Multi-level authentication protocol for enabling secure communication in IoT

Khushal Singh (khushals632@gmail.com)
Guru Gobind singh indraprastha university
Nanhay Singh
Ambedkar institut of advanced communication technologies and research

Research Article

Keywords: IoT, authentication, Elliptic Curve Cryptography (ECC), chebyshev polynomial, Security

Posted Date: July 2nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-382412/v1

Multi-level authentication protocol for enabling secure communication in IoT

[1]Khushal Singh and [2]Nanhay Singh

[1]Research Scholar

Research Scholar in Guru Gobind Singh Indraprastha University

khushals632@gmail.com

[2]Associate Professor

Ambedkar Institute of Advanced Communication Technologies And

Research, Geeta Colony, Delhi.

Abstract: Internet of Things (IoT) is the domain of interest for the researchers at the present with the exponential growth in technology. Security in IoT is a prime factor, which highlights the need for authentication to tackle various attackers and hackers. Authentication is the process that uniquely identifies the incoming user and this paper develops an authentication protocol based on the chebyshev polynomial, hashing function, session password, and Encryption. The proposed authentication protocol is named as, proposed Elliptic, chebyshev, Session password, and Hash function (ECSH)-based multilevel authentication**.** For authenticating the incoming user, there are two phases, registration and authentication. In the registration phase, the user is registered with the server and Authentication center (AC), and the authentication follows, which is an eight-step criterion. The authentication is duly based on the scale factor of the user and server, session password, and verification messages. The authentication at the eight levels assures the security against various types of attacks and renders secure communication in IoT with minimal communication overhead and packet-loss. The performance of the method is analyzed using black-hole and Denial-of-service

(DOS) attacks with 50 and 100 nodes in the simulation environment. The proposed ECSH-based multilevel authentication acquired the maximal detection rate, PDR, and QOS of 15.2%, 35.7895%, and 26.4623%, respectively in the presence of 50 nodes and DOS attacks, whereas the minimal delay of 135.922 ms is acquired in the presence of 100 nodes and DOS attacks.

Keywords: IoT, authentication**,** Elliptic Curve Cryptography (ECC), chebyshev polynomial, Security

1. Introduction

IoT is a interconnection of static or mobile devices provided with sensors, communication, and actuator modules linked via Internet [9][15]. IoT symbolizes vast application, supported with heterogeneous technologies and the emerging hypothesis of the interconnectedness among the devices among the physical surroundings, with the assistance of TCP/IP protocols [10] [12]. Additionally, the evolution of IoT improved the implementation process associated with the networked smart homes. Thus, the rapid evolution of IoT pushes the humans with a quality life and assures efficiency at work. IoT is a creative concept that links various things, which holds two meanings. One among the two is regarding the network nature of the core and IoT foundation, which stands as an extension and expansion for Internet. Secondly, the end users are connected with any other objects with the motive to exchange the information. As a result of sensing and communication capability of wireless, the IoT applications are rendering broad prospects. Wireless Sensor Networks (WSN) is one among the representative members of IoT, as it serves many domains, like measuring the environmental parameters including the light, pressure, temperature, humidity, and so on [13]. IoT applications find their wide range applications in economy, beginning from agriculture, water grids, building

and automation of management, systems with industrial smart grids, and smart cities. Such kind of networks uses energy-constrained sensors, which store and compute even when the communication happens over the lossy channels. In IoT, one of the basic driving forces includes networking and specifically routing that facilitates the interconnection between devices. Some of the considerations in IoT routing includes: autonomy, energy efficiency, scalability, and secure communication [11][12]. However, the uniqueness of IoT cause the networks susceptible to vulnerable attacks, which makes routing and security for data communication as hot topics in IoT research [12].

The area of concentration in IoT is about the security in the network and quality of services (QoS) during communication [14]. IoT security undergoes in-depth research as there is a necessity to secure the networks from attacks [12] and Trust-based approaches in IOT ensure secure routing functionality. On the other hand, reputation is established through the historical behaviour of the node and reveals the cooperativeness. When reputation is used in secure routing, it engages in evaluating the routing and forwarding through the application of authentication schemes along with encryption, and facilitates the effective transmission of acknowledgements while packet transmission. Trust [16] refers to the degree of confidence a node have on the neighboring nodes, which is the concatenation of all reputation measures, an entity possess for another entity. It is trustworthy to note that the higher values of reputation specify trustworthiness. Legitimate nodes mainly focus on the trustworthy entities for accomplishing the communication tasks. There are many trust-based systems employed to establish secure routing, each of which are evaluated under specific ad hoc applications and is capable of fighting the security threats [17]. Thus, assuring security in IoT system forms the basic requirement in Trust Management Mechanism (TMM), which verifies the individual request of service based on the security policy. TMM possesses numerous components, like secure routing, authorization, authentication, and so on [15]. The rule-based security schemes

never afford effective performance in the ever-changing traffic behaviours, as IoT interactions corresponds to higher complexity, which push the network to rise as the key point for establishing the security policies. On the other hand, network-based security mechanism offer effective security in the deployed IoT, enhances the Machine-to-Machine (M2M) communication, boost the diversity in the device hardware along with the interoperability constraints [14].

Authentication assures security in IoT through which a device/user verifies the data send from another device/user. Therefore, authentication forms the first initiative for faciliating a session once the IoT device is booted securely [4]. Authentication in IoT includes three entities: edge-device, end-device, and control center. In case of the IoT, end-devices perform under various tasks and contexts. For instance, in a smart home, the sensor or one particular thermal detector used may correspond to a home; a network specifically vehicular network, or a patrol car may correspond to a police station, and so on [7]. The authentication protocols are in such a way that they are resistive to malicious attacks and they are lightweight for deploying as end devices in WSN [18]. Routing protocol and Constrained application protocol (CoAP) for low-power and lossy networks (RPL) are available in the application and network layers in constrained IoT networks [19]. Some of the low-power applications include the physical and MAC layers as per the 802.15.4 protocol. An authentication protocol based on the certificate is employed for the distributed IoT systems [18] [4]. However, the edge node carries the cryptographic credentials, which is exposed to the cloning attacks.

The primary intention of the research is to design and develop a multi-level authentication protocol to improve the performance of IoT network through secure framework. The overall procedure of the authentication approach is given as follows: The authentication is considered in each transmission for avoiding different attacks by proposing a mutual authentication approach during each transmission in IoT. The profile of every user is maintained at IoT

server. The profile comprises of ID of the user and various attributes related to Anti-virus capabilities, IDS capabilities, and so on. Then, the information obtained from the last transmission is used to determine failure or success and stores in the threat profile. The profiles can be enhanced in a dynamic manner for each transmission of information, and the authentication is performed using these security attributes. Here, the mutual authentication is performed using Elliptic Curve Cryptography (ECC), chebyshev polynomial, session passwords, hashing operation, and so on, and is effectively integrated in the proposed authentication protocol to do the secure communication in IoT. The multi-level authentication is done based on the importance of the data request. Then, the various messages, and different levels of verification is carried out for authenticating IoT users for ensuing the security against various attacks. Through the secure authentication, the performance of the IoT network is improved by delivering the packets properly without any delay and drop.

