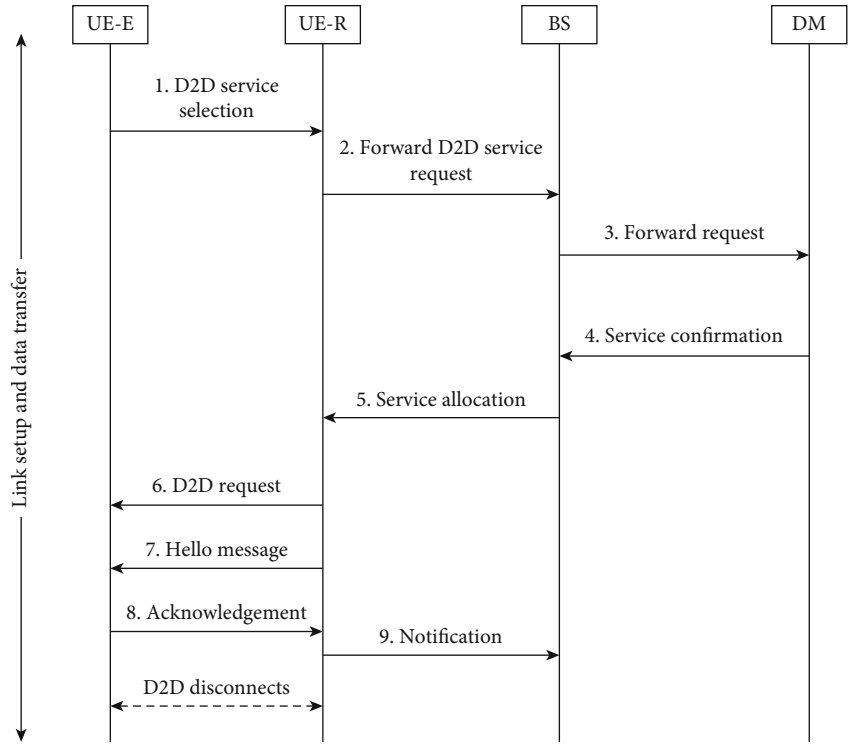

Figure 3: Link setup and data transfer process.

secret key is computed as:

$$\text{Key}_{\text{sec}} = (\text{PU}_k(\text{UE} - R))x = (\text{PU}_k(\text{UE} - E))y. \quad (5)$$

5.2. ELGamal (ELG) Scheme. This scheme allows exchange of secret key on an unsecured channel by users. This key is further used for message encryption [17]. Hence, security in this scheme is solely based on the difficulty lies in solving DH problem. Initially, out of all available numbers such as $1, 2, 3, \cdots, W - 1$, where W is a large prime number and is known to both UEs and UE-R and UE-E generates a secret number x and y, respectively. Afterwards, a public key is

computed by both UEs, UE-R computes $\mathrm{PU}_k(\mathrm{UE}-R) = h^x \bmod W$, and UE-E computes $\mathrm{PU}_k(\mathrm{UE}-E) = h^y \bmod W$. Here, h is a common generator known to both UEs in advance.

This scheme makes use of private key and public key for encryption and decryption, respectively.

Initially, UE-E calculates the hash $\mathrm{m} = \mathrm{Hash}(\mathrm{Mes})$ to sign a message such that m is a number in the range from $0 \le m \le W-1$. Further to this, UEs start with the process of digital signature as listed in the following steps:

Step 1: UE-E selects a random number A in such a way that A is relatively prime to $W-1$, and the following conditions hold: $1 \le A \le W-1$ and $\gcd(A, W-1) = 1$

Step 2: UE-E calculates $D_1 = h^A \bmod W$

Step 3: UE-E calculates $A^{-1} \bmod (W-1)$

Step 4: UE-E computes $D_2 = A^{-1}(m - AD_1) \bmod (W-1)$

Step 4: Finally, digital signature consists of $D_{\mathrm{sig}}UE-E = (D_1, D_2)$

The UE-R verifies signature as:

Step 1: UE-R calculates $F_1 = h^m \bmod W$

Step 2: UE-R calculates $F_2 = PU_k(UE-E)^{D_1}(D_1)^{D_2} \bmod W$

The digital signature is valid if $F_1 = F_2$, then UE-R authenticate UE-E.

