IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 10, 2022, accepted March 3, 2022, date of publication March 14, 2022, date of current version March 24, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3159686

Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks

ADNAN SHAHID KHAN[1], (Senior Member, IEEE), YASIR JAVED[2], (Member, IEEE), RASHAD MAHMOOD SAQIB[1,3], ZEESHAN AHMAD[1,4], (Member, IEEE), JOHARI ABDULLAH[1], KARTINAH ZEN[1], IRSHAD AHMED ABBASI[1,5], (Member, IEEE), AND NAYEEM AHMAD KHAN[6]

[1]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia
[2]Department of Computer Science, Prince Sultan University, Riyadh 11586, Saudi Arabia
[3]Faculty of Applied Studies, King Abdul Aziz University, Jeddah 21589, Saudi Arabia
[4]Department of Electrical Engineering, King Khalid University, Abha 62529, Saudi Arabia
[5]Department of Computer Science, Faculty of Science and Arts Belqarn, University of Bisha, Sabt Al-Alaya 61985, Saudi Arabia
[6]Faculty of Computer Science and Information Technology, Al Baha University, Al Baha 65731, Saudi Arabia

Corresponding author: Adnan Shahid Khan (skadnan@unimas.my)

This work was supported in part by the Prince Sultan University; and in part by the Research, Innovation and Enterprise Centre (RIEC), Universiti Malaysia Sarawak, under Grant F08/PGRG/2058/2021.

ABSTRACT With increased interest in 6G (6th Generation) cellular networks that can support intelligently small-cell communication will result in effective device-to-device (D2D) communication. High throughput requirement in 5G/6G cellular technology requires each device to act as intelligent transmission relays. Inclusion of such intelligence relays and support of quantum computing at D2D may compromise existing security mechanisms and may lead towards primitive attacks such as impersonation attack, rouge device attack, replay attack, MITM attack, and DoS attack. Thus, an effective yet lightweight security scheme is required that can support existing low computation devices and can address the challenges that 5G/6G poses. This paper proposes a Lightweight ECC (elliptic curve cryptography)-based Multifactor Authentication Protocol (LEMAP) for miniaturized mobile devices. LEMAP is the extension of our previous published work TLwS (trust-based lightweight security scheme) which utilizes ECC with Elgamal for achieving lightweight security protocol, confidentiality, integrity, and non-repudiation. Multi-factor Authentication is based on OTP (Biometrics, random number), timestamp, challenge, and password. This scheme has mitigated the above-mentioned attacks with significantly lower computation cost, communication cost, and authentication overhead. We have proven the correctness of the scheme using widely accepted Burrows-Abadi-Needham (BAN) logic and analyzed the performance of the scheme by using a simulator. The security analysis of the scheme has been conducted using the Discrete Logarithm Problem to verify any quantum attack possibility. The proposed scheme works well for 5G/6G cellular networks for single and multihop scenarios.

INDEX TERMS Multifactor authentication, LEMAP, D2D communication, 6G, BAN (BAN Logic), Elgamal.

I. INTRODUCTION

Demand for speed and increased connectivity has resulted in the evolution of 5G/6G cellular network standards. The mandatory requirements for 5G/6G are high speed, ubiquitous connectivity, intelligence, and quantum computing support. The newly developing 6G cellular network is considered innovative as it can support intelligently high-speed data, broadband, and multimedia services with lower latency. Device to Device (D2D) is an integral part of the 5G/6G cellular network to achieve higher data rates in ultra-dense small cells. It facilitates the discovery of geographically close devices to enable direct communication between neighboring devices thus improving communication capabilities, reducing power consumption and latency [1].

D2D was introduced initially in LTE-A to enhance network performance in ultra-dense environments and can work with or without the supervision of network infrastructure, thus making it more prevalent for deployment in disastrous areas or low coverage services areas [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Petros Nicopolitidis.

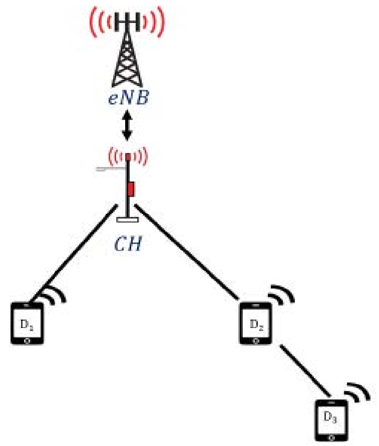

FIGURE 1. Basic multi-hop D2D cellular network communication.

Figure 1. illustrates the multi-hop communication architecture of D2D that shows devices are controlled by evolved node base station (eNB). These devices can connect with each other after establishing the authentication and authorization with eNB. Cluster Head (CH) acts as a relaying agent between eNB and devices for the establishment of a secure communication channel. In recent trends, it is observed that D2D communication has achieved additional features where multi-hop D2D communication is also possible. Multi-hop D2D communication allows local area communication between multiple devices where one or more devices can act as intelligent relays or CH. It also allows extended coverage so that devices outside the coverage area can be accommodated.

However, typical D2D communication in LTE-A/5G, when allowed to work as intelligent forwarding agent relays, consequently, exposed the communication to several security vulnerabilities and breaches, for instance, quantum attacks, 51% attacks [3], man in the middle (MITM) attack, masquerading attack, denial of service (DoS) attack, rouge relay attack and privacy issues in current 5G/6G cellular networks. Several security schemes have been proposed for D2D communication security which includes River Shamir Adleman (RSA) [4], Diffie Hellman (DH) [5], Elliptic Curve Cryptography (ECC) [6]–[8], Elliptic Curve Cryptography with Diffie Hellman (ECDH) [9], [10] are few combinations that have been used. These security challenges are more crucial and harder to mitigate because of the resource-constrained nature of cellular devices. Therefore, there is an acute need to consider security design requirements for ensuring a secure and trustworthy environment for D2D cellular communication. To solve these security challenges in D2D communication, a lightweight and secure D2D communication system is required that can provide secure mutual authentication, data confidentiality/integrity, and anonymity.

This paper is the extension of our previously published work where a trust-based lightweight security scheme (TLWS) for D2D multihop communication is proposed. This proposed scheme utilized an elliptic curve and Elgamal cryptosystem assisted with a secure hashing algorithm, timestamps, and blindfold challenge for secure communication and key agreements [6]. However, in this paper, we propose a lightweight multifactor authentication security scheme for a multihop scenario that can mitigate the above-mentioned attacks with reduced authentication overhead, computation cost, and lower communication cost. The proposed scheme is based on Elliptic Curve Cryptography (ECC) which is one of the lightweight asymmetric-key techniques compared to currently adapted public-key encryption algorithms such as RSA. ECC provides 3072-bit RSA cryptographic security using a 256-bit key [11].

A. MOTIVATION

Most of the authors tried to mitigate well-known and common MAC (medium access control) layer attacks, for instance, Replay attack, MITM, DoS attack, and impersonation attack. By taking few assumptions like identity can be shared publicly, communication channels are always secure, and some of the credentials can be sent without encryption, the timestamp cannot be modified, single hashing can resolve the integrity problem and cryptosystem is free of quantum brute force and password guessing attacks [12]–[15]. However, several researchers believed that if the above-mentioned assumptions are not carefully addressed, they can lead towards common MAC layer attacks [6], [16]–[18] For instance, an identity reveals attack can lead to theft of identity, which leads towards impersonation attack or man in the middle attack.

Most of the authors achieved a secure end-to-end communication at the expense of high computation cost and message authentication overhead in multihop [19]–[22] However, it is well agreed that using a lightweight security mechanism and transmitting a small number of messages over the communication link is always advisable to reduce the challenges of security threats, authentication overhead, and well suits to miniaturized devices [15], [23], [24].

Although current security schemes have addressed some of the challenges, several challenges require further attention. One of the challenges is that key size must be small as larger key size results in higher operational costs. Normally, a larger key size is required to make the security scheme safe against quantum attacks but this results in higher operational costs [25]. Previous research has shown that a very large key size cannot be used in the D2D security scheme due to memory, storage, and computation requirements [26].

B. CONTRIBUTIONS

The first contribution is a lightweight cryptographic multifactor authentication scheme that helps secure D2D communication in an open insecure environment. This is a novel cryptosystem that utilizes ECC with Elgamal for achieving confidentiality, integrity, and non-repudiation. Elgamal has a smaller key size which helps not only in the reduction of operational and communication costs but also makes it usable on miniature devices. This also applies a digital signature to achieve authentication while double hashing using SHAv3 combined with a timestamp and blindfold challenge scheme providing three-dimensional security that is integrity, freshness, and mutual authentication. Three-dimensional security using Double Hashing based on SHAv3 combined with multi-factor authentication provides integrity, confusion, diffusion, freshness, and mutual authentication. Multi-factors used for authentication include one-time password OTP (Biometrics, random number), timestamp, challenge, and password which provide mitigation of all major security attacks for complete secure communication. This scheme also offers reduced authentication overhead, communication, and computation cost due to the merged challenge-response scheme. The proposed scheme enhances the security performance by addressing all security requirements. It reduces the authentication overhead for single-hop and multi-hop communication. It has a lower computation overhead that helps devices to consume less computational power and has also lower communication overhead resulting in the reduction of network traffic significantly.

C. PAPER ORGANIZATION

The remainder of this paper is organized as follows. In Section II Related works are given. A proposed system model is presented in Section III. Formal security analysis is given in section IV, followed by the results and discussion in section V. Finally, conclusions are drawn in section VI.

II. RELATED WORKS

This section briefly reviews several mutual authentication schemes proposed in the literature. The design of authentication protocols has not been a smooth journey. Reference [27] proposed an efficient and secure two-factor password authentication scheme with a card reader (terminal) verification algorithm. Multifactor parameters which include (biometrics, password, and smart card) are used for authentication which ensures much better security. This scheme mitigates man-in-the-middle attack and provides multi-level hashing for rigorous authentication and integrity. The proposed scheme also provides Quantum attack safety. Despite the above strengths of the scheme, the proposed scheme is still vulnerable to some threats and drawbacks. For example, ID is sent as plain text without encryption on the open channel; this can result in location-identity reveals attack as explained in [28] and [29]. When data is sent from the user to cluster head, an unencrypted message is sent on an open channel which can cause modification of the message, and hence it can result in MITM [23], [30], [31]. Hash of data is sent without timestamp; this can cause replay attack. A smart card is used as multi-factor authentication which is vulnerable to identity theft and the duplication of card threats [32].

Park *et al.* [16] proposed another protocol 2PAKEP: provably secure and efficient two-party authenticated key exchange protocol for mobile environment uses multifactor authentication (biometrics, nonce, timestamp, OTP) and it is safe against replay attack. Although the scheme mitigates replay attacks, it is still vulnerable to some threats such as ID being sent as plain text which can result in a location-identity reveal attack. Data is shared unencrypted and modification of timestamp can cause a replay attack, so MITM is possible. Unencrypted data is received at the cluster head which will result in a rouge relay attack [15], [33]. The single hash function can result in a weak-collision attack [34]. This scheme offers high authentication overhead, higher computational cost, and high communication cost.