The major contribution of the research is given as:

Proposed ECSH-multi-authentication protocol: The authentication of the IoT devices is enabled using the proposed ECSH-based multi-level authentication, which possess eight-level authentication steps. Whenever a new user enters the network for communication, the user is necessary to get registered with the authentication center and necessary to get authenticated in order to afford the security of the network.

The rest of the paper is structured as: the motivation in section 2 highlights the need for proposing a new method for affording security in the network. The proposed authentication scheme is deliberated in section 3 and the results of the method are presented in section 4. Finally, the summary of the research is organized in section 5.

2. Motivation

In this section, the need for the research is presented through the survey of the existing methods with the merits and demerits of the methods. The section finally lists the challenges of the research.

2.1 Literature Survey

The review of the eight existing methods is given in this section. Jie Yuan and Xiaoyong Li [1] modelled a reliable and lightweight trust strategy, which enhanced the efficiency of the system and minimized the global convergence time. The drawback of the method was that the method failed to implement various other IoT computing systems. Mohammad Wazid *et al.*[2] developed a User Authenticated Key Management Protocol (UAKMP) that rendered higher security with minimal computational cost. The method failed considering the cluster heads, sensing nodes, and the Gateway Node (GWN) in the environment. Yanbing Liu *et al.*[3] developed a data transfer security model Middlebox-Guard (M-G) based on the Software-Defined Networking (SDN), which rendered high security performance. The method never used the sequences with loops for proper policy traversal, both under overload and failure conditions. Muhammad Naveed Aman *et al.*[4] used the mutual authentication and key exchange protocol that rendered minimal energy and energy requirements with high communication overhead. However, the method suffered from minimal storage space. Amjad Ali Alamr *et al.*[5] developed the authentication protocol using the Elliptic Curve cryptography(ECC), which seemed to be highly efficient and required minimal time. The method failed considering the reader to authenticate the tag to avoid cloned tag. Xiong Li *et al.* [6] used the Anonymity authentication protocol in the industrial IoT, which minimized the computational efficiency. The method suffered from unknown key share attack and stolen smart card attack. Zhiwei Wang [7] developed an authentication protocol, which was

Efficient and feasible and it was effective, which was difficult to choose an appropriate trade-off between security and privacy. Ruhul Amin *et al.* [8] developed a Light Weight Authentication Protocol, which was better in terms of computation, storage, and communication cost. The method failed to use password verifier table to update password and identity to legal user.

2.1. Challenges

The challenges of the research are given below:

- The main challenge in IoT is regarding the dynamic dataflow as the total users and volume of dataflow varies over time. However, most of the existing dataflow control methods assume themselves as a stable network. Thus, such methods are not actively considered for network security. When data streams are crowded in the IoT, the entire network may be paralyzed [3].
- WSNs contribute much in the Industrial Internet of Things (IIoT), and employed widely in industrial fields for collecting the data to monitor an area. However, the openness of wireless channel along with the resource-constrained nature of the sensor nodes raises a question regarding the acceptance guarantee in the nodes, how to prevail the system of permitting only the valid user to access the data, which is a hectic challenge in IoT [6].
- The other two basic challenges in IoT security include heterogeneity and scalability. On the contrary, the traditional devices are resource-constrained [20].
- Edge computing services in IoT suffer from a serious challenge of how to afford trustworthiness of IoT devices [1].
- In [3], network latency is minimized using the SDN-based data transfer security model and Middlebox-Guard (M-G). Even the security performance of the methods was

found to be better, but SDN is susceptible to new network attacks, causing the malfunctioning of the IoT device.

3. Proposed ECSH Authentication Protocol For Secure Communication In Iot

Authentication is the basic mechanism in IoT that assures the recognition of the user through enabling the secure communication throughout its lifetime, which insists that the unexpected behaviour is blocked for the lifetime. In case of the unusual malfunctions of the user, the administrator revokes the previleges. Thus, knowing the significance of affording security in IoT for enabling the secure communication, this paper introduces an effective authentication scheme. The authentication protocol developed in the research involves two major phases, including registration and authentication phase. In the first phase, all the IoT devices are registered under the IoT servers, which are registered under AC. In the authentication phase, there is a multi-level authentication to authenticate the IoT devices and servers with the AC. One can say that the details of the IoT device are maintained in the IoT server along with the information of the successful transactions or failed transactions of the device in IoT. However, the transaction details are updated even now and then dynamically. Moreover, the mutual authentication is performed using the operations, such as hashing function, chebyshev polynomial, session passwords, and so on. More significantly, the level of the verification in the authentication phase provides the existence of the device against various types of the network attacks thereby, enabling the communication in IoT without any communication delay or drop in packets. The symbols employed in the proposed protocol are demonstrated in Table 1.

Table1. Description of the symbols

Symbols	Description

P_k	Public key
P_u	Private key of user
P_s	Private key of server
P_A	Private key of the IoT device
W_u	password of the user
W_s	password of the server
S_u	session password of the user
S_s	session password of the server
C_u	chebyshev polynomial dependent user factor
C_s	chebyshev polynomial dependent server factor
U_u	user name of the user
U_s	user name of the server
I_1, I_2, I_3	Intermediate messages
R	Random number
$\Re$	Indicates the message/identityreceived
$+$	Indicates the message/identity stored
c	Indicates the computed message
$E_c(\ )$	ECC encryption
$h(.)$	Hashing function
$\oplus$	XOR function
$.\|\|$	Concatenation representation

3.1 Registration phase

As the initiation of the authentication protocol, the IoT devices and the servers are necessarily to be registered for which initially all the IoT devices are registered with the IoT servers, which is registered with the AC. In other words, any new device approaching to communicate in IoT is necessarily to be registered under the AC, which indicates the secure communication in IoT. The devices that are not registered ever continues communication in IoT. Thus, there are two entities playing a prominent role during registration, which includes the IoT servers and AC. Therefore, in the registration phase, there are two phases Server registration and device registration. Figure 1 depicts the registration phase in IoT.

3.1.1 IoT device registration: The registration of the IoT device is continued between the IoT device and the IoT server in which initially, the IoT device forwards the identity U_u and password W_u of the IoT device to the server such that the server saves the user name and password of the IoT device as, U_u^+ and W_u^+. Thus, it is well known that the identity of the IoT device is available in the server, which is employed for computing the messages F_a and F_b. The intermediate message F_a is computed using the public key and private key of the server, which are applied to the hashing function individually and concatenated, followed with the modulo operation with the random number as is shown in equation (1). Likewise, the intermediate message F_b is computed using the message F_a and random number as in equation (2) and (3).

$$F_a = h(P_s) \| h(P_k) \bmod R \tag{1}$$

$$F_b = split(F_a) \tag{2}$$

$$Split(.) = \frac{F_a}{R} \quad F_b \tag{3}$$

Once the intermediate messages are computed in the IoT server, it is forwarded to the IoT device trying to register with the server. Thus, the saved intermediate messages in the IoT device are notated $F_a^{\Re}$ and $F_b^{\Re}$. A the same time, the verification message F_c is computed at the user as,

$$F_c = F_b^{\Re} . R \tag{4}$$

$$F_C^c = F_b . R = \left(\frac{F_a}{R} \right) (R) \tag{5}$$

Likewise, the verification message F_C^c is computed in the server simultaneously and the verification messages of the IoT device and the IoT server is matched. If both the verification

messages are same then, the registration of the IoT device with the server terminates. Once the registration of the device with the server is successful, the authentication progresses.

$$F_c^{\Re} == F_c^C \tag{6}$$

Thus, once the registration terminates, the private key of the user and the chebyshov polynomial based user factor is derived in the server, which is forwarded to the user and saved in the user-side. The private key is generated through concatenating the hashing function of the private key of the server and verification message F_c followed with the modulo operation with the user factor, which is given as the 4th degree polynomial.

$$P_u = h(P_s) \| h(F_c) \bmod C_u \tag{7}$$

$$C_u = 8x^4 - 8x^2 + 1 \tag{8}$$

$$x = F_b \bmod R \tag{9}$$

The private key of the device generated in the server is saved in the device along with the user factor for the further processes associated with the authentication.

