Paper

LEES: a Hybrid Lightweight Elliptic ElGamal-Schnorr-Based Cryptography for Secure D2D Communications

Javeria Ambareen, M. Prabhakar, and Tabassum Ara

School of Computing and Information Technology, REVA University, Bengalore, India

https://doi.org/10.26636/jtit.2021.146020

Abstract—Device-to-device (D2D) communications in 5G networks will provide greater coverage, as devices will be acting as users or relays without any intermediate nodes. However, this arrangement poses specific security issues, such as rogue relays, and is susceptible to various types of attacks (impersonation, eavesdropping, denial-of-service), due to the fact that communication occurs directly. It is also recommended to send fewer control messages, due to authenticity- and secrecy-related prevailing requirements in such scenarios. Issues related to IoT applications need to be taken into consideration as well, as IoT networks are inherently resource-constrained and susceptible to various attacks. Therefore, novel signcryption algorithms which combine encryption with digital signatures are required to provide secure 5G IoT D2D communication scenarios in order to protect user information and their data against attacks, without simultaneously increasing communication costs. In this paper, we propose LEES, a secure authentication scheme using public key encryption for secure D2D communications in 5G IoT networks. This lightweight solution is a hybrid of elliptic curve ElGamal-Schnorr algorithms. The proposed scheme is characterized by low requirements concerning computation cost, storage and network bandwidth, and is immune to security threats, thus meeting confidentiality, authenticity, integrity and non-repudiation-related criteria that are so critical for digital signature schemes. It may be used in any 5G IoT architectures requiring enhanced D2D security and performance.

Keywords—5G networks, authentication, D2D communication, IoT, lightweight cryptography.

1. Introduction

Device-to-device (D2D) communication is a novel technology available in 5G networks, allowing two devices located nearby to communicate without approaching the base station. It is a boon for areas with low or no coverage. Smartphones and IoT devices may act as small base stations, providing all connectivity-related benefits of a 5G network to nearby devices, thus enhancing coverage. Two types of D2D communications are possible, as shown in Fig. 1, namely inband and outband. The inband scenario uses the licensed spectrum and may be divided into non-overlapping portions of D2D (overlay) or may not be divided at all (underlay). Outband communication uses the unlicensed spectrum and helps eliminate interference caused by such devices as Wi-Fi, Bluetooth, etc. It is further divided into controlled (where D2D communication is controlled by the network) or autonomous (where D2D control is left to users) varieties.

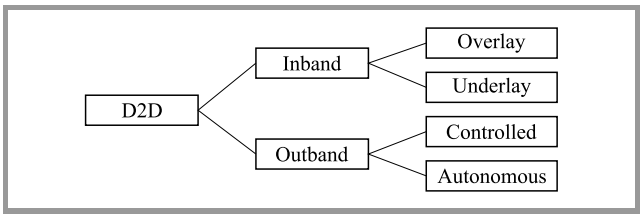

Fig. 1. Types of D2D communication.

In D2D communication, the devices act as relays. They may either be a transparent relay (TR), simply amplifying and forwarding the message, or a non-transparent relay (NTR), decoding and forwarding the message. Problems appear when these NTR-type relays become rouge and jeopardize the entire network, resulting in various security attacks. The situation gets aggravated since these devices are resource-constrained, with very limited computational and storage power. So, any new information security algorithms developed for the purpose of this scenario would need to be computationally lightweight. Authenticated encryption algorithms and digital signatures need to be used in any data transfers to secure these against common attacks and to maintain confidentiality, privacy and authenticity of the data involved.

Public key encryption and digital signatures are the key pillars of modern cryptography. In a real-world scenario, when two parties are communicating over a wireless communication channel which may be insecure, the encryption

algorithms data confidentiality of data and the digital signatures provide data authentication. Elliptic curve cryptography (ECC) was developed in 1985 and is one of the most widely used public key cryptography schemes. Finite keys are one of the main features in the algebraic structure of the solution. Its key sizes and the security level that it offers make it more popular compared to other algorithms. ElGamal is also a public key cryptographic technique but is based on the Diffie-Hellman key exchange. There are a few approaches to applying ECC combined with either ElGamal or Schnorr [1], both offering promising results, but no references are available in connection with combining elliptic curve-based ElGamal with Schnorr.