Owing to the growing number of attacks on D2D communication, researchers in academia and industry have invested many efforts in designing secure communication algorithms. Research about D2D security is still in the initial stages. Some researchers used the most common security algorithms for normal communication over the network. A few researchers have used MANETS algorithms for proposing security solutions [35], [36]. Most of the security algorithms only focus on one or two security requirements that must be met for designing a secure technique for D2D. Another issue is that D2D designing is still under development and creates an emerging security requirements issue. Some algorithms are proposed based on old requirements while some new requirements have emerged. Another issue is that devices involved in D2D have variable computation power and due to application probability across different devices; any device can act as communicating device. Hence, the developed solution must consider a low computation device. Owing to this issue, many of the proposed solutions may be vulnerable to new era attacks [6]. Numerous techniques and approaches focused on secure data transfer, some others focused on authentication and key agreements. These proposed techniques for D2D security usually focused on the security of data, sharing of data securely, authentication, and agreement of keys. Table 1. shows the comparison of attacks between our proposed scheme and two selected benchmark schemes that are TwoFactor and 2PAKEP. Most of the security techniques focus on single operators and security issues are considered individually without combining the security techniques with key management. D2D inherently poses several challenges and threats that can be categorized into single-hop and multi-hop challenges. D2D is more open to any kind of attacks that were even non-existent in the traditional 5G/6G network. But allowing the devices to act as relaying with intelligence devices opens a whole bunch of attacks that should be handled differently; as the devices have low computing power and are required to do many new tasks which were not their actual part before algorithms.

In this paper, we aim to design a Lightweight ECC-based Multifactor Authentication Protocol for D2D communication which mitigates all major security attacks to provide secure end-to-end communication with lower computational cost, communication cost, and authentication overhead.

TABLE 1. Device/relaying node computational parameters.

Attack Type	LEMAP	2PAKEP	TwoFactor
A Preimage attack	Yes	No	No
(MITM)	Yes	Yes	Yes
Impersonation Attacks	Yes	Yes	Yes
Privileged-Insider Attack	Yes	Yes	Yes
Mutual Authentication	Yes	Yes	Yes
Replay Attack	Yes	Yes	Yes
Password Change attack	No	Yes	Yes
Pass-the-Hash (PtH) attack	Yes	No	No
Masquerading Attack	Yes	No	No
Repudiation Attack	Yes	No	No
DoS	Yes	No	No
Eavesdropping attack	Yes	No	No
Rogue Relay Attack	Yes	No	No
Malicious Card Reader Attack	No	No	Yes

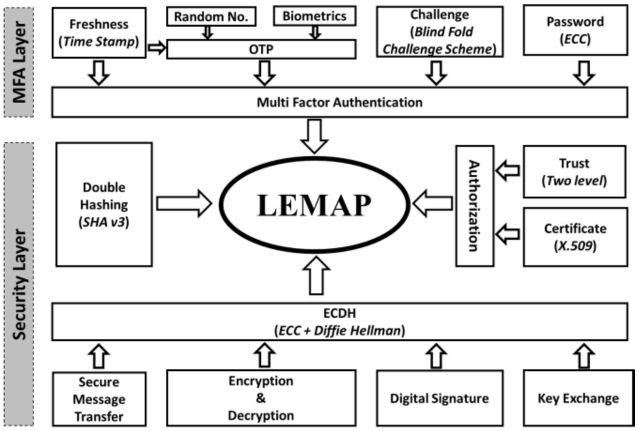

FIGURE 2. System model for proposed scheme.

III. SYSTEM MODEL

A. PROPOSED SOLUTION

To secure multi-hop D2D communication, a lightweight ECC-based multi-factor authentication protocol (LEMAP) has been proposed that ensures secure end-to-end communication along with lower authentication and communication overhead. The proposed scheme is secure against impersonation attacks, replay attacks, man in the middle (MITM) attacks, masquerading attacks, DoS attacks, rouge relay attacks, and privacy issues. To secure multi-hop D2D communication, the multi-factor authentication (MFA) layer and security layer are introduced as sublayers to the main security layer. The Block diagram of both layers is shown in Figure 2.

1) MULTI-FACTOR AUTHENTICATION LAYER

The multi-factor authentication layer consists of four components pseudo-IDs, random number, challenge, and timestamp. Pseudo IDs are assigned to devices to hide real identity during communication so that adversary should not be able to know the actual identity and location of the participating device. This helps to secure communication from identity reveal attacks. One-time password OTP is generated using a random number with specific time validity. Each device must respond and solve OTP to get validity trust from eNB to communicate with other devices. If a device is unable to respond to OTP within a specific time period, its validity expires which secures communication from malicious attackers who may try to use OTP after some time. Each request message is sent along with a challenge and every response is required to solve this challenge. When a message is sent, its hashed challenge solution is also sent with the actual message. When a receiver receives the message and solves the challenge, it decrypts the 'already sent solved challenge' and compares it with the solution. If 'solved challenge' and 'sent challenge solution' are the same, the message is considered valid and trusted. A blindfold challenge scheme is used in this algorithm to create challenge and challenge solutions.

The timestamp is another factor used to check the message's freshness and verify it for a replay attack. If the message responds within the timestamp, the message is considered fresh and free of any replay attack. All these above-mentioned factors combine to develop LEMAP a multi-factor authentication protocol to secure D2D communication with less authentication overhead and lightweight in communication and computation cost.

2) SECURITY LAYER

The security layer comprises five major components which include: key creation, secure key transmission, freshness, hashing, and cryptographic module. The key creation module is responsible for the creation of a secret point for communication. For this purpose, Elliptic curve cryptography (ECC) based algorithm is used. Secure key transmission is a very important part of secure D2D communication where secret keys generated using ECC are securely transmitted. Elgamal algorithm is used for sharing keys and sending encrypted messages. For message freshness, the timestamp is used, and this will secure the message from replay attack. To secure messages from the MITM attack, a simple challenge-response authentication scheme is used. This scheme will also ensure the delivery of the message. To ensure the integrity of the message, a double hashing technique is used which helps to avoid collisions in hash tables. The double hashing is done using the SHA v3 algorithm. In the cryptographic module, encryption and decryption of data are done at any device or eNB. ECC is used for both encryption and decryption, which is lightweight and has a small key size.

B. METHODOLOGY

To resolve mentioned challenges, in this paper we propose an ECC-based multifactor authentication that comprises

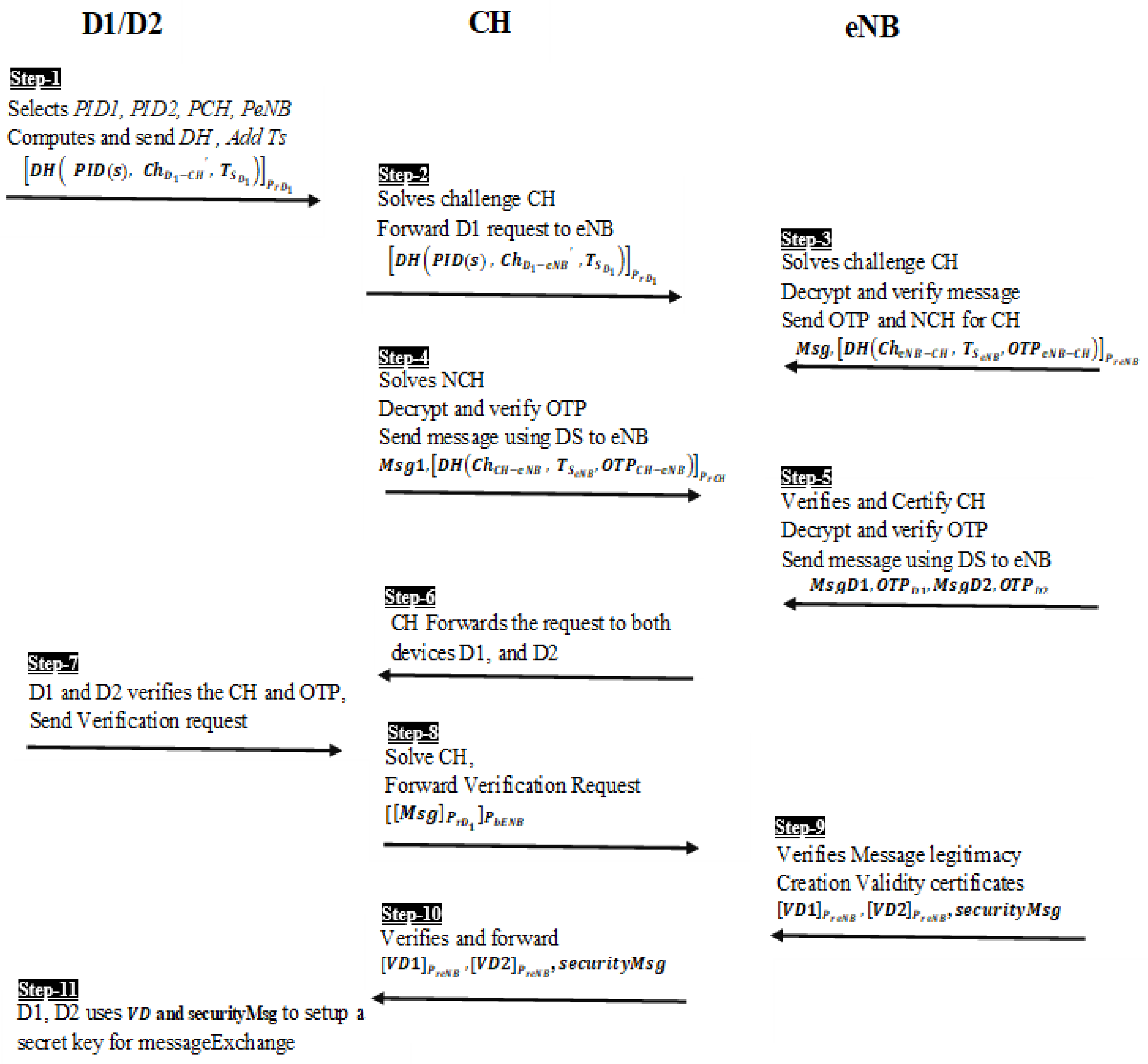
D1/D2
CH
eNB
Step-1
Selects PID1, PID2, PCH, PeNB
Computes and send DH , Add Ts
[DH(PID(s), Ch_{D1−CH}′, Ts_{D1})]_{PrD1}
Step-2
Solves challenge CH
Forward D1 request to eNB
[DH(PID(s), Ch_{D1−eNB}′, Ts_{D1})]_{PrD1}
Step-3
Solves challenge CH
Decrypt and verify message
Send OTP and NCH for CH
Msg, [DH(Ch_{eNB−CH}, Ts_{eNB}, OTP_{eNB−CH})]_{PreNB}
Step-4
Solves NCH
Decrypt and verify OTP
Send message using DS to eNB
Msg1, [DH(Ch_{CH−eNB}, Ts_{eNB}, OTP_{CH−eNB})]_{PrCH}
Step-5
Verifies and Certify CH
Decrypt and verify OTP
Send message using DS to eNB
MsgD1, OTP_{D1}, MsgD2, OTP_{D2}
Step-6
CH Forwards the request to both devices D1, and D2
Step-7
D1 and D2 verifies the CH and OTP, Send Verification request
Step-8
Solve CH,
Forward Verification Request
[[Msg]_{PrD1}]_{PbENB}
Step-9
Verifies Message legitimacy
Creation Validity certificates
[VD1]_{PreNB}, [VD2]_{PreNB}, securityMsg
Step-10
Verifies and forward
[VD1]_{PreNB}, [VD2]_{PreNB}, securityMsg
Step-11
D1, D2 uses VD and securityMsg to setup a secret key for messageExchange

FIGURE 3. Complete secure message exchange and authentication in LEMAP scheme.

pseudo-IDs, OTP, timestamp, challenge, and password and uses ECC with Deffie Hellmen for encryption-decryption and Elgamal for key exchange. The double hashing is done using the SHA v3 algorithm to send encrypted messages. Each message is double hashed and digitally signed with a private key of the sender and a public key of the receiver which ensures secure message transfer.