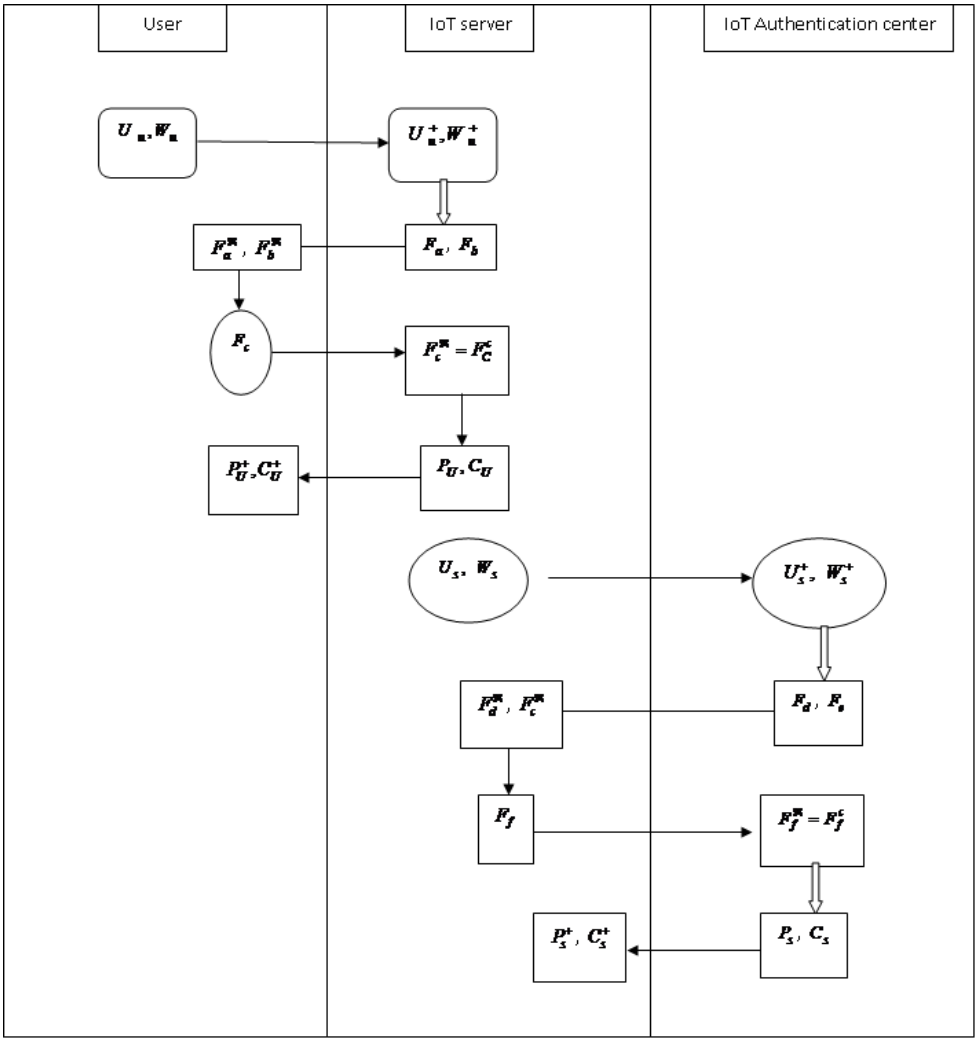


Figure1. Registration phase

3.1.2 Server registration: Prior to the registration of the device with the server, it is essential that the server is registered under the AC. For registering the server, the identity of the server is forwarded to the AC, which is stored in the AC for the generation of the intermediate messages F_d and F_e that are forwarded to the IoT server for the generation of the verification message F_f. The computation of F_d, F_e, and F_f are similar to the intermediate messages F_a, F_b, and F_c, and these intermediate messages are computed using the private key of the AC, respectively. F_f referred as the verification message and is generated in the server, which is matched with the verification message generated in AC F_f^c. Whenever the verification

messages of the server and AC matches, the verification is completed. Finally, the private key of the server P_s is generated in the AC, which is forwarded to the server and stored. Along with the generation of the private key of the server, the chebyshev polynomial dependent scale factor is generated in the AC and stored in IoT server.

The private key of the server is computed through concatenating the hashing function of private key of the IoT AC and verification message F_f followed with the modulo operation with the server factor that is a third-order polynomial. The calculations follow:

$$P_s = h(P_A) \| h(F_f) \bmod C_s \tag{10}$$

$$C_s = 8y^3 - 4y \tag{11}$$

where, y^3 specifies the third chebyshev polynomial of second kind.

$$y = F_e \bmod R \tag{12}$$

The intermediate message is computed using the public key and private key of the AC as,

$$F_d = E(P_A) \| h(P_k) \bmod R \tag{13}$$

where, $\mathrm{P_k}$ refers to the public key and P_U indicates the private key used. P_s is the private key of server and P_A is the private key of IoT.

$$F_e = Splis(F_d) \tag{14}$$

$$F_e = \left(\frac{F_d}{R} \right) \tag{15}$$

$$F_f = F_e^{\Re} . R \tag{16}$$

$$F_f^c = F_e . R \tag{17}$$

$$F_f^c = \left(\frac{F_d}{R} \right) . R \tag{18}$$

$$F_f^{\Re} == F_f^c \tag{19}$$

The equations from (14)-(19) specify the computation steps of the verification messages in the IoT AC. In short, the IoT device registers itself with the registered IoT server, which is the initiation of the secure communication without any delay or drop.

3.2 Authentication phase in IoT:

Once the IoT device registration terminates, the authentication is performed to continue the communication. The authentication protocol developed in this section carries multiple levels of confirmation based on the session password, ECC, and the private keys of server and device. Thus, there are eight level of authentication, which symbolizes the protection against various attacks.