Taking this forward, in this paper we present LEES – a lightweight authentication scheme for secure D2D communications in 5G IoT networks. It is a hybrid implementation of ECC ElGamal encryption and the Schnorr digital signature scheme.

The remaining sections of the paper are organized as follows. Section 2 discusses the related work and is followed by a discussion on security considerations in D2D communication, presented in Section 3. Section 4 discusses the encryption and various digital signature scheme preliminaries along with the notations used in this paper. Section 5 presents the system model, while Section 6 presents the implementation schema. Section 7 discusses the results, while the overall conclusion is presented in Section 8.

2. Related Work

Verifying user identity as part of the authentication process, hiding sensitive information to ensure anonymity, preserving data confidentiality and integrity through the use of encryption, hash functions or message authentication, as well as optimized and cost-effective implementation methods are the topics outlined in the security-related considerations of the authors o of [2]. Paper [3] proposes a secure service-oriented authentication framework, where fog nodes that are responsible for forwarding data in a 5G network use a slice selection mechanism that ensures preservation of privacy. The Diffie-Hellman based [1] present a security analysis of two schemes: the Huang-Chang convertible signcryption scheme (which serves as a basis for the Schnorr signature) and the Kwak-Moon group signcryption scheme. The results show that both schemes are insecure. The Huang-Chang scheme fails to ensure confidentiality, while the Kwak-Moon scheme does not satisfy the properties of unforgeability, coalition-resistance, and traceability in its current form.

Paper [4] identifies the keyescrow problem of major cryptographic schemes and proposes a certificate-less signature scheme (CLS) for lightweight devices in Industrial Internet of Things (IIoT). In this procedure the keys are retained during the post-decryption phase and an authorized entity has access to these, but under a few predefined conditions. The scheme enables the selection of keys based on exponentials and ensures integrity through the use of hash functions. This pairing-based scheme is proven to be secure against type I and type II adversaries under the extended bilinear strong Diffie-Hellman (EBSDH) and bilinear strong Diffie-Hellman (BSDH) assumptions.

Article [5] proposes that validity of each participating user equipment (UE) be authenticated by 5G authentication and key agreement (AKA) only once during its life time, and that these checks be performed before generating a D2D token. The base stations communicate their public key through elliptic-curve digital signature algorithm (ECDSA) to generate the D2D token. The D2D communication process comprises three stages [6], the first one consists in discovering the device that identifies nodes in its proximity by sending out a request message in the broadcast mode. A nearby node responds with a D2D token and UE identity subscription concealed identifier (SUCI) in an encrypted form. The link setup phase comes next, where each node sends SUCI and the D2D token to the base station for verification. After verification, the secret keys are exchanged using the elliptic-curve Diffie-Hellman (ECDH) algorithm. The last step is the secure data transmission stage that relies on the authenticated encryption with associated data (AEAD) cipher to encrypt the data using the D2D token, before transmitting the data. However, 5G AKA has limitations and is susceptible to replay attacks. Hence, alternatives need to be looked at, and this is precisely the goal of this paper.

3. Security Considerations

Digital signature schemes are one of the most important cryptographic primitives enabled by public-key cryptography. These methods allow messages to be authenticated through the use of asymmetric encryption systems in which the sender and the receiver are not required to share a common but secret key. Digital signatures are cryptographic primitives which play a fundamental role in ensuring entity authentication, data origin authentication, data integrity and non-repudiation. Functionalities provided by a digital signature can be summarized as follows:

- **Authentication**. A private key of the sender is used to sign the message, thus authenticating the source of the message. The private key is not shared with anyone. It is known to the sender only. It can be verified by anyone by decrypting it with the use of the sender's public key.
- **Integrity**. Integrity is the most important property of the message, as it ensures that the data has not been compromised. Integrity may be ensured by digitally signing the message. The signature is generated with respect to the data contained in the message. If the message is altered, the receiver may easily determine that at the time of verification. It is extremely challenging to alter the message or its signature without the knowledge of the private key. Hence, the data is unaltered during the transmission.

- **Non-repudiation**. This characteristic ensures the integrity of data and guarantees that a third party will be able to verify the source of data and its integrity. It ensures that the sender cannot deny sending of the message/data. And this is basically supported by digitally signing the message with the help of a private key of the sender itself. When the receiver performs verification using the public key of the sender, a proof is obtained that the message/data has been sent by the same sender. Hence, denying the message becomes impractical.