C. LEMAP ALGORITHM

Figure 3 shows all steps explained how D1 and D2 get authentication and authorization from eNB.

Step1: Device D1 sends a communication request to eNB. The request message contains the pseudo ID for devices D_1 and D_2, CH and eNB, challenge, timestamp, and the double hash of the message is sent to CH. The message is encrypted with the private key of D1 and the public key of CH which forwards the message to eNB. The message from D1 to eNB is encrypted with the public key of eNB.

Step2: The cluster Head forwards this request message from D1 to eNB with its new timestamp, challenge, and encrypted by the private key of CH. The whole message is encrypted with the public key of eNB.

Step3: eNB decrypts the message received from CH and sends it an OTP with a timestamp to verify the legitimacy of CH. The message is encrypted with the private key of eNB and the public key of CH.

Step4: CH solves OTP and responds to eNB with OTP solution, challenge. The hashed message is encrypted with the private key of CH and the public key of eNB is sent to eNB.

TABLE 2. Basic BAN logic formulas adopted for formal analysis.

No	Formal Message	Interpretation of Formal Message
1	$D_1 \mid\equiv Msg$	D_1 believes Msg.
2	$D_1 \triangleleft Msg$	D_1 sees Msg.
3	$D_1 \mid\sim Msg$	D_1 once said Msg.
4	$D_1 \Rightarrow Msg$	D_1 has jurisdiction over Msg.
5	$\# Msg$	Msg is fresh
6	$\{Msg\} K_{D(1,2)}$	Msg is encrypted with $K_{D(1,2)}$
7	$D_1 \overset{K_{D(1,2)}}{\longleftrightarrow} D_2$	D_1 and D_2 have a secret key of $K_{D(1,2)}$
8	$\rho_k(D_1, K_{D_1})$	D_1 has associated a good public key K_{D_1}
9	$\Pi(K_{D_1}^{-1})$	D_1 has a good private key $K_{D_1}^{-1}$
10	K_{CH}	Public key of CH
11	K_{eNB}	Public key of eNB

Step5: eNB decrypts message received from CH. eNB validates CH and now sends CH new OTP for both devices D1 and D2 to verify D1 and D2 legitimacy. The message is encrypted with the private key of eNB and public keys of D1 and D2. The whole message is encrypted by the public key of CH.

Step6: CH receives a message from eNB and decrypts the message with its private key. CH forwards this OTP to devices D1 with its timestamp and challenge. The message is encrypted by the private key of CH and the public key of D1.

Step7: CH receives a message from eNB and decrypts the message with its private key. CH forwards this OTP to devices D2 with its timestamp and challenge. The message is encrypted by the private key of CH and the public key of D2.

Step8: D1/D2 sends an authentication request message to CH with a new timestamp challenge with the double hash of the message. The message is encrypted by the private key of D1/D2 and the public key of eNB.

Step9: CH forwards validation request message from D1 and D2 to eNB. The message includes a timestamp, new challenge, and double hash of message encrypted by the private key of CH and public key of eNB.

Step10: Authentication Response Message where eNB validates both devices D_1 and D_2 and sends CH to forward validation response to both devices.

The request message contains credentials i.e. challenge and timestamp. This message also contains a double hash value of the challenge solution and timestamp which is signed by the private key of eNB. The message second portion contains response messages for D_1 and D_2 with credentials challenge, timestamp, and devices D_1&D_2 validation solution VD'_1, VD'_2 from eNB. The message is signed by the private key of eNB and encrypted by the public key of D_1 and D_2.

Step11: Authentication Response Message where eNB validates device D1 and CH forwards it to devices D1/D2. The message is prepared by utilizing two credentials i.e. challenge and timestamp. This message also contains the double hash value of the challenge solution and timestamp which is signed by the private key of CH. The message second portion contains validation response message VD1′ for D1 or VD2′ for D2 signed by the private key of eNB and signed and encrypted by the public key of device D1 or D2 respectively.

IV. FORMAL SECURITY ANALYSIS

In this section, formal verification of authentication protocols has been carried out. The proposed algorithm LEMAP with the desired authentication goals is verified using formal analysis based on Burrows, Abadi, and Needham (BAN) Logic [37].

A. BAN LOGIC RULES

For simplification of proof, Msg stands for the messages, and CH is used for Cluster Head. D_1 and D_2 stands for Device (1) and Device (2) respectively and eNB stands for evolved Node Base Station. K_p is used for a private key while P_k is used for the public key. During the analysis, device (1) will be used as D_1 and device (2) will be used as D_2. The basic notations are defined in Table 2.

The various inference rules are listed below; the lists above are the inference rules of the BAN logic. This research presents only related rules-based extensions.

$$\frac{D_1| \equiv D_2 \overset{K_{D(1,2)}}{\longleftrightarrow} D_1, D_1 \triangleleft \left(\{Msg\}_k\, SignedD_2\right)}{D_1 \mid\equiv D_2| \sim Msg} \tag{1}$$

$$\frac{D_1| \equiv (Msg)\,, D_1 \mid\equiv D_2| \sim Msg}{D_1 \mid\equiv D_2| \equiv (Msg)} \tag{2}$$

In Equation (2), D_1 believes that message Msg is fresh and D_1 believes that D_2 have sent once sent a message Msg. Thus D_1 believes that D_2 believes in message Msg.

$$\frac{D_1| \equiv D_2 \Rightarrow Msg, D_1 \mid\equiv D_2| \equiv Msg}{D_1| \equiv (Msg)} \tag{3}$$

In Equation (3), D_1 believes that D_2 have jurisdiction over message Msg. D_1 believes that D_2 believes in message Msg. Thus D_1 believes in message Msg.

$$\frac{D_1 \mid\equiv Msg, D_1| \equiv Rsp}{D_1| \equiv (Msg, Rsp)} \tag{4}$$

In Equation (4), D_1 believes in message Msg. D_1 also believes in message response Rsp. Thus D_1 believes in both messages Msg and response Rsp also as Equation (5).

$$\frac{D_1| \equiv (Msg, Rsp)}{D_1| \equiv Msg} \tag{5}$$

D_1 believes in both message Msg and response Rsp. Thus, in message Msg or vice versa D_1 believes in response Rsp shown as $D_1| \equiv Rsp$.

$$\frac{D_1| \equiv D_2| \equiv (Msg, Rsp)}{D_1 \mid\equiv D_2| \equiv Msg} \tag{6}$$

In Equation (6), D_1 believes that D_2 believes in both message Msg and response Rsp. Thus D_1 believes that D_2 believes in message Msg or vice versa D_1 believes that D_2 believes in message response Rsp written as $D_1 \mid\equiv D_2| \equiv Rsp$.

$$\frac{D_1 \mid\equiv D_2| \sim (Msg, Rsp)}{D_1 \mid\equiv D_2| \sim Msg} \tag{7}$$

In Equation (7), D_1 believes that D_2 once send both messages Msg and response Rsp. Thus D_1 believes that D_2 one sends message Msg. Equation (8), as shown at the bottom of the page, states, D_1 believes that P_{D_2} is the public key of D_2 and it has the corresponding private key K_{D_2}. D_1 also believes that it has a secure private session key that can decrypt the message. D_2 has jurisdiction to encrypt the message with its private key K_{D_2} and then encrypt with the public key of D_1 that is P_{D_1}. Thus D_1 believes that D_2 once sent message Msg. If D_1 has jurisdiction to do the message signature send to D_2. Thus D_1 has jurisdiction over message Msg such as $D_1 \lhd \mathrm{Msg}$.

$$\frac{D_1 \lhd \mu\left(\mathrm{Msg}, K_{D(1,2)}\right)}{D_1 \lhd \mathrm{Msg}} \tag{9}$$

Equation (9) shows, D_1 has jurisdiction to take the encryption of message Msg using the shared private key. Thus D_1 has jurisdiction over message Msg and vice versa, D_2 also has jurisdiction to use a shared private key and thus D_2 has jurisdiction over message Msg also shown in Equation (10).

$$\frac{D_1 \lhd \mu\left(\mathrm{Msg}, K^{-1}_{D(1,2)}\right)}{D_1 \lhd \mathrm{Msg}} \tag{10}$$

Equation (11) shows D_1 has jurisdiction to decrypt the message Msg using the shared private key. Thus D_1 has jurisdiction over message Msg and vice versa, D_2 also has jurisdiction to decrypt the message using a shared private key and thus D_2 has jurisdiction over message Msg.

$$\frac{D_1 \mid\equiv D_2 \mid \equiv \Delta\left(t_1, t_2\right), D_1 \mid\equiv D_2 \mid \sim \left(\theta(t_1, t_2), \mathrm{Msg}\right)}{D_1 \mid\equiv D_2 \mid \equiv (\mathrm{Msg})} \tag{11}$$

D_1 believes that D_2 selects a good time interval that is between t1 and t2. D_1 believes in D_2 that D_2 once sent message Msg and that is between time interval t1 and t2. Thus D_1 believes that D_2 believes in message Msg as stated in Equation (11). Before analyzing and verifying the authentication protocols, D2D security goals need to be clearly defined.

B. ANALYSIS OF LEMAP PROTOCOL

In the 2PAKEP benchmark protocol, assumptions are used to prove the security goals. The first assumption is that public and private keys have been distributed before the start of communication. The second assumption is that the message reaches within timestamp and due time is not expired. The third assumption is that channel is secure, and no attack can occur on the transmission. The proposed algorithm LEMAP is introduced where these assumptions are handled by introducing sound security principles and techniques.

1) AUTHENTICATION GOALS

This section elaborates the desired authentication goals to be achieved for multi-hop Device to Device (D2D) authentication protocols. Following authentication goals will be needed in LEMAP to prove that secure mutual authentication is achieved. In authentication goals, it is believed that all devices in communication shared a secret key and achieved the required goals to achieve secure mutual authentication.