3.2.1 Authentication level-1 and level-2: The first and second level of authentication occurs in the server between the user and the server for which the intermediate message and the factor x_c, are computed in the IoT device as,

$$I_1 = \left[h\left(P_U^+\right) \| E\left(U_u\right)\right] \oplus F_c \tag{20}$$

It is well known from the equation (20) that the intermediate message I_1 is computed through EXORing the computed verification message with the concatenated result of the encrypted username of the device and the hashed password of the device. Additionally, the factor x^c is computed using received intermediate message from the server $F_b^{\Re}$. Then, the intermediate message I_1 and factor x^c computed in the IoT device are forwarded to the server, where the intermediate message is computed for first level verification for which the private key of the user and saved user name of the user are interpreted as,

$$I_1^c = \left[h\left(P_U\right) \| E\left(U_u^+\right)\right] \oplus F_c^C \tag{21}$$

ECC enables decoding only by the trusted individuals and it is a factor for enabling security in IoT through the private keys and more importantly, the key size rendered is less. Once the intermediate message and the factor are same, the authentication level-1 terminates.

$$I_c^{\Re} == I_1^c \tag{22}$$

Likewise, the chebyshev polynomial dependent user factor is computed in server and compared with the user factor at the IoT device for marking the termination of level-2 authentication in the server.

$$x^c = F_b^{\Re} \bmod R \tag{23}$$

$$C_u^c = 8x^{\Re^4} + 8x^{\Re^2} + 1 \tag{24}$$

$$C_u^c == C_u \tag{25}$$

Equation (25) presents the termination of level-2 authentication.

3.2.2 Authentication level-3 and level-4: The third and the fourth level of authentications occur in the AC through the verification of the intermediate message I_2 and chebyshev polynomial-based scale factor. Initially, the intermediate message is generated in the server through three operations, EXOR, Encryption, and Hash function. The private key of the server stored in the server and the encrypted username of the server are concatenated and the concatenated result is subjected to the hashing function, which is finally EXORed with the message F_f as,

$$I_2 = h\left(P_s^+ \left\| E\left(U_s\right)\right.\right) \oplus F_f \tag{26}$$

At the same time, the intermediate message is computed in the AC for matching with the message in the server. The saved user name of the server is encrypted and concatenated with the private key of the server and the entire term is hashed followed with EXORing the hashed term with the computed message F_f^c as,

$$I_2^c = h\left(P_s \left\| E\left(U_s^+\right)\right.\right) \oplus F_f^c \tag{27}$$

$$I_2^{\Re} == I_2^c \tag{28}$$

Equation (28) defines the verification of the intermediate messages at the AC, if both the messages are same, the third level verification terminates. As the mark of the fourth level verification, the factor y^c is calculated in the server using the received message and random number as,

$$y^c = F_d^{\Re} \bmod R \tag{29}$$

Then, the chebyshev polynomial is computed as,

$$C_s^c = 8y^{\Re^3} - 4\,y^{\Re} \tag{30}$$

$$C_s^c == C_s \tag{31}$$

Equation (31) specifies the authentication level-4. C_s^c is computed in the AC and C_s is measured in the server.

3.2.3 Authentication level-5 and level-6: The level-5 and level-6 authentication steps are based on the intermediate message I_3 and session password of the server and these two levels of authentication occur in the server. If the session password generated in the AC is same as that of the received session password then, it marks the termination of the level-5 authentication. The session password is EXORed with the hashing function of the concatenated value of the saved user name and password of server to generate the intermediate message I_3. For level-5 verification, the factor X_1 is compared with the received session password and if the comparison is true, the verification is successful.

$$I_3 = h\left(U_s^+ \left\| W_s^+\right.\right) \oplus S_s \tag{32}$$

$$X_1 == S_s^{\Re} \tag{33}$$

Likewise, the message Y_1 is computed through EXORing the received intermediate message I_3 and hashing function of the identity of the server as,

$$Y_1 = I_3^{\Re} \oplus h\left(U_s \| W_s\right) \tag{34}$$

where, W_s refers to the password of the server and W_u refers to the password of the user. If the messages Y_1 and X_1 are same, the verification level-6 terminates and the levels-5 and 6 occurs in the server.

$$Y_1 == X_1 \tag{35}$$

3.3.4 Authentication levels-7 and 8: For the initiation of the level-7 and level-8 authentication, the intermediate message I_4 and the session password of the user S_u are computed in the server. Then, the session password and intermediate message are forwarded to the IoT device/user for authentication at the last levels. The intermediate message is computed using the application of the hashing function and EXOR function using the saved identity of the device and the session password in the server as,

$$I_4 = h\left(U_u^+ \| W_u^+\right) \oplus S_u \tag{36}$$

$$X_2 = S_u^{\Re} \tag{37}$$

Equation (37) reminds the authentication level-7, where the session password from the server is forwarded to the user and compared with X_2. On the other hand, the message Y_2 is computed using the received intermediate message, which is EXORed with the hashing function of the identity of the user (concatenated user name and password). Thus, equation (39) marks the authentication level-8.

$$Y_2 = I_4^{\Re} \oplus h\left(U_u \| W_u\right) \tag{38}$$

$$Y_2 == X_2 \tag{39}$$

All the above steps specify the authentication levels for verifying the user against various attacks. By doing so, the security for the user communication is assured. Figure 2 demonstrates the eight levels of authentication.

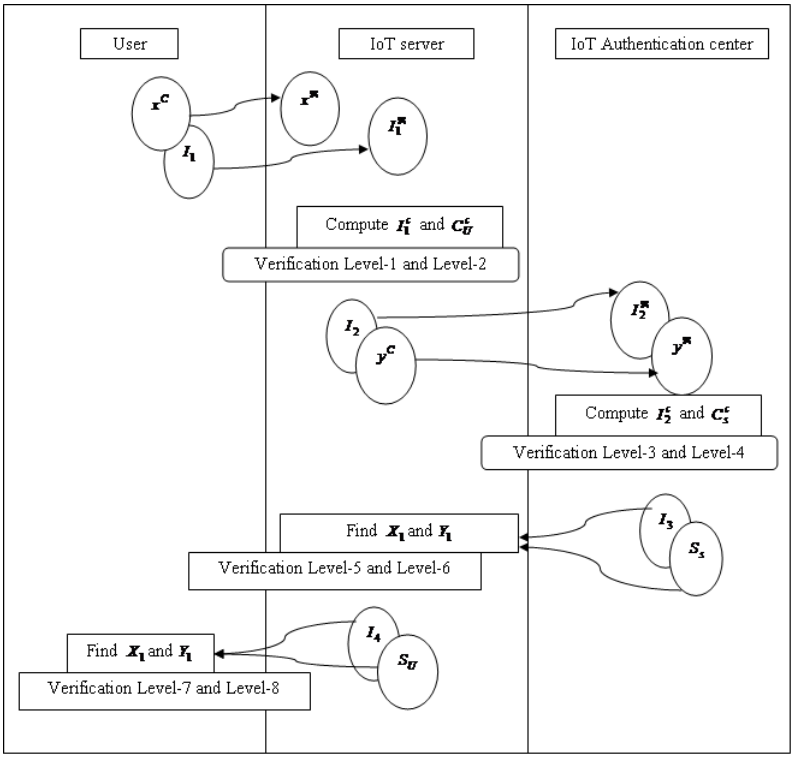


Figure2. Authentication phase

3.3 RPL routing in IoT

Once the IoT device is registered and authenticated, it commits itself in the communication for which the RPL strategy is used. The communication delay and the packet loss associated with the communication is reduced through enabling higher throughput/bit rates. The computational complexity is less with minimal message overhead.