In general, each algorithm used for signing a message will comprise two different key processes: one for signing and the other for verifying the message at the other end. Below, various security threats that loom large over D2D communications are enumerated.

3.1. Attacks in D2D Communications

Security threats in D2D communications are primarily related to the fact that the process is based on radio transmissions [5]. The most common types of attacks include the following:

- **Eavesdropping** – in this attack the intruder is able to listen-in without the actual participating devices (PDs) being aware of that fact. If confidentiality of cryptographic data is maintained, this attack may be thwarted.
- **Impersonation** – the intruder comes across as a valid participating device – or worse the base station (BS) – and steals data. If cryptographic authentication is enforced, this attack may be thwarted.
- **Forgery** – the intruder may send forged or malicious content to all participating devices, thereby confusing the entire system. If cryptographic data integrity via digital signature is enforced, this attack may be thwarted.
- **Control data** – the attacker may change the control data itself. Cryptographic techniques, such as authentication, confidentiality and integrity, are required to thwart this attack.
- **Denial of service** (DoS) – this kind of attack may render a service unavailable. Cryptographic actions, such as authentication, confidentiality and integrity are needed to thwart this attack.

3.2. Attack Resiliency

To cope with the attacks listed above and to secure D2D communications, it is worth looking at some attack resiliency requirements suggested in [4], [7], [8]:

- **Authentication** – identity check of participating devices performed on a frequent basis.
- **Data confidentiality** – data sent between participating devices should be encrypted.
- **Data integrity** – data sent with the use of authenticated devices should be verified to ensure it has not been tampered with.
- **Privacy** – all confidential information of participating devices must be kept secret, e.g. number, location, etc.
- **Traceability** – the source of malicious messages should be traceable.
- **Anonymity** – identity of participating devices should not be disclosed to neighboring devices or to intruders.
- **Non-repudiation** – a digital signature is an effective solution for both transmission and reception non-repudiation, wherein one can stop the participating devices from saying no to transmitting or receiving a message.
- **Revocability** – revoking privileges of participating devices in the event of a malicious D2D service.

4. Preliminaries and Notations

4.1. Encryption and Digital Signature Schemes

There are many digital signature schemes, with ElGamal, elliptic curve and Schnorr algorithms being the most popular of them. The elliptic curve digital signature algorithm (ECDSA) is based on the modified digital signature algorithm (DSA). It works on elliptic curves that are defined over a mathematical group and discrete logarithmic problems for its key formats. The smaller footprints and efficiency of elliptic curve cryptography have led to its widespread adoption.

ElGamal combines the discreet logarithmic problem and the algebraic properties of modular exponentiation. At the core of the algorithm is a key pair which includes a private and a public key. When the sender sends a message, a digital signature is generated for it by the private key. Verification of the signature is carried out using the public key of the signer. The three key properties that a digital signature is supposed to offer, i.e. authentication, integrity, and nonrepudiation, are ensured by the digital signature in this case. The ElGamal signature algorithm is rarely used in practice. The ECDSA and other variants are used on a much wider scale. However, it is worth mentioning that ElGamal encryption, i.e. an asymmetric key encryption algorithm, is widely used in public key cryptography. The Diffie-Hellman key exchange forms the basis of this scheme.

The Schnorr signature offers numerous advantages over ECDSA and ElGamal signatures. It is an amalgamation of these schemes that is much simpler and faster. Its proven

security record is another of its advantages, provided that a random hash function with sufficient entropy is used with a sufficiently hard elliptic curve discrete logarithm problem (ECDLP). There is no security proof for ECDSA, however there is a definitive proof for Schnorr, according to which breaking the Schnorr algorithm implies breaking the discrete logarithmic problem. The linearity property is another key advantage of the Schnorr signature.
The parameters and notations used in the paper are described in Table 1.

Table 1
Notations and descriptions used

Parameters	Description
K	Private key
R	Random nonce
G	Generator point on elliptic curve
msg	Message
H'	Hash(msg)
P	Public key ($P = K \times G$)
S	Signature
CA	Certifying authority
PD	Participating device
BS	Base station

In ElGamal and ECDSA, the need to find the signature requires a division of the random nonce. Since it is a modulo operation, performance suffers, as an extended Euclidean algorithm or Fermat's little theorem may be required, calling for plenty of multiplication operations to be performed. The Schnorr signature is linear with no modulo division, thus making the process simpler and faster. ECDSA relies on a modulo division over different random nonces, making it difficult to add up ECDSA signatures. Schnorr's linear property makes it feasible to add up Schnorr signatures. This linearity makes it possible for multiple participating entities to collaboratively produce a signature for the sum of their public keys.
Considering the above as a motivation, lightweight elliptic ElGamal Schnorr-based authentication scheme is proposed (LEES).