All goals have been formulated in equations (12) – (15). In Equation (12), D1 believes in CH and shared a secret key with CH. Similarly, in Equation (13) CH believes at D1 and shared a secret key with D1. Hence it is clear from equations, D1 and CH both must have shared secret keys to get authentication.

$$\textbf{Goal 1}: D_1 \mid\equiv \mathrm{CH} \xleftrightarrow{SK} D_1 \tag{12}$$

$$\textbf{Goal 2}: \mathrm{CH} \mid\equiv D_1 \xleftrightarrow{SK} \mathrm{CH} \tag{13}$$

In Equation (14), D2 believes at CH and shared a secret key with CH. Similarly, CH believes in D2 and shared a secret key with D2. Thus, it is clear from Equations (14) and (15), D2 and CH both must have shared secret keys to get authentication.

$$\textbf{Goal 3}: D_2 \mid\equiv \mathrm{CH} \xleftrightarrow{SK} D_2 \tag{14}$$

$$\textbf{Goal 4}: \mathrm{CH} \mid\equiv D_2 \xleftrightarrow{SK} \mathrm{CH} \tag{15}$$

In Equation (16), CH believes at eNB and shared a secret key with eNB and in Equation (17), eNB believes at CH and shared a secret key with CH. So being a multi-hop scenario, D1, CH and eNB all shared secret keys to get secure mutual authentication.

$$\textbf{Goal 5}: \mathrm{CH} \mid\equiv \mathrm{eNB} \xleftrightarrow{SK} \mathrm{CH} \tag{16}$$

$$\textbf{Goal 6}: \mathrm{eNB} \mid\equiv \mathrm{CH} \xleftrightarrow{SK} \mathrm{eNB} \tag{17}$$

2) ASSUMPTIONS

The following assumptions are considered to prove that the proposed algorithm LEMAP achieves secure mutual authentication. For instance, it is assumed that all participating devices in communication shared a secret key. And all messages received at the destination are always fresh. It is assumed that D1 believes CH and has jurisdiction over request message X and CH believes in eNB and has jurisdiction over response message Y. All five assumptions are listed below;

1. A1: $D_1 \xleftrightarrow{SK} \mathrm{eNB}$ 2. A2: $\mathrm{eNB} \xleftrightarrow{SK} D_1$
3. A3: $\mathrm{eNB} \mid\equiv \#\mathrm{Ts}$ 4. A4: $D_1 \mid\equiv \mathrm{eNB} \Rightarrow X$
5. A5: $D_1, D_2 \mid\equiv \mathrm{eNB} \mid\equiv D_1, D_2 \xleftrightarrow{SK} \mathrm{eNB}$.

The first analysis of the authentication request message and the idealization of the message is tested as given below. Each

$$\frac{D_1 \mid\equiv P_{D2}\left(D_2, K_{D_2}\right), D_1 \mid\equiv \Pi(K^{-1}_{SS}), D_2 \lhd \{\{\mathrm{Msg}\}\, K_{D_2}\} P_{D_1}}{D_1 \mid\equiv D_2 \mid \sim \mathrm{Msg}} \tag{8}$$

communication message is explained and analyzed using BAN logic to verify security goals and how it helps to avoid different types of attacks.

Message 1 indicates that the authentication request message is sent from D_1 to D_2. This message contains pseudo-IDs, the timestamp, challenge, and hash of the message. The message is sent to CH and contains a message for eNB which is a trusted powerful device and all devices are registered with eNB. The double hash message is signed with the private key of the sender device D_1. An adversary cannot generate the message and a modification attack will not work even if the message is read and modified. This will also help to avoid DoS attacks as well. The message contains a timestamp that will prevent any replay attack. The temporal secret key SK is also sent so that a secret point of communication can be established without sharing any private key.

Idealization message 1:

$$\left\{\begin{array}{l}\mathrm{PID}_1, \mathrm{PID}_2, \mathrm{Ch}_{\mathrm{D}_1-\mathrm{eNB}}, \mathrm{T}_{\mathrm{S}_{\mathrm{D}_1}}, \\ \left[\mathrm{DH}\left(\mathrm{PID}_1, \mathrm{PID}_2, \mathrm{Ch}_{\mathrm{D}_1-\mathrm{eNB}}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{D}_1}}\right)\right]_{\mathrm{P}_{\mathrm{rD}_1}}\end{array}\right\}_{\mathrm{P}_{\mathrm{eNB}}}$$

Idealization message 2:

$$\left\{\begin{array}{l}\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}_{\mathrm{eNB}-\mathrm{D}_1}, \\ \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_1}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}\end{array}\right\}_{\mathrm{P}_{\mathrm{D}_1}},$$

$$\left\{\begin{array}{l}\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}_{\mathrm{eNB}-\mathrm{D}_2}, \\ \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_2}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}\end{array}\right\}_{\mathrm{P}_{\mathrm{D}_2}}$$

Idealization message 3:

$$\left\{\begin{array}{l}\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}_{\mathrm{eNB}-\mathrm{D}_1}, \\ \left[\mathrm{DH}\left(\mathrm{Ch}'_{\mathrm{eNB}-\mathrm{D}_1}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_1}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}\end{array}\right\}_{\mathrm{P}_{\mathrm{D}_1}}$$

Idealization message 4:

$$\left\{\begin{array}{l}\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}_{\mathrm{eNB}-\mathrm{D}_2}, \\ \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}_{\mathrm{eNB}-\mathrm{D}_2}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}\end{array}\right\}_{\mathrm{P}_{\mathrm{D}_2}}$$

Idealization message 4:

$$\left\{\mathrm{Ch}_{\mathrm{D}_1-\mathrm{eNB}}, \mathrm{T}_{\mathrm{s}_{\mathrm{D}_1}}, \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{D}_1-\mathrm{eNB}}{}', \mathrm{T}_{\mathrm{s}_{\mathrm{D}_1}}\right)\right]_{\mathrm{Pr}_{\mathrm{D}_1}}\right\}_{\mathrm{P}_{\mathrm{eNB}}}$$

Idealization message 5:

$$\left\{\mathrm{Ch}_{\mathrm{D}_2-\mathrm{eNB}}, \mathrm{T}_{\mathrm{s}_{\mathrm{D}_2}}, \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{D}_{21}-\mathrm{eNB}}{}', \mathrm{T}_{\mathrm{s}_{\mathrm{D}_2}}\right)\right]_{\mathrm{Pr}_{\mathrm{D}_2}}\right\}_{\mathrm{P}_{\mathrm{eNB}}}$$

Idealization message 6:

$$\left\{\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{VD}'_1\right)\right]_{\mathrm{Pr}_{\mathrm{eNB}}}\right\}_{\mathrm{P}_{\mathrm{D}_1}}$$

Idealization message 7:

$$\left\{\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{VD}'_2\right)\right]_{\mathrm{Pr}_{\mathrm{eNB}}}\right\}_{\mathrm{P}_{\mathrm{D}_2}}$$

It is seen from above that all different inference rules, D1, D2, and eNB have full belief on authentication response message and all its credentials especially secret key (OTP) that it is sent by the legitimate eNB which leads towards the authenticity and secrecy of the message. So, authentication goals 12, 13, 14, and 15 have been achieved and assumptions 18-23 have been verified. LEMAP protocol is fully secure against a MITM attack, replay attack, DoS attack, impersonation attack, and rogue device attack. Thus, it can be concluded that the proposed LEMAP single-hop authentication protocol has achieved secure mutual authentication and is fully secure against the given attacks.

C. PROOF USING BAN LOGIC

To achieve the above goals, we have the following steps:

Step 1: In accordance with *Msg*1, we can get:

$$S1 : \mathrm{eNB} \lhd \left[\mathrm{DH}\left(\mathrm{PID}_1, \mathrm{PID}_2, \mathrm{Ch}_{\mathrm{D}_1-\mathrm{eNB}}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{D}_1}}\right)\right]_{\mathrm{P}_{\mathrm{rD}_1}}$$

Step 2: From $S1$ and $A1$, we apply the message meaning rule to get:

$$S2 : \mathrm{eNB}| \equiv \mathrm{D}_1 \sim \left[\mathrm{DH}\left(\mathrm{PID}_1, \mathrm{PID}_2, \mathrm{Ch}_{\mathrm{D}_1-\mathrm{eNB}}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{D}_1}}\right)\right]_{\mathrm{P}_{\mathrm{rD}_1}}$$

Step 3: In accordance with $A2$, we apply the freshness rule to obtain:

$$S3 : \mathrm{eNB}| \equiv \# \left[\mathrm{DH}\left(\mathrm{PID}_1, \mathrm{PID}_2, \mathrm{Ch}_{\mathrm{D}_1-\mathrm{eNB}}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{D}_1}}\right)\right]_{\mathrm{P}_{\mathrm{rD}_1}}$$

Step 4: From $S2$ and $S3$, we apply the nonce verification rule to obtain:

$$S4 : \mathrm{eNB}| \equiv \mathrm{D}_1 | \equiv \left[\mathrm{DH}\left(\mathrm{PID}_1, \mathrm{PID}_2, \mathrm{Ch}_{\mathrm{D}_1-\mathrm{eNB}}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{D}_1}}\right)\right]_{\mathrm{P}_{\mathrm{rD}_1}}$$

Step 5: In accordance with *Msg*2, we can get:

$$S5 : \mathrm{eNB} \lhd \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_1}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}$$

Step 6: From $S5$ and $A3$, we apply the message meaning rule to obtain:

$$S6 : \mathrm{D}_1 | \equiv eNB \sim \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_1}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}$$

Step 7: In accordance with $A4$, we apply the freshness rule to obtain:

$$S7 : \mathrm{D}_1 | \equiv \# \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_1}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}$$

Step 8: From $S6$ and $S7$, we apply the nonce verification rule to get:

$$\begin{aligned} \mathrm{S}_8 : \mathrm{D}_1 | \equiv {} & \mathrm{eNB}| \\ & \equiv \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_1}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_1}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}} \end{aligned}$$

Step 9: In accordance with *Msg*4, we can get:

$$\mathrm{S}_9 : \mathrm{eNB} \lhd \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}_{\mathrm{eNB}-\mathrm{D}_2}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}$$

Step 10: From $S5$ and $A5$, we apply the message meaning rule to obtain:

$$S_{10} : \mathrm{eNB}| \equiv \mathrm{D}_2 \sim \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}_{\mathrm{eNB}-\mathrm{D}_2}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}$$

Step 11: In accordance with $A6$, we apply the freshness rule to obtain:

$$S11 : \mathrm{eNB}| \equiv \# \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB}-\mathrm{D}_2}{}', \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_2}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}$$

Step 12: From to $S10$ and $S11$, we apply the nonce verification rule to get:

$$S12 : eNB| \equiv \mathrm{D}_2| \equiv \left[\mathrm{DH}\left(\mathrm{Ch}'_{\mathrm{eNB}-\mathrm{D}_2}, \mathrm{T}_{\mathrm{S}_{\mathrm{eNB}}}, \mathrm{OTP}'_{\mathrm{eNB}-\mathrm{D}_2}\right)\right]_{\mathrm{P}_{\mathrm{r}_{\mathrm{eNB}}}}$$

Step 13:

According to $S4$; $S8$; $S12$; $A1$ and $A2$, we can get:

$$S_{13} : \mathrm{D}_1| \equiv \mathrm{eNB}| \equiv \mathrm{D}_1 \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{eNB} \qquad \text{(Goal 1)}$$

and

$$S_{14} : \mathrm{eNB}| \equiv \mathrm{D}_1| \equiv \mathrm{D}_1 \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{eNB} \qquad \text{(Goal 2)}$$

Step 14: From $S13$ and $A3$, we apply the jurisdiction rule to obtain:

$$S_{15} : \mathrm{D}_2| \equiv \mathrm{D}_2 \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{eNB} \qquad \text{(Goal 3)}$$

Step 15: From $S14$ and $A4$, we apply the jurisdiction rule to obtain:

$$S_{16} : \mathrm{eNB}| \equiv \mathrm{D}_2 \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{eNB} \qquad \text{(Goal 4)}$$

Goals 1-4 prove that LEMAP achieves mutual authentication between D_1, D_2 and eNB.

V. RESULTS AND ANALYSIS

A. SIMULATION SETUP

The performance study has been conducted in NCTUns 6.0 version to find the effect of Packet Delivery Ratio, Packet Overhead, and Processing times while comparing it with increasing the number of hops and non-transparent relays with and without the presence of attackers. For simulation four protocols LEMAP, TwoFactor, Chaotic and 2PAKEP were analyzed and tested. While implementing devices, this research considers the relaying devices like mobile devices having a 1GHZ processor with 500 MB RAM and 4GB ROM. This research does not include battery power or time as it was not considered as part of this study. The details are shown in Table 3.