4. Results and Discussion

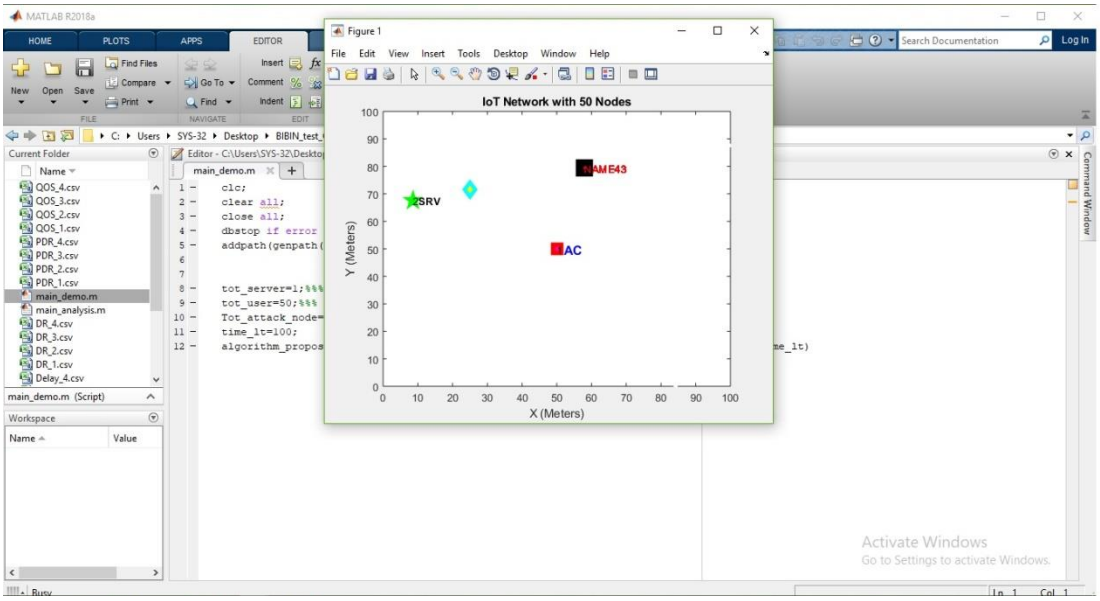
The results and discussion of the methods is deliberated in this section and the end of the section reveals the comparative analysis of the methods in order to prove the effectiveness of the proposed authentication scheme to assure security in IoT.

4.1 Experimental setup

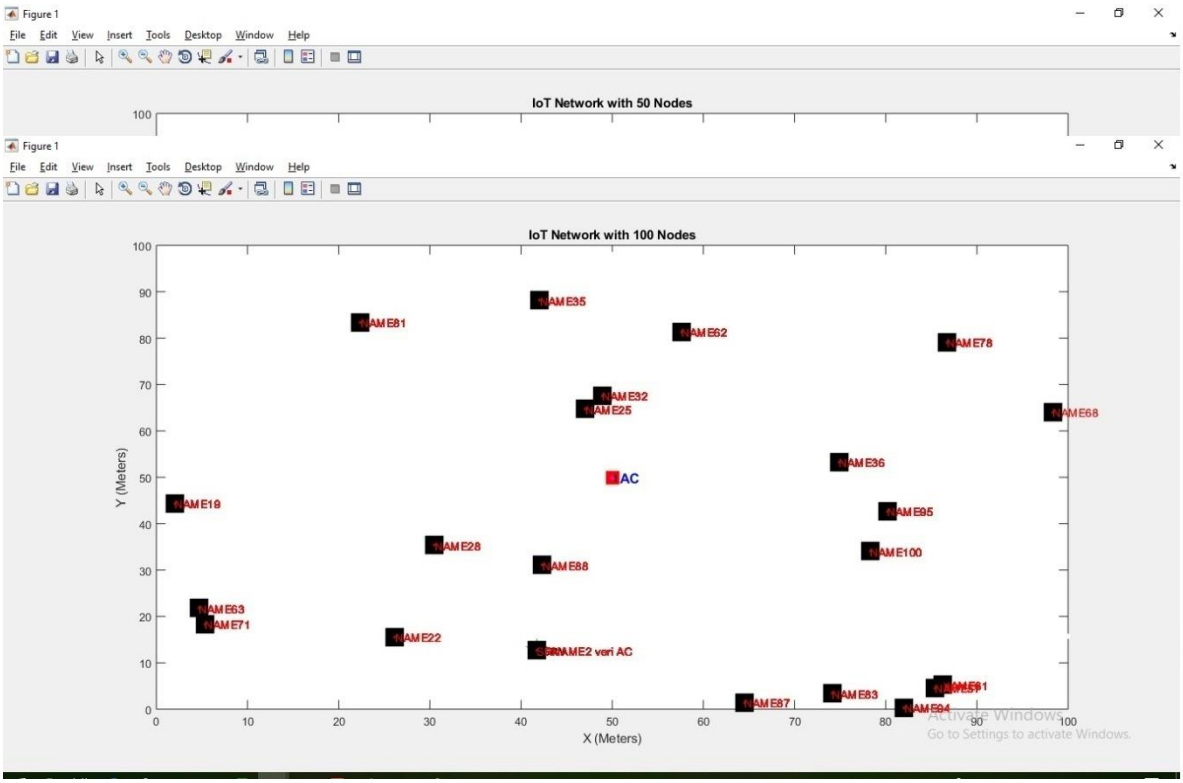
The implementation of the multilevel authentication approach is done in MATLAB and the performance is evaluated using different attacks with QoS and security parameters.

4.2 Experimental analysis

The analysis section demonstrates the simulation environment at round_0 and round_50. Figure 3 demonstrates the experimental analysis using the proposed protocol and figure 3 a) depicts the simulation at round_0. The figure 3 a) shows the simulation environment with the server and AC with a user. Likewise, figure 3 b) shows the simulation environment with multiple users with AC and server.



a)



b)

Figure3. Simulation results, a) Simulation of network at round_0, b) Simulation of network at round_50

4.3 Performance metrics

The performance of the IoT network against security attacks is evaluated based on the detection rate, whereas the performance of the IoT network is determined based on the performance parameters, QoS, Packet Delivery Ratio (PDR) and delay. The detection rate defines the rate at which the security attacks are determined using the methods and it should be higher for the effective method and is represented in %. The QoS and PDR of the methods should be greater for higher performance and is represented in %, whereas the delay of the effective method should be minimal and is represented in ms.

4.4 Competing methods

The effectiveness of the proposed ECSH multilevel authentication protocol is compared with the existing methods, Reliable and Lightweight Trust strategy (RLT) [1], User authenticated key management protocol (UAKMP) [2], and SDN-based data transfer security model, Middlebox-Guard (M-GILP) [3].

4.5 Comparative analysis

The comparative analysis of the methods are demonstrated in this section and the analysis is performed using 50 nodes and 100 nodes, respectively

4.5.1 Analysis using 50 nodes in the presence of the black-hole attacks: Figure 4 shows the analysis using 50 IoT nodes and black hole attack is considered for the analysis. Figure 4 a) depicts the analysis based on the delay with respect to the number of rounds. When the round is 20, the delay of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 81.157 ms, 73.391 ms, 65.573 ms, and 65.308 ms, respectively. It is noted that the delay of the methods increases with increasing rounds, but the ECSH-Multilevel authentication protocol acquired the minimal value of the delay. Figure 4 b) shows the analysis based on the detection rate with respect to the number of rounds. When the round is 20, the detection rate of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 61.06%, 61.06%, 67.84%, and 71.23 %, respectively. It is noted that the detection of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the detection rate. Figure 4 c) shows the analysis based on the PDR with respect to the number of rounds. When the round is 20, the PDR of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 71.9400%, 73.5443%, 74.6146%, and 83.4727%, respectively. It is noted that the PDR of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication

protocol acquired the maximal value of the PDR. Figure 4 d) shows the analysis based on the QOS with respect to the number of rounds. When the round is 20, the QOS of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 67.6054%, 68.3620%, 69.3772%, and 79.4750%, respectively. It is noted that the QOS of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the delay.