5. System Model

The proposed model comprises the participating devices (PD) or a relay which provides coverage and connectivity to nearby devices (Fig. 2). A base station (BS) is a high computation node deployed by the mobile network service provider. There is a certification authority (CA) which is responsible for issuing certificates to all communicating nodes. As a pre-requisite for communication, the nodes (including PD and BS) have to register with the CA being responsible for whitelisting the public keys of all the nodes in the network. Thus, to avoid the key escrow problem, PD and BS generate their private and public keys. This generation of keys is not shouldered by CA.

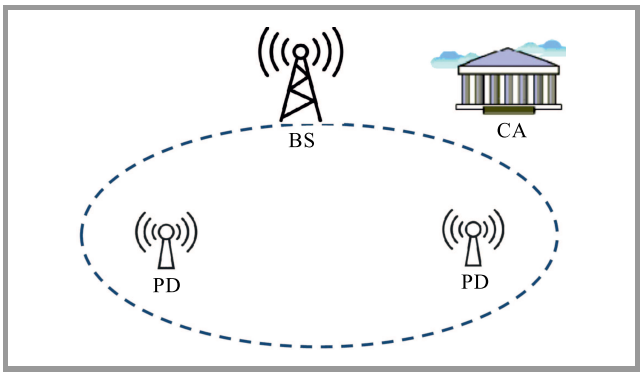

Fig. 2. System model diagram of the proposed solution.

6. Implementation

The proposed signcryption scheme is a hybrid implementation of the elliptic curve-based ElGamal encryption algorithm fused with the Schnorr digital signature scheme for enhanced security. The choice is based on the proven secure nature of the ElGamal cryptosystem and on the security of the Schnorr signature scheme. However, user identity is sent in plain text in this technique. Later it was refined with encrypted ID, but it still remains susceptible to replay attacks.
The proposed system may be split into four stages:

Stage 1 – yoke stage,

Stage 2 – entity detection stage,

Stage 3 – corroboration stage/trust establishment stage,

Stage 4 – secure data communication stage.

We assume that the 5G-AKA+ authentication and privacy preserving protocol is used prior to this stage or in accordance with this stage, so as to establish a foundation for secure communications ahead. We use the ElGamal public key as the encryption and decryption algorithm. The parameters generated at this stage are listed in Table 2.

Table 2
Parameters generated at the setup stage

Parameter	Description
a	A huge prime number
b	A huge prime factor of $(a-1)$
c	An integer which is of the order b mod a
$h()$	A secure one-way hash function
KH	One-way hash function with a key K
(E,D)	E encipher and D decipher

Here, two keys using public key infrastructure (PKI) are generated initially by the base station and participating devices and certified by the certifying authority. This stage can then be split as shown below:

KeyGen PD. Let K_{PD} and P_{PD} be the private and public key of the PD (sender) certified by CA:

$$PD = (K_{PD}, P_{PD}) , \tag{1}$$

where P_{PD}= C^{-K_PD} mod a.

Initially, when PD wants to communicate with BS, PD computes points on the elliptic curve (EC) which are then broadcast with base point F after periodic intervals. To compute K_{PD} from a field J_N $(1 < K_{PD} < N) J_N$, the public K_{PD} is computed as:

$$P_{PD} = K_{PD} \cdot G . \tag{2}$$

KeyGen BS. Let K_{BS} and P_{BS} be the private and public key of the BS (receiver) certified by CA:

$$BS = (K_{BS}, P_{BS}) , \tag{3}$$

where P_{BS}= $C^{-K_{BS}}$ mod a.

The signcryption stage. Calculate:

$$K = h\left(P_{BS}^{K_{BS}}\right) \bmod a . \tag{4}$$

Divide K into K_1 and K_2 of suitable length and:

$$x = KH_{K1}(msg) , \tag{5}$$

$$y = r + (d \cdot K_{PD}) \bmod b , \tag{6}$$

$$z = E_{K1}(msg) , \tag{7}$$

which is the ElGamal encryption of the plaintext with K_1 key.