Each device has similar capabilities and even the attacking nodes simplify the analysis, the attacking result thus may be affected if the illegitimate devices are high computation power devices. Each algorithm while their implementation within this research comparison considers the following properties and sizes to have a fair comparison as shown in Table 4.

TABLE 3. Device/relaying node computational parameters.

Device Properties	Formal Message
CPU	1GHZ
Cores	1
RAM	1GB
ROM	4GB
Cache	100 MB embedded with Processor
Battery Time	direct power

TABLE 4. Message sizes declaration of different message parts.

Communicating Message Part	Size
Hashing (SHA - V3)	512 bits
Message	4096 bits
Timestamp	512 bits
Nonce/ Random Number	128 bits
Pseudo-Identifier	512 bits
Identifier	128 bits
Private key	512 bits
Public key	512 bits
Smart Key Identifier	512 bits
Biometrics	1026 bits
XOR of two Data	512 bits
Session Key	512 bits

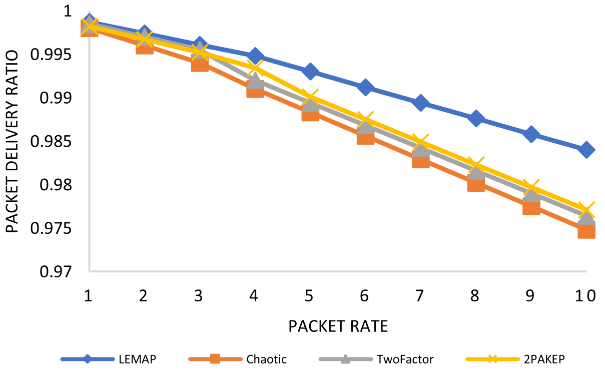

FIGURE 4. Packet delivery ration without attacker.

B. EXPERIMENTAL RESULTS AND ANALYSIS

Figure 4 shows the effect of packet delivery ratio (PDR) without an attacker in the network. The result shows that the proposed protocol LEMAP has the highest packet delivery ratio as the number of packets increases per message. PDR in the figure is set as per million bit/second. In the 2PAKEP protocol, PDR falls as the number of packets is increased. two-factor protocol PDR further lowers with the increase of packets per message and the Chaotic scheme shows the lowest PDR among all protocols. In LEMAP, the number of packets sent per message is smaller in size and requires low computation while the other two schemes 2PAKEP and TwoFactor have slightly lower PDR due to the computational complexity and new hash generation for forwarding messages. It is seen as the number of nodes increases, the PDR drops around 0.014% which is because of the increase in overhead caused by devices and nodes verification time. LEMAP as stated earlier perform better than 2PAKEP by around 0.07 millisecond and perform better than TwoFactor by 0.02 millisecond. The PDR of Chaotic is lower by 0.05 millisecond as compared to LEMAP. This difference is caused because of several changes in LEMAP as compared to other protocols such as embedding the acknowledgment inside normal messages and multi-factor verification at once. This difference is quite significant as more nodes add to the communication and request for data shown as packet rate. This may reach a difference of 0.92 milliseconds for Chaotic where Chaotic takes more time. Secondly, TwoFactor takes a slightly higher time than LEMAP that is 0.76 milliseconds. The least difference is with 2PAKEP which takes 0.07 milliseconds lower than TwoFactor due to short message size. Overall, the whole algorithm performs better in an ideal situation when there is no security breach.

When the attacker enters the network, the performance of LEMAP is still better than other benchmark protocols as it does not allow any MITM and replay attack and thus has higher throughput as compared to TwoFactor and 2PAKEP which do not handle replay attacks as shown in Figure 5. Also, the packet rate is still lower than the packet delivery ratio without attacks. Here attackers are considered as rogue devices or nodes that are jeopardizing the communication by not forwarding the communication, re-authentication request, and non-receipt of packet request. It is observed that all benchmarks and the proposed algorithm have a slight effect on PDR such as Chaotic is 0.13 millisecond slower than LEMAP while TwoFactor is slower than Chaotic by 0.042 milliseconds. The least difference is with 2PAKEP which is 0.01 milliseconds. When the illegitimate packets get higher in number, the PDR drops which is around the maximum for Chaotic that takes 0.31 milliseconds higher time than LEMAP because of the non-availability of certification validation option. The second-highest difference is with 2PAKEP which is around 0.272 milliseconds. The two-factor takes 0.26 milliseconds higher than LEMAP. The PDR drop is significant in other benchmarks due to re-verification requests, acknowledgment/NACK at one packet, and trust. LEMAP itself only has an effect of 0.08 millisecond that keeps the PDR above 87% achievement level which can help it in selection as one of the potential candidates for D2D communication.

Packet Overhead is the total time taken to send packets over a network that is the time taken from source to destination. In figure 6, it is obvious from simulation results that the proposed protocol LEMAP performs better compared to other benchmark protocols. In LEMAP, initial packets are hello packets that are smaller in size so they can be transmitted easily. LEMAP scheme shows a better approach as compared to 2PAKEP and Chaotic. The quick drop shows several authentication messages starting to validate the authentication. The complete diagram is shown in Figure 6. The packet overhead of LEMAP is lower as it reduces the packet size as compared to other schemes with added security and mitigation of various attacks. The Packet Overhead is the highest with TwoFactor which is 6.875% while 2PAKEP has the lowest packet overhead that is 2.675% higher than LEMAP. Chaotic takes 4.84% higher than LEMAP. All schemes have lower packet overhead as they use hash and drop all the illegitimate packets. Secondly, LEMAP uses a double hash scheme of multi-factors that make it slightly better than other schemes in catching the illegitimate packets.

If an attacker enters the network, the packet overhead is lower as the multi-factor authentication scheme allows the LEMAP to skip the packet exchange due to the introduction of multi-factor. If the attacker succeeds in its attack, the attacking node will be blocked. The results of packet overhead with the attacker are shown in Figure 7. When the

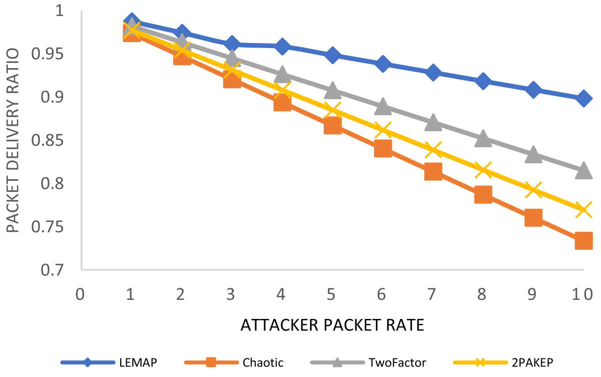

FIGURE 5. Packet delivery ration with attacker.

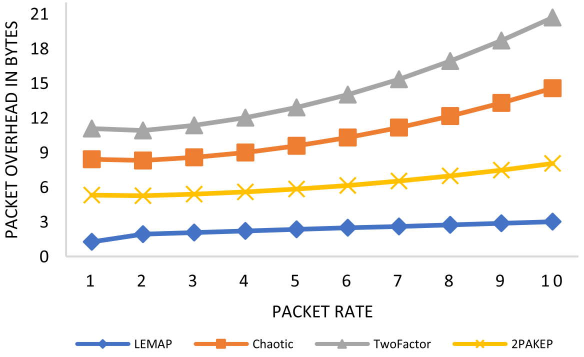

FIGURE 6. Packet overhead without attacker.

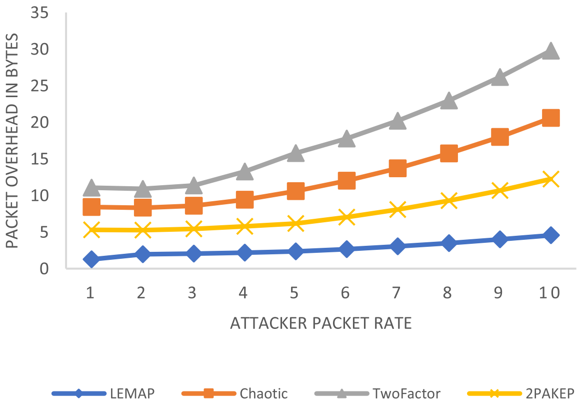

FIGURE 7. Packet overhead with attacker.

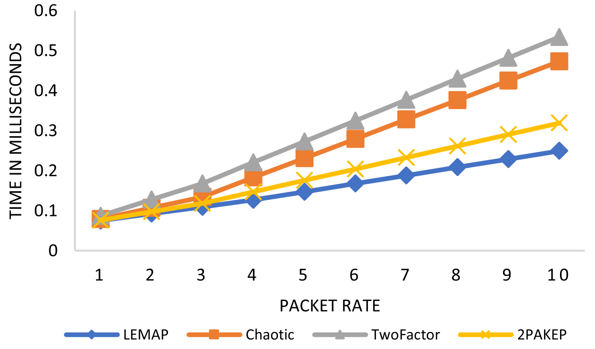

FIGURE 8. Processing time.

attacker is introduced, all schemes can mitigate the attacks with the usage of hash and timestamp but still, the packet drop will cause an extra packet that increases by packet overhead. The packet overhead further increases with the introduction of the attacker by 1.54% in LEAMP as compared to without attacker approaches. The highest packet overhead is with TwoFactor is 9.1% as compared to LEMAP approach due to an increase in packet drop rate as well as the creation of re-authentication packets. The second highest packet overhead is 6.0% of Chaotic as compared to LEMAP while 2PAKEP has 4.18% higher packet overhead as compared to LEMAP. LEMAP uses trust validation, multi-factor authentication, and double hash which lead to a slight improvement in the performance of the proposed algorithm. Current schemes also provide security at the same level but packet size increases significantly which causes lower PDR and higher computation costs.

Processing time in the security algorithm is an important parameter as it is directly related to delivery rate or ratio. If processing time is higher, it can result in higher processing costs as well as will be difficult to be adapted to small-scale devices. From simulation analysis, the processing time of the proposed protocol LEMAP is far lower than other benchmark algorithms. The processing time of LEMAP remains lower even the number of packets is increasing. It is better than 2PAKEP in terms of lower processing costs while other benchmark algorithms have higher processing costs. The processing cost is fully dependent on computation operations, encryption or decryption operations, and time to compute the signature. The complete graph is shown in Figure 8. The processing time of LEMAP is lower as compared to 2PAKEP by 6.9%, while chaotic takes 22.37% more time as compared to LEMAP. The time taken by other algorithms is higher due to their increased data size, separate processing of hash, timestamps, and key exchange. The maximum processing time is taken by TwoFactor is 28.4% due to the extra processing of two hashes.

As mentioned in the literature, with the increase of the number of rouge relays, the number of attacks also increases and when rouge relays number increases as compared to legitimate relays, the traffic cannot be transmitted which may result in a DoS attack. LEMAP still ensures that no illegitimate traffic can pass through the network due to prior registration and mutual authentication. The effect of rouge relays and PDR is shown in Figure 9. The delay in the LEMAP scheme is due to the verification of nodes and sending of the verification message again. In this experiment, we considered a total of 25 nodes out of which a maximum of 10 nodes is compromised. This research did not check the effect of rouge relays above 10 as one of the benchmarks, Chaotic PDR has dropped to a non-acceptable level. There is a significant drop in LEAMP PDR that is around 50% but this experiment considered only 25 nodes in the experiment out of which 40% are compromised. This is better as the trust and validation model is embedded in the proposed algorithm while another benchmark lacks this feature. The only acceptable level is at 25% for other benchmarks where chaotic has a PDR of 49.47%, 2PAKEP has PDR to 55.62% and TwoFactor has a PDR of 66.48% while LEMAP has a PDR of around 75%. Later, the drop in PDR of these benchmarks was already explained due to no feedback on transmission and non-consideration of more than two or three nodes being compromised.