6. Proposed Security Mechanism in D2D Communication

The proposed mechanism for providing security in D2D communication utilizes lightweight modified elliptic curve cryptography (LMECC). The traditional elliptic curve cryptosystem (ECC) is a cutting-edge lightweight cryptosystem that uses smaller keys than other modern cryptosystems like RSA [2]. As a result, ECC can perform additive finite group operations more effectively than RSA's modular exponentiation process.

ECC follows random selection of private key. Moreover, in case the parameters picked at random are not correctly chosen, wrong calculations will lead to inaccurate plain text formation. The objective is to keep intruders out of the messages sent between UEs. We created a protocol with security enhancements for this purpose. The communication channel between UEs is open; therefore, an attacker could intercept the messages. Due to identity-oriented encryption as well as the LMECC protocol, two UEs in close proximity to each other can discover themselves, setup authentication and key agreement in this part. As shown in Figure 4, on reception of D2D invitation from UE-R, UE-E commences the security enhancement procedure.

LMECC uses asymmetric cryptography, which consists of both private and public keys. The user who is in charge of the private key is responsible for its safety. A shared key generation point PT is agreed upon by two communicating users. Let communicating users UE-R and UE-E's private keys be $\mathrm{Key}_{\mathrm{Pr}_R}$ and $\mathrm{Key}_{\mathrm{Pr}_E}$, respectively. Their public keys are then computed as $\mathrm{Key}_{\mathrm{PU}_R} = \mathrm{Key}_{\mathrm{Pr}_R}.\mathrm{PT}$ and $\mathrm{Key}_{\mathrm{PU}_E} = \mathrm{Key}_{\mathrm{Pr}_E}.\mathrm{PT}$, respectively.

The authentication procedure begins with the selection of domain parameters, followed by computation using LMECC and the Diffie–Hellman key exchange protocol. LMECC is a two-factor authentication system.

(i) Step 1: To pick the elliptic curve parameters, two users are UE-R and UE-E

(ii) Step 2: User UE-R selects PT on the selected elliptic curve and transmits it to user UE-E

(iii) Step 3: UE-R chooses the private key, $\mathrm{Key}_{\mathrm{Pr}_R}$ to be kept with him

(iv) Step 4: $\mathrm{Key}_{\mathrm{Pr}_R}$ generates the public key, which is then sent to UE-E

(v) Step 5: The private key $\mathrm{Key}_{\mathrm{Pr}_E}$ is chosen by UE-E and kept by him

(vi) Step 6: The public key after generation is forwarded to the UE-R

(vii) Step 7: UE-R computes the last verification point, $K_{\mathrm{UE}_R} = \mathrm{Key}_{\mathrm{Pr}_R}.\mathrm{Key}_{\mathrm{PU}_E}$

(viii) Step 8: User UE − E calculates the final verification point as follows: $K_{\mathrm{UE}_E} = \mathrm{Key}_{\mathrm{Pr}_E}.\mathrm{Key}_{\mathrm{PU}_R}$

(ix) Step 9: The concept of a shared secret key is implemented as:-
$K_{\mathrm{UE}_R} = \mathrm{Key}_{\mathrm{Pr}_R}.\mathrm{Key}_{\mathrm{PU}_E} = \mathrm{Key}_{\mathrm{Pr}_R}.\mathrm{Key}_{\mathrm{Pr}_E}.\mathrm{PT} = K_{\mathrm{UE}_E}$

7. Results and Discussions

The performance of the proposed LMECC is being evaluated for overhead analysis using MATLAB simulation environment. The considered scenario consists of 100 devices uniformly distributed in a $100\,\mathrm{m} \times 100\,\mathrm{m}$ cell. Inside the multicast group, including all user equipments, a portion of devices is served according to proposed approach, while those in worst channel conditions receive data via D2D connections. A bandwidth of 20 MHz with 100 RBs is available. The results retrieved from overhead calculation will decide the suitability of security scheme for D2D communication.