A time stamp (TS) is added and the PD sends (x, y, z, TS) to the BS.

The unsigncryption stage. To recover the plaintext *msg* from (x, y, z, TS), the base station calculates the hash function:

$$K = \mathrm{hash}\left(C^s \cdot P_{PD}^d\right)^{K_{BS}} \bmod a . \tag{8}$$

Split K in K_1 and K_2, compute:

$$msg = DK_1(z) \tag{9}$$

where *msg* is assumed to be a valid message if $KH_{K2}(msg) = x$.

As mentioned above, for encryption and decryption algorithms, we use the ElGamal public key. For public key cryptography needs, this is an asymmetric key encryption algorithm. It has two other advantages. Firstly, since it is based on solving the difficult discrete logs in a large prime modulus, its security is tight. Secondly, its encryption is probabilistic, which ensures that the same plaintext produces a new cipher text every time encryption occurs. The algorithm may be divided into three key elements: key generator, encipher, and decipher.

- Key generation. Select a random x from $1, \ldots, b$ and determine $h = c^x$.
- Encipher. Select y from $1, \ldots, b-1$, determine $C_1 = C^x \bmod a$ nd $A = P_{PD}^x \bmod b$. Change the secret message *msg* into a factor msg' of B. Determine $C_2 = (A.msg) \bmod b$. The cipher text is (C_1, C_2).
- Decipher. Calculate the shared secret $S = C_1^x$ and compute $msg' = C_2 S^{-1}$, where S^{-1} is the inverse of S in group B.

The message is then converted back into plaintext message *msg* by the BS.

In the event of any dispute, the BS just needs to change a valid cipher text into a signature which can be verified publicly to satisfy a third-party certifying authority that the cipher text is, as a matter of fact, generated by the participating device only.

7. Result and Analysis

The proposed scheme scores well on both computation cost and memory consumption. This is due to the fact that LEES uses ECC, as this operation forms an Abelian group due to it being performed in a finite field. Hence, both addition and multiplication of points are different and faster from normal multiplication. It is lightweight and does not suffer from a lower security level in spite of ECC keys being shorter compared to RSA/DH, as shown in Fig. 3. Therefore, LEES usage leads to lower computational overheads and eases the handling of keys, since the number of bits required is lower compared to RSA/DH. This leads us to conclude that even memory consumption and network traffic will be reduced significantly as a lower number of bits is sent.

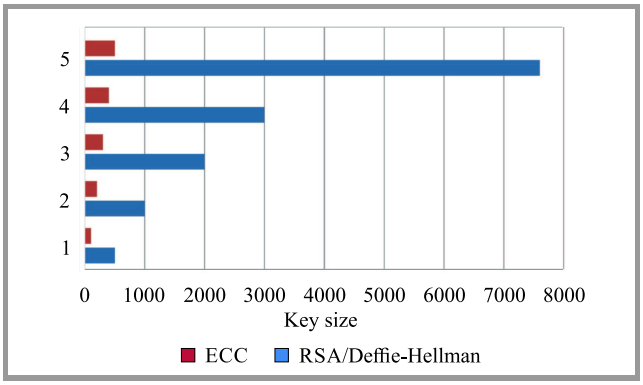

Fig. 3. Comparison of key size of ECC and RSA/DH.

In the proposed scheme, we used 5G-AKA+ for primary authentication of a PD before initiating the D2D setup stage. This framework, available in 5G networks, offers unlinkability and also satisfies both efficiency and design drawbacks in 5G-AKA. Moving forward, secondary authentication is performed by the CA based on the private and public keys generated by the PD and BS. This is followed by signcryption and unsigncryption stages which encrypt/decrypt messages using the ElGamal algorithm and verify

the Schnorr digital signature before the receiver receives any data. Thus, authentication takes place at each stage, thereby ensuring secure D2D communications.

Except for PD, any attacker (including BS) cannot forge a valid cipher text (x, y, z) for any message *msg*, such that the verification equations mentioned above are all satisfied. Also, except for the designated receiver, i.e. the BS, no third-party can derive the message *msg* from the cipher text (x, y, z).

5G networks inherently provide encrypted identity and thus anonymity to PD. In addition, the private and public key of PD and BS is unique and certified by CA. Further data sent by PD is encrypted with private key of BS, which offers further anonymity to PD.