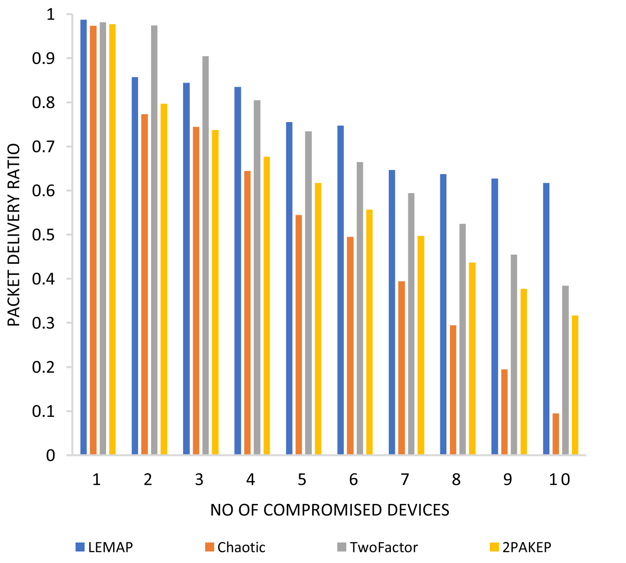

FIGURE 9. Effect of increasing rouge relays in terms of traffic simulation.

C. DISCUSSION ON COMPUTATIONAL SECURITY ANALYSIS

The proposed protocol LEMAP validates that it is lightweight than other benchmark protocols. Packet delivery ratio of LEMAP protocol is better than other protocols in both situations either the network is without an attacker or the attacker is present in the network but still LEMAP results in high data rate and increased performance. Results have proved that the packet overhead of LEMAP is also better than other protocols due to hello packets of smaller size. The processing time of LEMAP is also proved that it is lower than other protocols even with an increased number of packets.

But in the case of vulnerable situations and normal traffic, one of the other benchmark protocols that perform better is TwoFactor. It provides PDR up to 73% when there are around 25% of rouge relays but as the percentage of rouge nodes increases, the effect on transmission failure increases. One of the reasons is that trust validation and certificate are not part of current security schemes, especially in selected benchmarks. Secondly, this research considers that devices can be compromised in bulk as compared to existing security schemes that only consider two devices' communication with a third device acting as an attacker. The authentication overhead of LEMAP is the lowest and hence it can be adapted even in case of vulnerable situations such as an increase in rouge relays or DoS attacks.

1) SECURITY ANALYSIS

It is mandatory for any method or algorithm to be considered fully secure if it works well against any kind of brute force attack or intelligent attack. In this section, LEMAP will be checked thoroughly against well-known computational attacks i.e. discrete logarithm problem (DLP). DLP is one of the trapdoor functions that can easily be calculated but is very critical to go back to its original shape and is very challenging from computational perspectives as compared to factorization problems utilized in RSA or DH algorithm [38], [39]. LEMAP also belongs to such a category where the finding of the key is tremendously challenging. LEMAP utilizes an ECC cryptosystem where the key selection size between devices and eNB will be to be 512 bits and the session key will be 384 bits.

ECC is constructed on a finite cyclic group F_c, for two primitive elements α and β where both α *and* $\beta \epsilon F_c$. While DLP is finding the integer k where k satisfies the following criteria $\alpha^K \equiv \beta$ or $k = \log_\alpha \beta$. Now in terms of ECC, we are required to calculate multiplicative inverse k while $\alpha, \beta \text{and} F_c$. To conduct a DLP check, there are several mechanisms are available. However, in this article, we use brute force attack (BFA), Pollard's rho method, and the Baby Step Giant Step_(BsGs) method.

2) BRUTE FORCE ATTACK (BFA)

In BFA, we must find the K time point multiplication with the base point F_c such that α is achieved. While the Elliptic curve works on an elliptic equation that makes the rotation with K, so the complexity becomes more when the key is rotated β times. Even if this communication is cracked, the proposed algorithm uses session-based encryption using the same algorithm making the cracking to be done for each session. Thus, the complexity will add up for each session and vice versa; if one of the sessions is hacked (that is not possible) so only the session communication may become compromised and not the rest of the sessions.

Usually, the attacker will start with K = 1 then k =2, and so on. If the size of k = 4, bits then about after 4096 tries we can find k. But for our case, as the key is 512 bits large so it is practically impossible to conduct an attack as required possible attempts will be 2^{15360}. Or even attack 384 bits that means will be 2^{7680} cannot be performed. Suppose we have a world-fast supercomputer that is IBM AC922 costing 200 million USD [40]. The speed of single processing on this processor is 2^{50} per second as explained around 3 billion cycles to be executed. Thus, around 1536 years will be required to do the cracking process or we can buy 1536 computers to crack the key in one year. We have set the refresh time to be one week for the main key while for the session the smaller key will change after each session. This proves that brute force attack is highly expensive (around 3 trillion USD) that is almost impossible to conduct. Moreover, we have taken the assumption that each key can be computed in one second while it requires more computation for a higher key size.

TABLE 5. Key size comparison.

RSA/DH	ECC	AES (Symmetric)
1024	160	80
2048	224	112
3072	256	128
7680	384	192
15360	512	256
1966080	1024	512

TABLE 6. Processing time of computing operations.

Operation	Notation Used	Time Required in milliseconds
Encryption symmetric	t_e	0.5 ms
Encryption asymmetric ECC	t_h	1.8 ms
Multiplication encryption	t_m	1.8 ms
Pairing time	t_p	13.5 ms

3) POLLARD's RHO METHOD

It is a better and more intelligent way to attack the setup as it supports parallelization and random walk. Pollard's rho method reduced the permutations by a square root. So only possible keys will reduce the number of permutations by one equation to 2^{15359}, hence requiring almost the same time as the BFA. The Pollard rho method will fail here also. LEMAP is a generic algorithm and allows the key size to be increased according to the security required such as if the key size is 1024 then we have almost $2^{1966080}$ combinations that will require above 1.9 million years.

4) BABY STEP GIANT STEP (BsGs)

BsGs is also a method that required an intelligent approach to crack the security key in two directions. It also reduced the number of efforts to $\sqrt{N}$ times thus making it half the size. In BsGs, the task is to find k where $k > \sqrt{\#\beta}$ and compute $\alpha = g^k$ where g can from 0 to k. As still, it is computationally expensive even after $\sqrt{\#\beta}$, it will just reduce the efforts by half providing surety to have complexity such as DLP.

5) KEYSPACE

A keyspace is a way to store all possible permutations of pair and then just compare the results. We are considering that

TABLE 7. Computation cost.

Security Protocol	Computation Cost
LEMAP	$21t_m + 22t_e + 21t_h$
Chaotic	$23t_h + 4t_m + 5t_p + t_e$
TwoFactor	$29t_h + 2t_m + 6t_p$
2PAKEP	$31t_h + t_m + 5t_p + 2t_e$

the key calculation takes a second, so the validity holds true for the keyspace. This means we require 215359 * 29, which is equal to 215368 bits or 215365 bytes to store the key or 215347 petabytes minimum, making it extremely complex for parallel processing even through IBM AC922.

6) KEY SIZE

Key size is an important feature of ECC that makes it extremely usable in the current era where supercomputers can compute billions of computations per second. ECC is based on elliptic curves and thus their key size complexity is far higher than that of RSA and DH. Table 5 shows the detailed comparison of the key size of ECC as compared to symmetric key as well as RSA and DH. Table 5 is made on values reported by [17], [41]–[44]. It is clear from table 4 that ECC consumes lesser space than traditional asymmetric algorithms and double the space than symmetric algorithms. Thus, ECC provides the best approach to date to use for small devices. As storage, processing, and security of ECC are highly better than any other security algorithms in practice.

7) PROCESSING COST

The major cost in all ECC-based algorithms is pairing, multiplication, and encryption as mentioned by [12], [45]–[47]. Thus, we will only consider these operations as a major contributor to computations. We have considered the world's fastest and most powerful supercomputer for the attack but in practice, the purpose of LEMAP is to be executed on small devices such as mobile phones or small computing devices. Thus to consider the computation cost or processing cost we will use benchmark device power where each implementation was executed on Intel 3.0 GHz Pentium processor. The curve used in the implementation was 6 degrees with a 160-bit size. The processing time took around 4.5ms on average for pairing while 0.6ms for multiplication. Approximately, for a 1GHZ processor, the time taken will be 13.5ms as 4.5 * 3 over 1 GHz is 13.5ms. The time to compute the exponential computation is 1.8ms for a 1 GHz processor. For ECC the encryption and decryption are also multiplication thus it will be a multiple of multiplication steps. While in the case of symmetric encryption, it takes 0.5ms for performing the encryption on a 1Ghz processor. Let t_p the cost of pairing while t_m the cost of multiplication and t_e be the cost of encryption as shown in Table 6.

For Chaotic protocol, there are several operations required such as one exponential computation and encryption operation thus requiring $23t_h + 4t_m + 5t_p + t_e$ in time. There are twenty-three hashing operations requiring $23t_h$ in time.

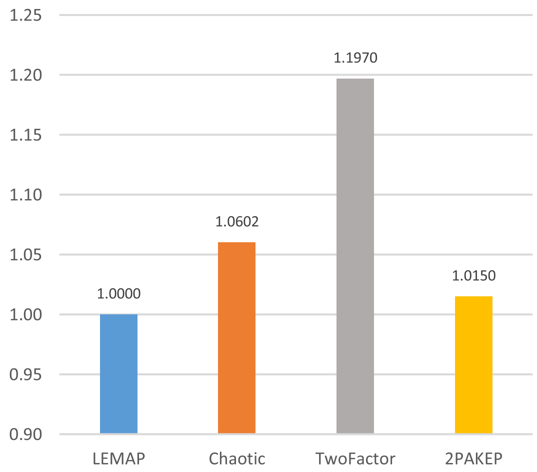

FIGURE 10. Ratio of computational cost.

For key generation, there are encryption using public and private keys of the session thus requiring $4t_m$ in time. For pairing five operations are required $5t_p$.Thus in total, it will be $23t_h + 4t_m + 5t_p + t_e$. For a two-factor protocol, each node must calculate their key and two hashing operations, thus requiring $2t_m$ time cost. With each random number, there is a key generation that requires $2t_m$ time in cost. Four signature generation operations will require $6t_p$ time. There are two encryption operations thus requiring $2t_m$ time. Hence, it will be $29t_h + 2t_m + 6t_p$intotal. For the 2PAKEP protocol, there are thirty-one hashing operations for each key so it requires $31t_h$ in time. Each device must generate the key pairs which will require $2t_m$ in time. There are five signature operations requiring $5t_p$ in time. For each encryption, it will require t_m time. Merging the messages in signature encryption will require $2t_e$ operation time in cost. Thus, in total $31t_h + t_m + 5t_p + 2t_e$ will be time cost.