7.1. Overhead Analysis. The amount of overhead associated with the proposed design is measured as the count of service discovery messages needed to establish a D2D session between two users. We are assuming total Q UE-Es scattered randomly inside area A and at a distance of P from UE-R. Only q UE-E(s) desire to communicate with UE-R via D2D, and suppose $R \le Q$ establish D2D pairs, requiring proximate service (ProSe) discovery. For every D2D setup based on LMECC scheme, 18 handshakes are required. In addition, the BS sends a multicast message to all UEs on a regular basis, resulting in a total of $(2 + 18R)$ handshakes for R D2D pairs. On the other hand, Diffie–Hellman protocol for security requires 20 handshakes for every D2D establishment, giving a total of $(2 + 20R)$ handshakes for R D2D

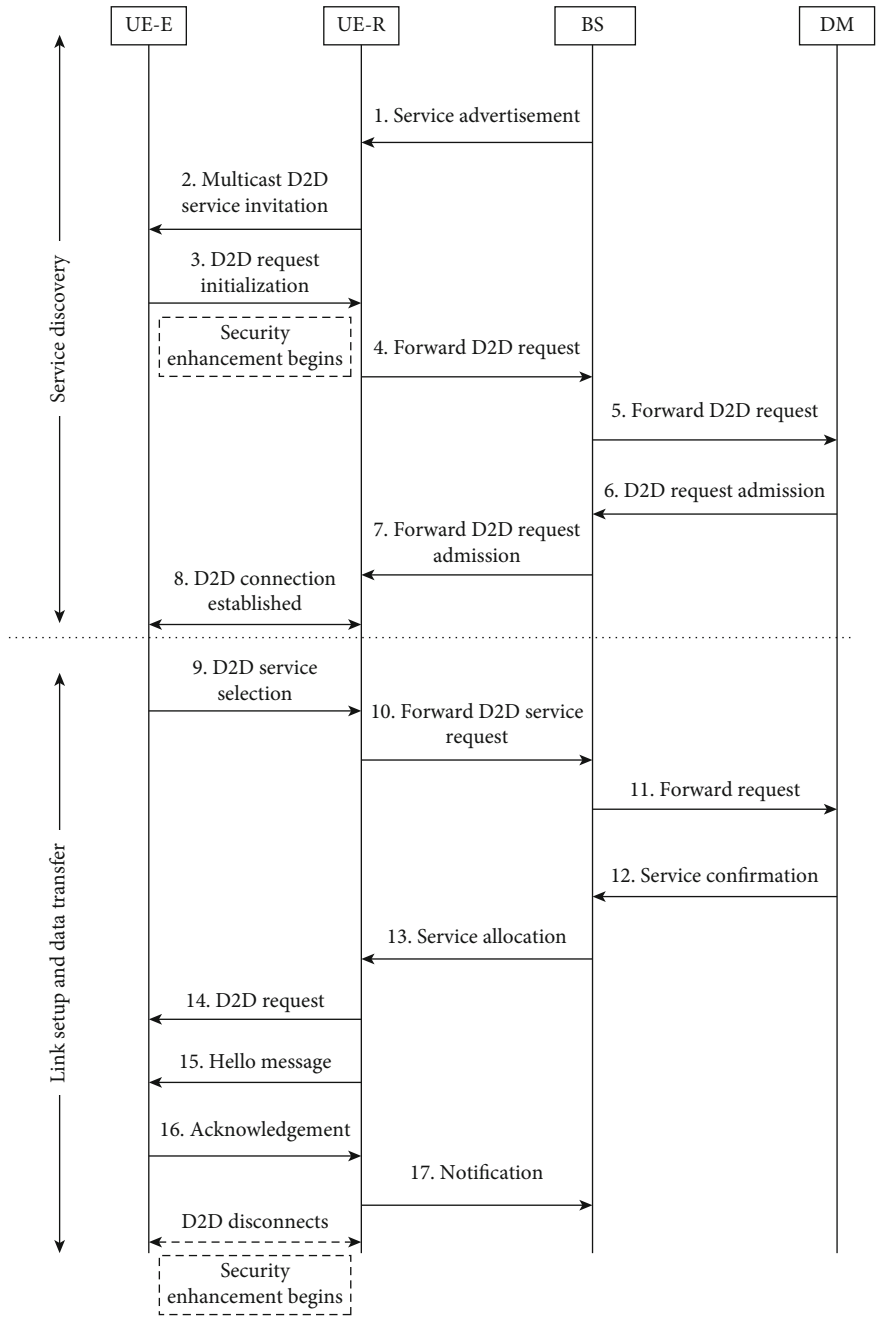

Figure 4: Proposed security in D2D communication.

Table 3: Simulation parameters.