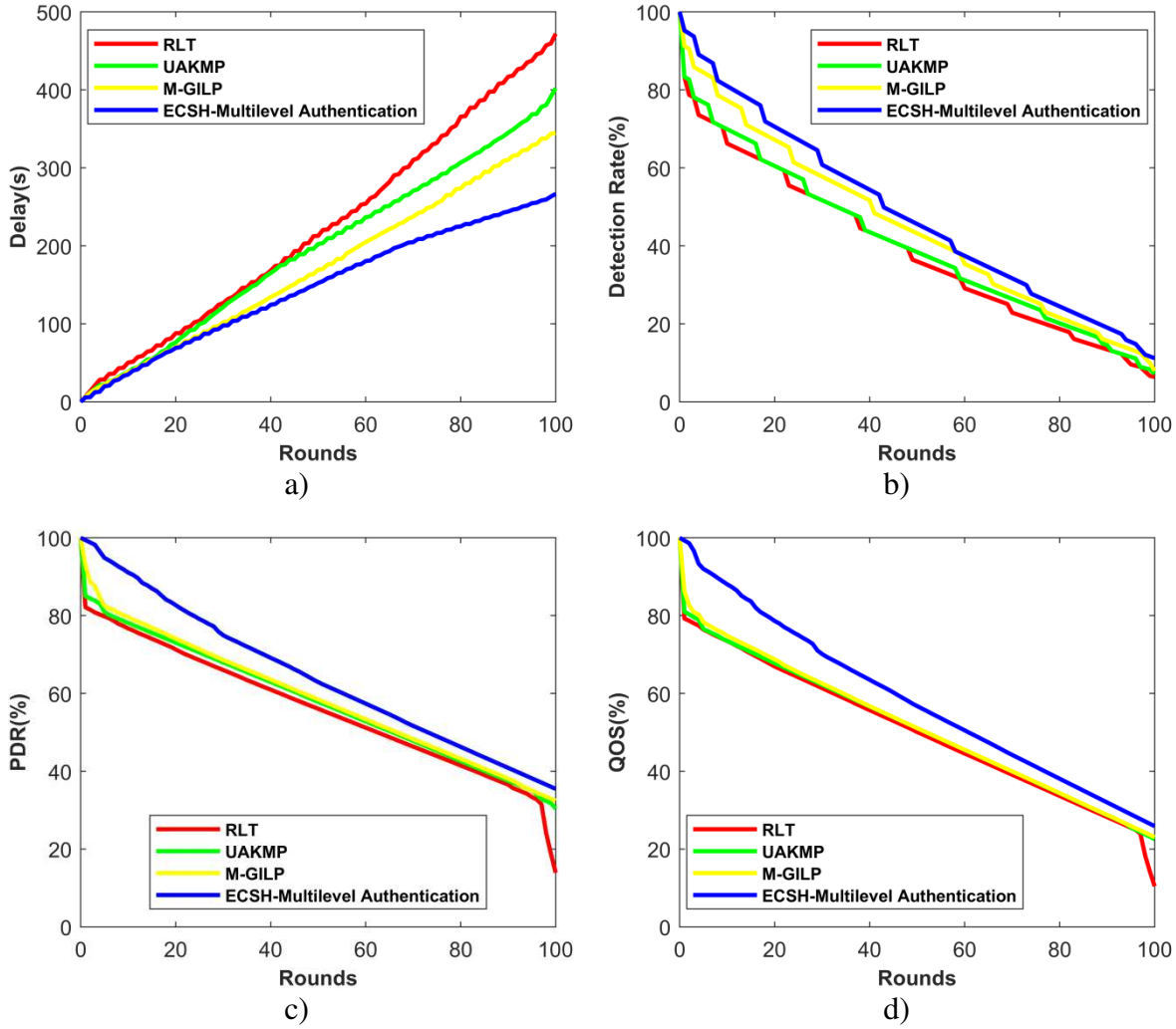


Figure4. Comparative analysis using 50 nodes in the presence of the black-hole attack, a) delay, b) detection rate, c) PDR, d) QoS

4.4.2 Analysis using 50 nodes in the presence of the DOS attacks: Figure 5 shows the analysis using 50 IoT nodes and DOS attack is considered for the analysis. Figure 5 a) shows the

analysis based on the delay with respect to the number of rounds. When the round is 20, the delay of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 107.815 ms, 86.985 ms, 71.434 ms, and 42.043 ms, respectively. It is noted that the delay of the methods increases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the minimal value of the delay. Figure 5 b) shows the analysis based on the detection rate with respect to the number of rounds. When the round is 20, the detection rate of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 54.272%, 67.840%, 74.624%, and 78.016%, respectively. It is noted that the detection rate of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the detection rate. Figure 5 c) shows the analysis based on the PDR with respect to the number of rounds. When the round is 20, the PDR of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 57.7084%, 69.8792%, 79.8773%, and 82.8909%, respectively. It is noted that the PDR of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the PDR. Figure 5 d) shows the analysis based on the QOS with respect to the number of rounds. When the round is 20, the QOS of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 50.9202%, 66.2825%, 75.2175%, and 78.3594%, respectively. It is noted that the QOS of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the delay