Once BS reveals a triple (msg, y, z), anyone can verify that (y, z) is PD's signature. Hence, an authority may settle any potential disputes between PD and BS.

LEES authentication and data encryption processes are designed using a lightweight cryptographic protocol. It is lightweight, since it uses a ECC-based public key cryptosystem which utilizes only a 256 bit key compared to a 1024 bit RSA key offering the same level of security.

Since all 5G IoT devices will be resource-constrained, the lightweight cipher used in LEES works efficiently by ensuring data confidentiality, integrity and authentication.

7.1. Analysis Based on Security Against Key Attacks

Impersonation attack. LEES is robust against impersonation attacks. This is a common problem in D2D communications with devices acting as relays. As per the proposed scheme, this is avoided in a two-step approach. Firstly, the PD will encrypt the message by its private key. The receiving BS fetches the public key P_{PD} from the whitelist maintained by the CA. This does not allow it to open the message and decryption fails. Thus, LEES is secure against impersonation attacks.

Baby step and giant step (BSGS) method. The solution proposed by Shank helps solve the DLP problem by focusing on collisions and by minimizing complexity at approx. by $\sqrt{N}$ times, which is almost 50% of the original size. If a 192-bit curve is used, considering $\sqrt{N}$, we get 10^{16} points, which will require 10^{21} bytes for storing the hash – a result that is much lower compared to the proposed scheme which works out to the order of 10^{156} attempts, thus making it impossible to guess the key.

Brute force attack. An intruder may lay its hands on the public key of PD and BS and, say, also the base point F on the elliptic curve EC. If it obtains access to the private key of BS (P_{BS}), then the entire network is compromised. If P_{PD} is accessed, the small network that PD is serving gets compromised. However, since LEES uses ECC for key selection, is based on DLP and the key size is over 384 bits, the network is secured against such attacks.

Pollard's Rho method. It is a lightweight attack. It performs two operations called parallelization and random walk. It attempts to reduce to the square root of the attack to find the secret key. Since LEES uses ECC, it needs to be mentioned that the key size of ECC is ~ 571 bits, which is equal to around 15360 bits of RSA as shown in Table 3. Therefore, considering the first key and taking its square root, the problem becomes unfeasible to solve. As seen in Fig. 3, the size of RSA increases significantly compared to ECC, which increases moderately.

Table 3
LEES vs. RSA/DH key comparison

LEES [bits]	RSA/DH [bits]
112	512
224	2048
571	15360

Relay attack. Here, the intruder saves the accessed message and sends it at some other time intervals, leading to great losses. To avoid such attacks, a time stamp is introduced in (x, y, z, TS) during the signcryption stage. Based on the session, the time to live (TTL) is calculated and, if the difference between the current time and the message time is greater than TTL, the message is considered to be a fresh message. Otherwise, it is a stale message.

7.2. Analysis of Authentication Overhead

Generally, four steps are involved in a normal authentication process to ensure a secure transmission. However, in the proposed scheme, communication may be of the occur in one-step only, or in two-steps maximum, to deliver the cipher text and to perform authentication. Therefore, a comparison between LEES and other contemporary schemes shows that the communication overhead and, thereby, network bandwidth are highly reduced, by up to four times, without compromising security. Hence, the solution is lightweight. Also, a comparison between LEES and other contemporary designs, such as the ultra-lightweight mutual authentication protocol (ULMAP) and the session initiation protocol (SIP), shows that the proposed scheme outperforms the above solutions in term of the number of messages exchanged with almost the same level of trust and security, as shown in Fig. 4.

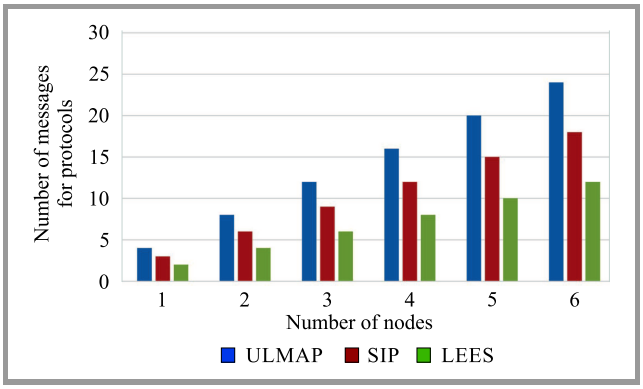

Fig. 4. Comparison of authentication message overhead.