Parameters	Values
Total UEs	20
Total timeslots	20
D2D request per timeslot	6
Number of participating UEs	15

pairs, and the ElGamal protocol requires 22 handshakes for every D2D establishment, giving a total of $(2 + 22R)$ handshakes.

For the proactive procedure, we examine two scenarios when estimating control overhead. In scenario I, the amount of D2D requests in a single timeslot is assumed to be the same across all timeslots. In scenario II, we assume that the quantity of D2D requests changes in each time slot.

Scenario I: Each time slot receives the same number of requests.

This scenario deals with the situation where each timeslot has the equal amount of D2D requests. Considering a scenario in which each timeslot's totality of device to device

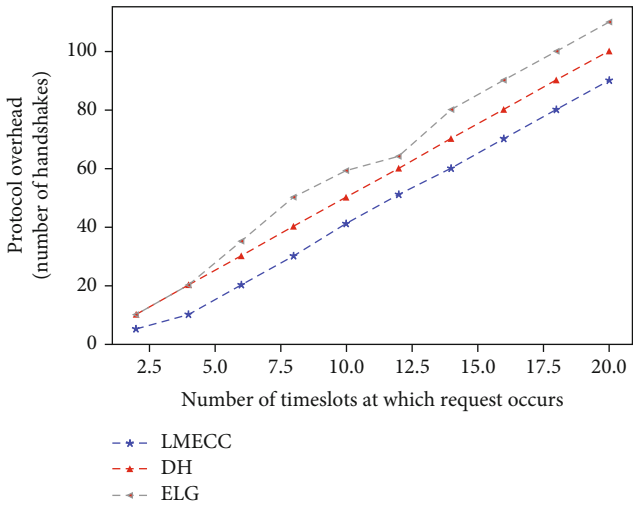

Figure 5: Protocol overhead when $R = 6$.

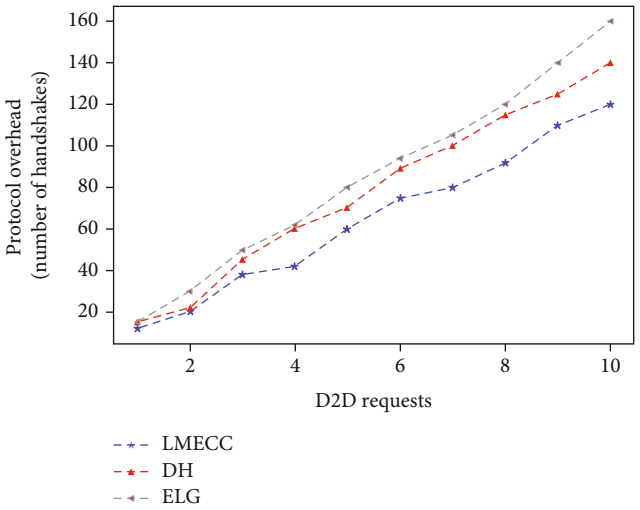

Figure 6: Protocol overhead vs D2D requests.