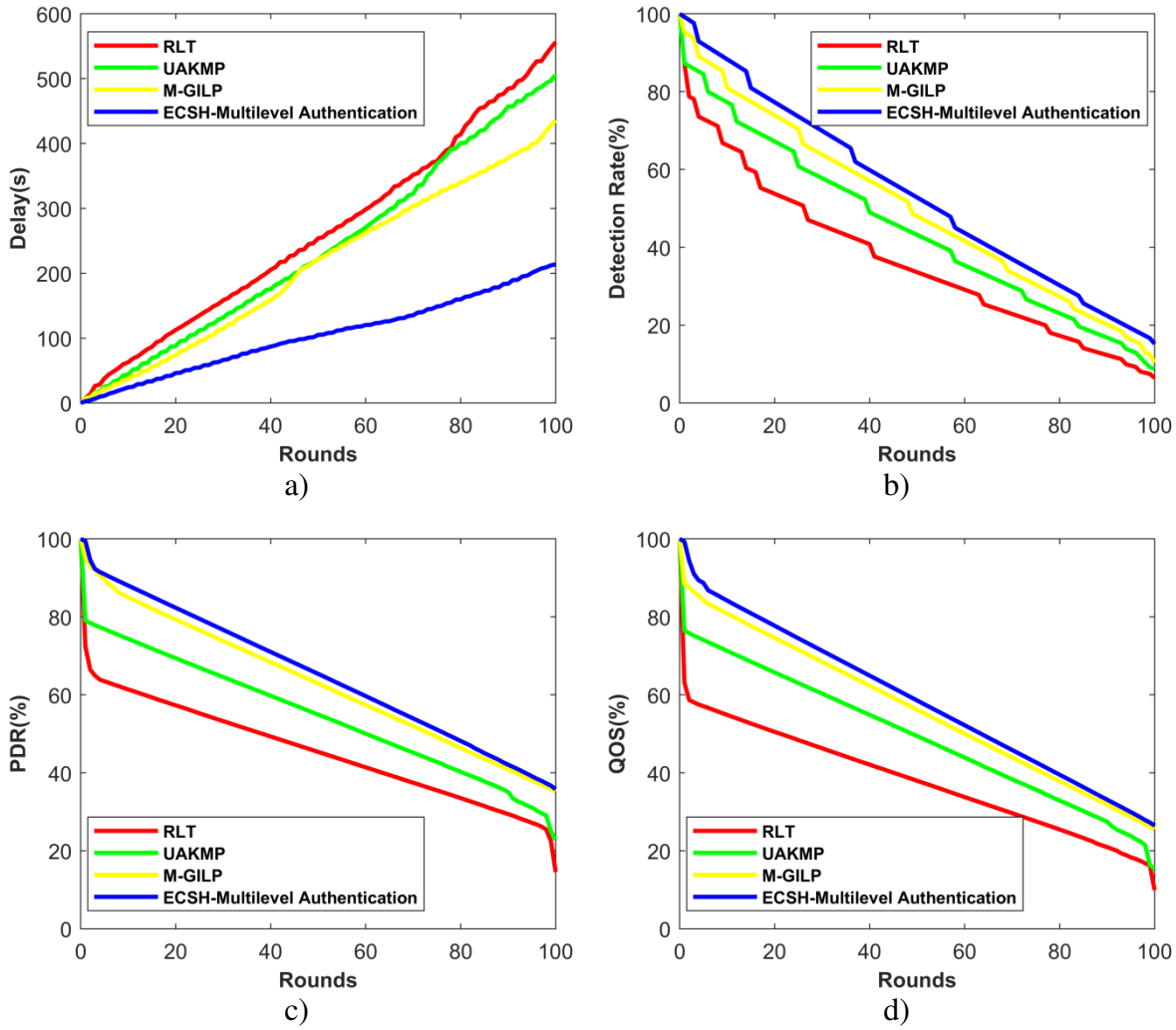
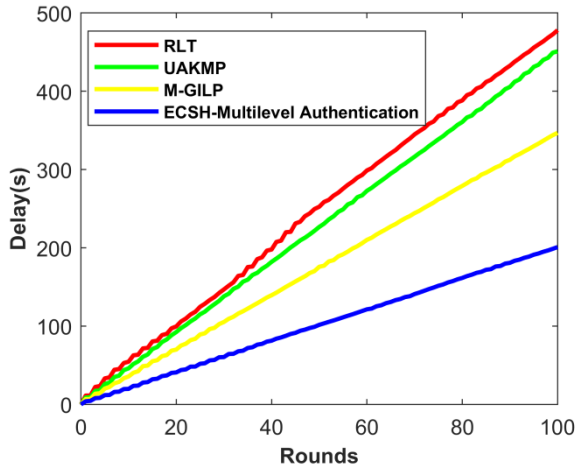


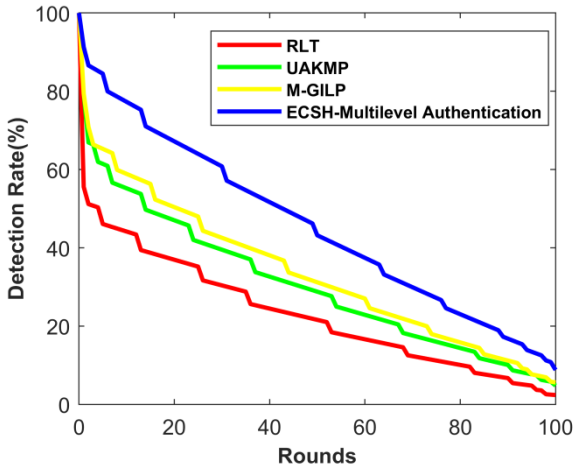
Figure5. Comparative analysis using 50 nodes in the presence of the DOS attack, a) delay, b) detection rate, c) PDR, d) QoS

4.4.3 Analysis using 100 nodes in the presence of the black-hole attacks: Figure 6 shows the analysis using 100 IoT nodes and black hole attack is considered for the analysis. Figure 6 a) shows the analysis based on the delay with respect to the number of rounds. When the round is 20, the delay of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 97.185 ms, 88.336 ms, 68.641 ms, and 40.262 ms, respectively. It is noted that the delay of the methods increases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the minimal value of the delay. Figure 6 b) shows the analysis based on the detection rate with respect to the number of rounds. When the round is

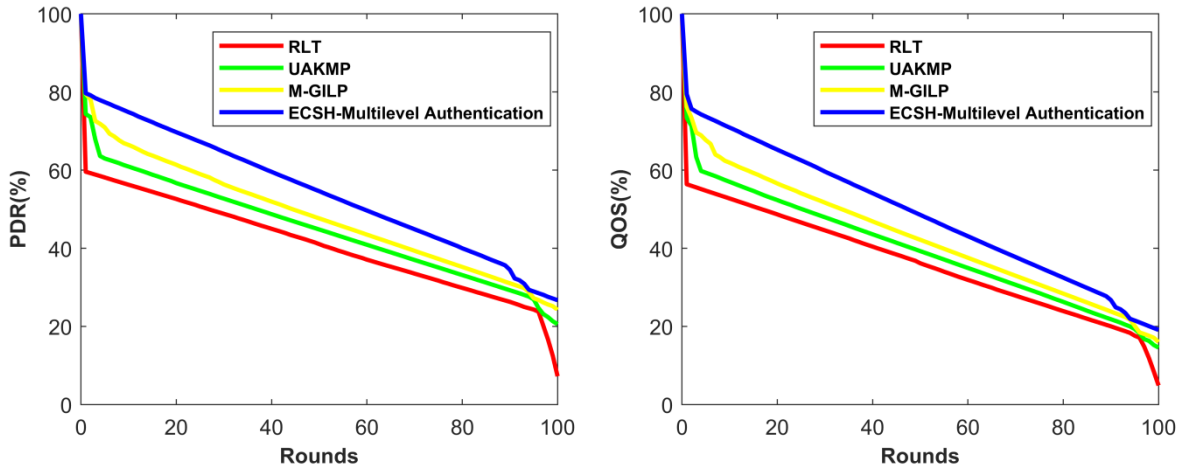
20, the detection rate of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 37.312 %, 47.488 %, 50.88 %, and 67.84%, respectively. It is noted that the detection of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the detection rate. Figure 6 c) shows the analysis based on the PDR with respect to the number of rounds. When the round is 20, the PDR of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 52.9701%, 57.1897%, 61.8392%, and 70.1976%, respectively. It is noted that the PDR of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the PDR. Figure 6 d) shows the analysis based on the QOS with respect to the number of rounds. When the round is 20, the QOS of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 49.0923%, 52.7739%, 57.1534%, and 65.7806%, respectively. It is noted that the QOS of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the delay



a)



b)



c) d)