For LEMAP protocol, there are twenty-two encryption operations requiring $22t_e$ time cost. There are twenty-one hash operations that will require $21t_h$ time. Thus, in total, we will need $21t_m+22t_e+21t_h$ as the time cost. Table 7 shows the computation cost of each security algorithm along with LEMAP.

Figure 10 shows the computation cost for each of the major operations such as signature, encryption, hashing, and random number calculation. It is observed that in terms of signature operation, LEMAP performs better than other benchmark algorithms. In the case of encryption, the time cost of LEMAP and 2PAKEP is the lowest while in the case of other operations cost of LEMAP and Chaotic have the lowest. Thus overall, the time cost of the proposed LEMAP is the lowest as compared to selected benchmark algorithms. It also provides better security as compared to existing security algorithms

8) VERIFICATION OF SECURITY REQUIREMENTS

It is mandatory to verify whether LEMAP fulfilled all the security requirements, for instance, confidentiality, integrity, non-repudiation, and mutual authentication. This section will elaborate in-depth security analysis against the baseline security requirements.

9) DATA CONFIDENTIALITY

The basic definition of confidentiality is that the date must not be seen by any third party. Thus, to ensure confidentiality of the proposed LEMAP, it must be evaluated whether the data sent can be seen by any third party. For this, it can be seen that given below Equations (18) & (19) are first encrypted by the receiver's public key. In equation 18, there are three receivers, i.e. CH, eNB, and D1, thus, it can be seen that respective messages are encrypted using their respective public keys. The same concepts apply to Equation (19). Thus, it can be said that the proposed scheme well ensure the confidentiality of data.

$$\left\{\begin{array}{l}\mathrm{Ch}_{\mathrm{CH-D_1}}, \mathrm{T}_{\mathrm{S_{CH}}}, \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{CH-D_1}}{}', \mathrm{T}_{\mathrm{S_{CH}}}\right)\right]_{\mathrm{Pr_{CH}}},\\ \mathrm{Ch}_{\mathrm{eNB-D_1}}, \mathrm{T}_{\mathrm{S_{eNB-D_1}}},\\ \mathrm{VD_1}'\left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB-D_1}}{}', \mathrm{T}_{\mathrm{S_{eNB-D_1}}}, \mathrm{VD_1}'\right)\right]_{\mathrm{Pr_{eNB}}}\end{array}\right\}_{\mathrm{P_{D_1}}} \tag{18}$$

$$\left\{\begin{array}{l}\mathrm{Ch}_{\mathrm{CH-D_2}}, \mathrm{T}_{\mathrm{S_{CH}}}, \left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{CH-D_2}}{}', \mathrm{T}_{\mathrm{S_{CH}}}\right)\right]_{\mathrm{Pr_{CH}}},\\ \mathrm{Ch}_{\mathrm{eNB-D_2}}, \mathrm{T}_{\mathrm{S_{eNB-D_2}}},\\ \mathrm{VD_2}'\left[\mathrm{DH}\left(\mathrm{Ch}_{\mathrm{eNB-D_2}}{}', \mathrm{T}_{\mathrm{S_{eNB-D_2}}}, \mathrm{VD_2}'\right)\right]_{\mathrm{Pr_{eNB}}}\end{array}\right\}_{\mathrm{P_{D_2}}} \tag{19}$$

10) DATA INTEGRITY, TRACEABILITY, AND NON-REPUDIATION

To ensure data integrity during the end to end to communication, the message is first encrypted with the sender's private key and later the message is hashed using SHA-3. Over the insecure channel, the hashed value together with an encrypted message is sent. On the receiver end, the receiver hashed the encrypted message and matched it with the hashed value (the hashed value sent over the insecure channel), if both values matched which proves that the message is not tempered. Moreover, since the sender's message is encrypted with the sender's private key, there is no method, the sender can deny the sending of messages. This also ensures the non-repudiation property of security requirements.

11) USER PRIVACY

In device-to-device communication, if real identities are not hidden properly then it can cause several privacy issues, which consequently can lead towards identity theft attacks which can be a major cause for impersonation attacks. Pseudo-identities of every participating device are utilized in LEMAP to hide the real identities. However, only eNB knows the real identity of the participating devices for secrecy and authenticity purposes. Thus, our proposed LEMAP ensures user privacy.

12) MUTUAL AUTHENTICATION

In LEMAP, it is mandatory for all the participating devices to first register with eNB and get their public and private keys to avoid impersonation attacks. MFT contains all registration records of validated devices and is shared with eNB. Thus, the validation trust on keys is already established. Secondly, LEMAP is a multifactor authentication scheme, where a second phase and third phase OTP and biometrics are utilized respectively. These OTP and biometrics are shared mutually by both parties thus ensuring mutual authentication.

VI. CONCLUSION

This research has developed a Lightweight ECC-based Multi-factor Authentication Protocol (LEMAP) D2D to ensure security in multi-hop D2D communication. The developed security algorithm provides not only better security but also decreases extra communication and computation overhead due to its lightweight mechanism. Consequently, it will reduce the processing and storage burden on small devices. There is a lot of research on security algorithms for single-hop D2D, while multi-hop D2D research is still at the beginning stage. This research focused on both multi-hop D2D as well as direct D2D communication. The algorithm is based on ECC and multi-factor authentication of devices as multi-hop D2D allows miniature cellular devices to act as decode and forwarding relay. To secure communication between two devices, a LEMAP protocol has been developed. LEMAP is safe against impersonation attacks, replay attacks, MITM attacks, DoS attacks, and device rogue attacks. D2D multi-hop communication for disastrous areas where there is a lack of infrastructure deployment can be considered as a key research area. LEMAP provides an adaptive approach but still, the performance and security of multi-hop for LEMAP can be a potential research direction. Multi-hop D2D networks can increase the cost as the dual interface is required for users to switch to either D2D or cellular. This area can be future research to decrease the D2D infrastructure deployment cost.

ACKNOWLEDGMENT

Yasir Javed and Adnan Shahid Khan received the grant. The sponsors' websites: https://ric.psu.edu.sa/ and https://www.riec.unimas.my.

REFERENCES

[1] A. Asadi, Q. Wing, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, 4th Quart., 2014, doi: 10.1109/COMST.2014.2319555.

[2] G. S. Gaba, G. Kumar, T.-H. Kim, H. Monga, and P. Kumar, "Secure device-to-device communications for 5G enabled Internet of Things applications," *Comput. Commun.*, vol. 169, pp. 114–128, Mar. 2021, doi: 10.1016/j.comcom.2021.01.010.

[3] J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchain design for trusted decentralized IoT networks," in *Proc. 13th Annu. Conf. Syst. Syst. Eng. (SoSE)*, Jun. 2018, pp. 169–174, doi: 10.1109/SYSOSE.2018.8428720.

[4] C. Suraci, S. Pizzi, A. Molinaro, A. Iera, and G. Araniti, "An RSA-based algorithm for secure D2D-aided multicast delivery of multimedia services," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Oct. 2020, pp. 1–6, doi: 10.1109/BMSB49480.2020.9379851.

[5] J. Liu, L. Zhang, R. Sun, X. Du, and M. Guizani, "Mutual heterogeneous signcryption schemes for 5G network slicings," 2018, *arXiv:1811.03741*.

[6] A. S. Khan *et al.*, "Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS)," *J. Ambient Intell. Hum. Comput.*, 2021, doi: 10.1007/s12652-021-02968-6.

[7] N. Koblitz, ''Elliptic curve cryptosystems, *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[8] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, ''Securing the Internet of Things in a quantum world,'' *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017, doi: 10.1109/MCOM.2017.1600522CM.

[9] 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,'' *Appl. Sci.*, vol. 10, no. 1, p. 217, Dec. 2019, doi: 10.3390/app10010217.

[10] C. Suraci, S. Pizzi, D. Garompolo, G. Araniti, A. Molinaro, and A. Iera, ''Trusted and secured D2D-aided communications in 5G networks,'' *Ad Hoc Netw.*, vol. 114, Apr. 2021, Art. no. 102403, doi: 10.1016/j.adhoc.2020.102403.

[11] S. A. Vanstone, ''Next generation security for wireless: Elliptic curve cryptography,'' *Comput. Secur.*, vol. 22, no. 5, pp. 412–415, 2003. [Online]. Available: http://dblp.uni-trier.de/db/journals/compsec/compsec22.html#Vanstone03

[12] M. Wang, Z. Yan, and V. Niemi, ''UAKA-D2D: Universal authentication and key agreement protocol in D2D communications,'' *Mobile Netw. Appl.*, vol. 22, no. 3, pp. 510–525, Jun. 2017, doi: 10.1007/s11036-017-0870-5.

[13] M. Cao, L. Wang, H. Xu, D. Chen, C. Lou, N. Zhang, Y. Zhu, and Z. Qin, ''Sec-D2D: A secure and lightweight D2D communication system with multiple sensors,'' *IEEE Access*, vol. 7, pp. 33759–33770, 2019, doi: 10.1109/ACCESS.2019.2900727.

[14] P. Gope, ''LAAP: Lightweight anonymous authentication protocol for D2D-aided fog computing paradigm,'' *Comput. Secur.*, vol. 86, pp. 223–237, Sep. 2019, doi: 10.1016/j.cose.2019.06.003.

[15] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, ''Secure trust-based blockchain architecture to prevent attacks in VANET,'' *Sensors*, vol. 19, no. 22, p. 4954, Nov. 2019, doi: 10.3390/s19224954.

[16] K. Park, Y. Park, Y. Park, and A. K. Das, ''2PAKEP: Provably secure and efficient two-party authenticated key exchange protocol for mobile environment,'' *IEEE Access*, vol. 6, pp. 30225–30241, 2018, doi: 10.1109/ACCESS.2018.2844190.

[17] Y. Javed, A. Khan, A. Qahar, and J. Abdullah, ''EEoP: A lightweight security scheme over PKI in D2D cellular networks,'' *J. Telecommun. Electron. Comput. Eng.*, vol. 9, nos. 3–11, pp. 99–105, 2017.

[18] Z. Ahmad, A. Shahid Khan, K. Nisar, I. Haider, R. Hassan, M. R. Haque, S. Tarmizi, and J. J. P. C. Rodrigues, ''Anomaly detection using deep neural network for IoT architecture,'' *Appl. Sci.*, vol. 11, no. 15, p. 7050, Jul. 2021, doi: 10.3390/APP11157050.

[19] H. A. U. Mustafa, M. A. Imran, M. Z. Shakir, A. Imran, and R. Tafazolli, ''Separation framework: An enabler for cooperative and D2D communication for future 5G networks,'' *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 419–445, 1st Quart., 2016, doi: 10.1109/COMST.2015.2459596.

[20] V. Adat, I. Politis, C. Tselios, P. Galiotos, and S. Kotsopoulos, ''On blockchain enhanced secure network coding for 5G deployments,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7, doi: 10.1109/GLOCOM.2018.8647581.

[21] F. Hu and N. K. Sharma, ''Security considerations in ad hoc sensor networks,'' *Ad Hoc Netw.*, vol. 3, no. 1, pp. 69–89, 2005, doi: 10.1016/j.adhoc.2003.09.009.

[22] F. Ahmad, Z. Ahmad, C. A. Kerrache, F. Kurugollu, A. Adnane, and E. Barka, ''Blockchain in Internet-of-Things: Architecture, applications and research directions,'' in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Apr. 2019, pp. 1–6, doi: 10.1109/ICCISCI.2019.8716450.