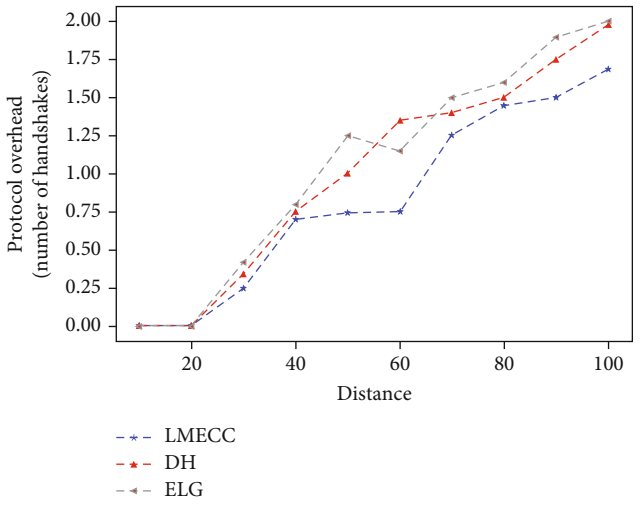

Figure 7: Protocol overhead vs distance.

requests equals to one, and another case, where each timeslot's totality of device to device requests becomes multitudinous, the number of D2D requests is considered to be six for the calculation of the second criterion. The proactive overhead is determined as follows:

$$O_{\mathrm{LMECC}} = \frac{T'(2 + (18 * R)) + \left(2 * \left(T - T'\right)\right)}{T},$$
$$O_{\mathrm{DH}} = \frac{T'(2 + (20 * R)) + \left(2 * \left(T - T'\right)\right)}{T}, \quad (6)$$
$$O_{\mathrm{ELG}} = \frac{T'(2 + (22 * R)) + \left(2 * \left(T - T'\right)\right)}{T}.$$

The parameters chosen for calculating the control overhead in scenario 1 are listed in Table 3.

As shown in Figure 5, when the number of D2D requests is six, it is evident that LMECC is the preferable option since the protocol overhead with LMECC is lower than ELG or DH cryptography, which has a higher overhead. When compared to traditional techniques like ELG or DH, elliptic curve cryptography keys are considerably small and provide equivalent security. At a given number of D2D requests to be 25, this method outperforms the DH scheme by 10.8 percent and the ELG scheme by 23.7 percent for protocol control overhead.

Scenario II: D2D requests appear at random. This scenario represents the occurrence of D2D requests at random in each time frame. As shown in Figure 6, when there is no D2D request, all three forms of proactive protocols have the same overhead. With the growing number of requests, the proactive protocol using LMECC ensures comparatively lesser overhead than using ELG or DH cryptography. Protocol overhead is decreased by 9.37 percent when using the LMECC scheme, and by 18.9 percent when using the ELG scheme, when the number of D2D requests is set to 10.

The number of UE-Es grows as the goal distance increases (refer Figure 7). There are more D2D requests when there are more UE-Es. In comparison to ELG or DH cryptography, LMECC perform better since they have less overhead. If there are multiple UE-E(s) involved in D2D communication, the LMECC is chosen; otherwise, ELG or DH cryptography is used. At a target distance of 100 m, the LMECC scheme reduces protocol overhead by 14.7 percent compared to the DH scheme and by 26.47 percent compared to the ELG scheme.

8. Conclusion

In this study, a proposal is presented to enhance the security in D2D communication networks by leveraging a proactive protocol. To accomplish this, the communication system in D2D environment has been setup in three phases such as service discovery, link setup, and data transfer. The security to the communication in D2D network has been provided through proposed lightweight modified ECC (LMECC) security enhancement scheme. The security mechanism has

been made light to meet the requirements of IoT device's limited resources availability.