8. Conclusion

The scheme developed has been analyzed in terms of its key parameters: computational overhead, security, key attacks and authentication overhead. It is observed that LEES requires less computational resources and eases the handling of keys, since the number of bits required is lower by a factor compared to RSA/DH. This leads us to conclude that even memory consumption and network traffic will be significantly reduced, as lower number of bits are sent. The analysis of the proposed scheme focusing on attack resiliency shows that it offers, when implemented, good levels of authentication, data confidentiality, anonymity and efficiency. In terms of protection against attacks, it has been determined as being secure against most attacks. Finally, a comparison between LEES and other algorithms showed that the communication overhead and, thereby, network bandwidth are highly reduced (by as much as four times) with LEES, without compromising security.

References

[1] G. Wang, R. H. Deng, D. Kwak, and SangJae Moon, "Security analysis of two signcryption schemes", in *Information Security 7th International Conference, ISC 2004, Palo Alto, CA, USA, September 27-29, 2004, Proceedings*, K. Zhang and Y. Zheng, Eds. *LNCS*, vol. 3225, pp. 123–133. Berlin: Springer, 2004 (DOI: 10.1007/978-3-540-30144-8_11).

[2] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in LTE-advanced networks: A survey", *IEEE Commun. Surv. and Tutor.*, vol. 17, no. 4, pp. 1923–1940 2015 (DOI: 10.1109/COMST.2014.2375934).

[3] L. M. Theobald *et al.*, "Device-to-device discovery for proximity-based service in LTE-advanced system", *IEEE J. on Selected Areas in Communication*, vol. 33, no. 1, pp. 55–66, 2015 (DOI: 10.1109/JSAC.2014.2369591).

[4] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S. C.-H. Huang, H.-H. Chen, "Physical layer security in wireless networks; A tutorial", *IEEE Wireless Communication*, vol. 18, no. 2, pp. 66–74, 2011 (DOI: 10.1109/MWC.2011.5751298).

[5] A. S. Khan, Y. Javed, J. Abdullah, J. M. Nazim, and N. Khan, "Security issues in 5G device to device communication", *Int. J. of Comp. Sci. and Netw. Secur.* (*IJCSNS*), vol. 17 no. 5, pp. 366–375 [Online]. Available: http://paper.ijcsns.org/07_book/201705/20170550.pdf

[6] W. Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Boston: Addison-Wesley Professional, 2015 (ISBN: 9780367378158).

[7] H. Lazrag, H. Chaibi, S. Rachid, and M. D. Rahmani, "An optimal and secure routing protocol for wireless sensor networks", in *Proc. of 6th Int. Conf. on Multime. Comput. and Systems ICMCS 2018*, Rabat, Morocco, 2018 (DOI: 10.1109/ICMCS.2018.8525911).

[8] M. Alenezi, K. Almustafa, and M. Hussein, "On virtualization and security-awareness performance analysis in 5G cellular networks", *J. of Engin. Sci. and Technol. Rev.*, vol. 11, no. 1, pp. 199–207, 2018 (DOI: 10.25103/jestr.111.24).

Javeria Ambareen, a passionate security techie, has over a decade of academic and industry experience. Having an M.Tech. degree, her key areas of interest include IoT security, application security, automation and machine learning.

E-mail: javeriaster@gmail.com
School of Computing and Information Technology
REVA University
Bangalore, India

M. Prabhakar received his M.Sc. and Ph.D. degrees in Computer Engineering from Anna University, Chennai. He has 21 years of teaching experience and is currently working as an Associate Professor at the School of Computing & Information Technology, REVA University, Bangalore, India. His areas of research interest include adhoc networks and cybersecurity.
E-mail: prabhakar.m@reva.edu.in
School of Computing and Information Technology
REVA University
Bangalore, India

Tabassum Ara is a Research Scholar in Computer Science at Reva University, Bangalore, Karnataka, India. With 20 years of academic experience, she holds B.Eng., M.Sc. and M.Tech. degrees and is an Assistant Professor at the Department of Computer Science at HKBK College of Engineering in Bangalore, India. Her research interests focusing on IoT, security and WSN.
E-mail: tabuara@gmail.com
School of Computing and Information Technology
REVA University
Bangalore, India