[23] S. O. Maikol, A. S. Khan, and Y. Javed, ''A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities,'' *Int. J. Integr. Eng.*, vol. 13, no. 2, pp. 127–135, 2021.

[24] S. Aqeel, A. S. Khan, Z. Ahmad, and J. Abdullah, ''A comprehensive study on DNA based Security scheme using deep learning in healthcare,'' *EDPACS*, pp. 1–7, Oct. 2021, doi: 10.1080/07366981.2021.1958742.

[25] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, ''A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions,'' *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020, doi: 10.1109/COMST.2019.2933899.

[26] A. Zhang and X. Lin, ''Security-aware and privacy-preserving D2D communications in 5G,'' *IEEE Netw.*, vol. 31, no. 4, pp. 70–77, Jul./Aug. 2017, doi: 10.1109/MNET.2017.1600290.

[27] W. Xiong, F. Zhou, R. Wang, R. Lan, X. Sun, and X. Luo, ''An efficient and secure two-factor password authentication scheme with card Reader(Terminal) verification,'' *IEEE Access*, vol. 6, pp. 70707–70719, 2018, doi: 10.1109/ACCESS.2018.2869535.

[28] 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 Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017, doi: 10.1109/COMST.2017.2649687.

[29] T. Balan, A. Balan, and F. Sandu, ''SDR implementation of a D2D security cryptographic mechanism,'' *IEEE Access*, vol. 7, pp. 38847–38855, 2019, doi: 10.1109/ACCESS.2019.2904909.

[30] A. S. Khan, Y. Javed, J. Abdullah, J. Nazim, and N. Khan, ''Security issues in 5G device to device communication,'' *Int. J. Comput. Sci. Netw. Secur.*, vol. 17, no. 5, p. 366, 2017.

[31] D. Kim, S. Seo, H. Kim, W. G. Lim, and Y. K. Lee, ''A study on the concept of using efficient lightweight hash chain to improve authentication in VMF military standard,'' *Appl. Sci.*, vol. 10, no. 24, p. 8999, 2020, doi: 10.3390/app10248999.

[32] M. Amine Ferrag, L. Maglaras, A. Derhab, and H. Janicke, ''Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues,'' 2018, *arXiv:1803.10281*.

[33] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, ''A comprehensive guide to 5G security,'' in *A Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2018, pp. 1–440, doi: 10.1002/9781119293071.

[34] J. Xiong, Y. Zhang, X. Li, M. Lin, Z. Yao, and G. Liu, ''RSE-PoW: A role symmetric encryption PoW scheme with authorized deduplication for multimedia data,'' *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 650–663, 2018, doi: 10.1007/s11036-017-0975-x.

[35] M. Wang and Z. Yan, ''A survey on security in D2D communications,'' *Mobile Netw. Appl.*, vol. 22, no. 2, pp. 195–208, Apr. 2017, doi: 10.1007/s11036-016-0741-5.

[36] N. Khan, J. Abdullah, and A. S. Khan, ''Defending malicious script attacks using machine learning classifiers,'' *Wireless Commun. Mobile Comput.*, vol. 2017, Feb. 2017, doi: 10.1155/2017/5360472.

[37] C. Boyd and W. Mao, ''On a limitation of BAN logic,'' in *Advances in Cryptology—EUROCRYPT'93* (Lecture Notes in Computer Science), vol. 765, T. Helleseth, Ed. Berlin, Germany: Springer, 1994, doi: 10.1007/3-540-48285-7_20.

[38] K. Gupta and S. Silakari, ''ECC over RSA for asymmetric encryption: A review,'' *Int. J. Comput. Sci. Issues*, vol. 8, no. 2, p. 814, 2011. [Online]. Available: http://www.IJCSI.org.

[39] R. Steinfeld and Y. Zheng, ''A signcryption scheme based on integer factorization,'' in *Proc. Int. Workshop Inf. Secur.* 2000, pp. 308–322, doi: 10.1007/3-540-44456-4_23.

[40] R. Nohria and G. Santos, *IBM Power System AC922–Technical Overview and Introduction*. IBM Redbooks, 2018.

[41] R. Mahmood Saqib, A. Shahid Khan, Y. Javed, S. Ahmad, K. Nisar, I. A. Abbasi, M. Reazul Haque, and A. Ahmadi Julaihi, ''Analysis and intellectual structure of the multi-factor authentication in information security,'' *Intell. Autom. Soft Comput.*, vol. 32, no. 3, pp. 1633–1647, 2022, doi: 10.32604/IASC.2022.021786.

[42] L. F. Abdulrazak, A. S. Khan, A. A. Julaihi, and S. Tarmizi, ''RSSI and public key infrastructure based secure communication in autonomous vehicular networks,'' *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 12, pp. 298–304, 2018.

[43] M. S. Dildar, N. Khan, J. B. Abdullah, and A. S. Khan, ''Effective way to defend the hypervisor attacks in cloud computing,'' in *Proc. 2nd Int. Conf. Anti-Cyber Crimes (ICACC)*, Mar. 2017, pp. 154–159, doi: 10.1109/ANTI-CYBERCRIME.2017.7905282.

[44] J. Bos, M. Kaihara, and T. Kleinjung, ''On the security of 1024-bit RSA and 160-bit elliptic curve cryptography,'' *IACR Cryptol. ePrint*, vol. 57, no. 1, pp. 1–19, 2009. [Online]. Available: http://lacal.epfl.ch/files/content/sites/lacal/files/papers/ecdl2.pdf.

[45] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, ''SeDS: Secure data sharing strategy for D2D communication in LTE-advanced networks,'' *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659–2672, Apr. 2016, doi: 10.1109/TVT.2015.2416002.

[46] A. Zhang, L. Wang, X. Ye, and X. Lin, ''Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems,'' *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 662–675, Mar. 2017.

[47] J. Y. Kim, W. Hu, H. Shafagh, and S. Jha, ''SEDA: Secure over-the-air code dissemination protocol for the Internet of Things,'' *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 6, pp. 1041–1054, Nov. 2018, doi: 10.1109/TDSC.2016.2639503.

ADNAN SHAHID KHAN (Senior Member, IEEE) received the B.Sc. degree (Hons.) in computer science from the University of the Punjab, Lahore, Pakistan, in 2005, and the master's, Ph.D., and Postdoctoral degrees in networks and information security from Universiti Teknologi Malaysia, Johor Bahru, Malaysia, in 2008, 2012, and 2013, respectively. He is currently a Senior Lecturer with the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak. His research interests include wireless communication, cloud computing, the Internet of Things, software-defined networking, cryptography, networks, and information security.

YASIR JAVED (Member, IEEE) received the Ph.D. degree from UNIMAS, Sarawak, in 2020. He is a Skilled Senior Programmer/Developer with more than 15 years of experience in programming, software development, project management, and analytics. He is also working as Research Engineer at the COINS Research Group. He has successfully completed various international and national research funding projects. He has served as an Analyst Programmer at the Prince Megren Data Center, Center of Excellence and Research, and Initiative Center, Prince Sultan University. He is currently an Active Member of the RIOTU Group, Prince Sultan University. His research interests include programming, robotics, drones, vehicular platoons, secure software development, mobile apps security, signal processing, the IoT analytics, intelligent applications, statistics, data analytics, forensics analysis, big data, and predictive computing.

RASHAD MAHMOOD SAQIB received the master's degree in computer science (networks) from the University of the Punjab, Lahore, Pakistan. He is currently pursuing the Ph.D. degree with the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Malaysia. He has worked at the Ministry of Foreign Affairs, Pakistan, as the Deputy Director Networks, from 2008 to 2010. He has also worked as a Network Manager with the Higher Education Commission of Pakistan, from 2006 to 2008. He is currently working as a Lecturer with the Computer Science Department, Applied College, King Abdul Aziz University, Jeddah, Saudi Arabia. His research interests include cryptography, cyber security, wireless communication, and cloud.

ZEESHAN AHMAD (Member, IEEE) received the B.S. degree in computer engineering from COMSATS University Islamabad, Pakistan, in 2005, the M.S. degree in electrical engineering (telecommunication) from Kalmar University College, Sweden, in 2008, and the M.S. degree in computer science (networks) from the Virtual University of Pakistan, in 2019. He is currently pursuing the Ph.D. degree with Universiti Malaysia Sarawak (UNIMAS), Sarawak, Malaysia. He worked with the Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain, for his M.S. degree thesis for six months, from 2007 to 2008. He has also worked as a Research Assistant with the Institute of Theoretical Information Technology, RWTH Aachen University, Germany, from 2008 to 2010. He is currently affiliated with the Department of Electrical Engineering, King Khalid University, Abha, Saudi Arabia, as a Lecturer. His research interests include machine learning and deep learning methods for networks and information security in the Internet-of-Things networks.

JOHARI ABDULLAH received the bachelor's degree in computer science (networking) from Universiti Putra Malaysia, the master's degree in information technology (IT) from the Queensland University of Technology, Brisbane, Australia, and the Ph.D. degree in computing science from Newcastle University, U.K. He is currently serving as an Associate Professor with the Faculty of Computer Science and IT, UNIMAS, Sarawak. His research interests include ICT is wide and ranging from trusted systems, blockchain technology, web system design and development, system architecture, and problem-solving using tools, such as TRIZ, ICT education for children and youth through computational thinking, scratch, computer science unplugged, and open-source system and software.

KARTINAH ZEN received the Ph.D. degree in sensor network from Edith Cowan University (ECU), Australia. She is currently an Associate Professor and Dean of the Faculty of Science and Information Technology, Universiti Malaysia Sarawak (UNIMAS). She is also a Research Fellow at the Centre of Excellence for Rural Informatics and currently working on project in wireless sensor networks. Her research interests include wireless sensor networks data transmission and sensor-related network technology and application.

IRSHAD AHMED ABBASI (Member, IEEE) received the Ph.D. degree in computer science from Universiti Malaysia Sarawak, Malaysia, and the M.S. degree in computer science from COMSATS University, Pakistan. He worked as a Senior Lecturer at King Khalid University, Saudi Arabia, from 2011 to 2015. He is currently working as an Assistant Professor with the Computer Science Department, University of Bisha, Saudi Arabia. He has over 12 years of research and teaching experience. He is the author of many articles published in top quality journals. He was declared as the Best Teacher at the Faculty of Science and Arts Belqarn, University of Bisha, in 2016. His research interests include VANETs, MANETs, FANETs, mobile computing, the IoT, cloud computing, cybersecurity, soft computing, and drone security and authentication. He has received multiple awards, scholarships, and research grants. He is serving as an editor. He is also acting as a reviewer for many well reputed peer-reviewed international journals and conferences.

NAYEEM AHMAD KHAN received the Ph.D. degree in computer science from University Malaysia Sarawak, in 2018. He is currently working as an Assistant Professor with the Faculty of Computer Science and Information Technology, Al Baha University, Al Baha, Saudi Arabia. He is an expert on attacks on critical infrastructures and has led many research projects. His research has been published in several reputed international journals and he has presented his research findings at many international conferences. He has several patents to his name. His research interests include cybersecurity, cyber intelligence and analysis, unmanned aerial vehicles, deep learning, and the Internet of Things. He has won many awards, fellowships, grants, and appreciations for his work and has written a remarkable book on malicious JavaScript attack detection using machine learning. He has been a reviewer of many high impact journals and has been the chair and the co-chair for many conferences and technical sessions.

• • •