In order to evaluate the performance of the proposed protocol, a simulation campaign has been conducted by using the Matlab tool. The performance of the proposed LMECC security enhancement scheme is compared to that of the DH and ELG schemes. The control overhead with the proposed LMECC security enhancement is modest, according to the results. Results proved the outstanding performance of the proposed LMECC for strengthening data secrecy with approximate 13% and 22.5% lower overhead than DH and ELG schemes. Therefore, the proposed approach can be utilized to increase the secrecy and robustness of service discovery in D2D networks in a variety of scenarios. Furthermore, the security of any communication can be enhanced by ensuring confidentiality, integrity, authentication, and availability of message transmission. The listed security parameters can be evaluated to compute the performance of the proposed security enhanced D2D communication approach. As a future work, we tend to implement the proposed approach for this variety of parameters to calculate its security measure. This could be made possible by enabling security and reliability through OFDM-SIS algorithm based on URLLC.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

References

[1] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: a review," *IEEE Communication Surveys and Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[2] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, "Secure D2D communication for 5G IoT network based on lightweight cryptography," *Applied Sciences*, vol. 10, no. 1, pp. 217–231, 2020.

[3] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.

[4] A. Hussein, S. El-Rabaie, and M. G. El-Mashed, "Proactive discovery protocol with security enhancement for D2D communication system," *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 5047–5066, 2021.

[5] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 86–92, 2014.

[6] D. Samanta, A. H. Alahmadi, M. P. Karthikeyan et al., "Cipher block chaining support vector machine for secured decentralized cloud enabled intelligent IoT architecture," *IEEE Access*, vol. 9, pp. 98013–98025, 2021.

[7] S. K. Singh, M. M. Salim, J. Cha, Y. Pan, and J. H. Park, "Machine learning-based network sub-slicing framework in a sustainable 5g environment," *Sustainability*, vol. 12, no. 15, pp. 6250–6272, 2020.

[8] W. Stallings, *Cryptography and Network Security, 4/E*, Pearson Education India, 2006.

[9] Y. Javed, A. S. Khan, A. Qahar, and J. Abdullah, "EEoP: a lightweight security scheme over PKI in D2D cellular networks," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 3-11, pp. 99–105, 2017.

[10] A. Abro, Z. Deng, and K. A. Memon, "A lightweight elliptic-Elgamal-based authentication scheme for secure device-to-device communication," *Future Internet*, vol. 11, no. 5, pp. 108–120, 2019.

[11] H. Tan, Y. Song, S. Xuan, S. Pan, and I. Chung, "Secure D2D group authentication employing smartphone sensor behavior analysis," *Symmetry*, vol. 11, no. 8, pp. 969–980, 2019.

[12] Y. Sun, J. Cao, M. Ma, H. Li, B. Niu, and F. Li, "Privacy-preserving device discovery and authentication scheme for D2D communication in 3GPP 5G Het net," in *In 2019 International Conference on Computing, Networking and Communications (ICNC), IEEE*, pp. 425–431, Honolulu, HI, USA, 2019, February.

[13] P. Das, A. Vashisth, D. Chadha, S. Ananda Kumar, A. Banerjee, and S. Shiaeles, "LIMAP: a lightweight multilayer authentication protocol for WBAN," *Wireless Personal Communications*, vol. 121, no. 4, pp. 2857–2884, 2021.

[14] S. Rani, D. Gupta, S. Garg, M. Jalilpiran, and M. S. Hossain, "Consumer electronic devices: evolution and edge security solutions," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 15–20, 2022.

[15] S. B. M. Baskaran and G. Raja, "A lightweight incognito key exchange mechanism for LTE-A assisted D2D communication," in *2017 ninth international conference on advanced computing (ICoAC)*, pp. 301–307, IEEE, 2017.

[16] S. K. Singh, Y. Pan, and J. H. Park, "OTS scheme based secure architecture for energy-efficient iot in edge infrastructure," *CMC-COMPUTERS MATERIALS CONTINUA*, vol. 66, no. 3, pp. 2905–2922, 2021.

[17] G. Zheng, B. Gong, and Y. Zhang, "Dynamic network security mechanism based on trust management in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2021, 10 pages, 2021.