Figure6. Comparative analysis using 100 nodes in the presence of the black-hole attack, a) delay, b) detection rate, c) PDR, d) QoS

4.4.4 Analysis using 100 nodes in the presence of the DOS attacks: Figure 7 shows the analysis using 100 IoT nodes and DOS attack is considered for the analysis. Figure 7 a) shows the analysis based on the delay with respect to the number of rounds. When the round is 20, the delay of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 115.054 ms, 104.848 ms, 88.843 ms, and 26.243 ms, respectively. It is noted that the delay of the methods increases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the minimal value of the delay. Figure 7 b) shows the analysis based on the detection rate with respect to the number of rounds. When the round is 20, the detection rate of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 50.88%, 54.272%, 57.664%, and 61.056%, respectively. It is noted that the detection of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the detection rate. Figure 7 c) shows the analysis based on the PDR with respect to the number of rounds. When the round is 20, the PDR of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 43.3940%, 57.4992%, 59.4023%, and 59.7234%, respectively. It is noted

that the PDR of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the PDR. Figure 7 d) shows the analysis based on the QOS with respect to the number of rounds. When the round is 20, the QOS of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 40.2634%, 52.4357%, 55.0467%, and 56.4846%, respectively. It is noted that the QOS of the methods decreases with the increase in the number of rounds, but the ECSH-Multilevel authentication protocol acquired the maximal value of the delay

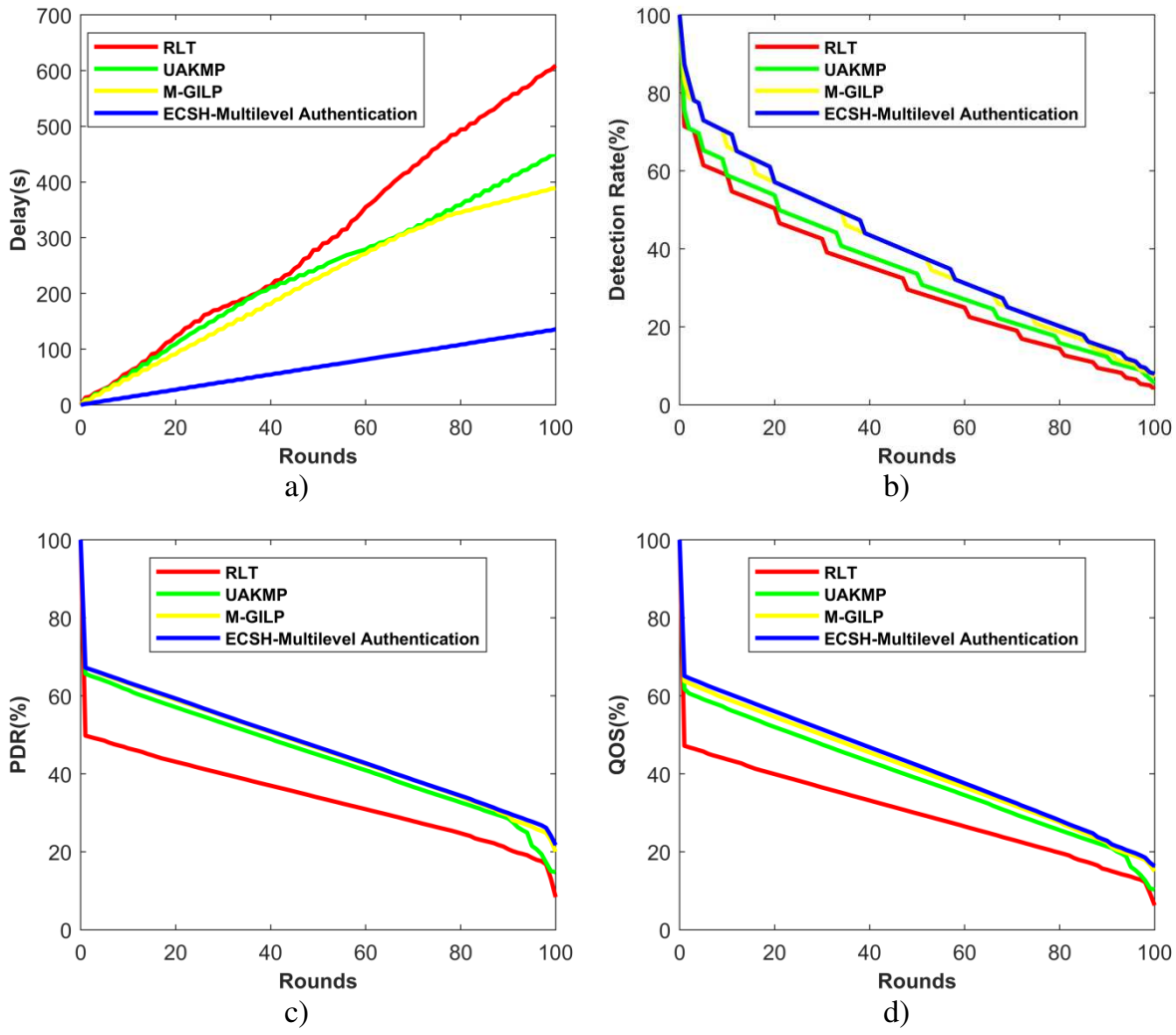


Figure7. Comparative analysis using 100 nodes in the presence of the DOS attack, a) delay, b) detection rate, c) PDR, d) QoS

4.5 Comparative discussion

Table 2 shows the comparative discussion of the methods based on the delay, PDR, detection rate, and QOS with respect to the round-100 and for two types of attacks in the presence of 50 nodes. When the round is 100, the delay of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 471.997 ms, 402.068 ms, 344.677 ms, and 266.705 ms, respectively in the presence of 50 nodes and black hole attacks. It is noted that the delay of the existing methods is higher compared with the ECSH-Multilevel authentication protocol that acquired the minimal value of the delay in ms. When the round is 100, the detection rate of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 6.4%, 7.2%, 8%, and 11.2%, respectively in the presence of 50 nodes and black hole attacks. It is noted that the detection rate of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the detection rate in percentage. When the round is 100, the PDR of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 13.9333%, 30.4000%, 32.4476 %, and 35.4779%, respectively in the presence of 50 nodes and black hole attacks. It is noted that the PDR of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the PDR in %. When the round is 100, the QOS of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 10.450 %, 22.552%, 23.077%, and 25.899%, respectively in the presence of 50 nodes and black hole attacks. It is noted that the QOS of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the QOS in %.

Similarly, the analysis of the methods using DOS attacks is demonstrated in the same table 2. When the round is 100, the delay of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 556.389ms, 506.558 ms, 435.666 ms, and 213.781 ms, respectively in the presence of 50 nodes and DOS attacks. It is noted that the delay of the existing methods is higher compared with the ECSH-Multilevel authentication protocol that

acquired the minimal value of the delay in ms. When the round is 100, the detection rate of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 6.4%, 8.8%, 10.4%, and 15.2%, respectively in the presence of 50 nodes and DOS attacks. It is noted that the detection rate of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the detection rate in percentage. When the round is 100, the PDR of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 14.5391%, 22.7778%, 35.2381%, and 35.7895%, respectively in the presence of 50 nodes and DOS attacks. It is noted that the PDR of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the PDR in %. When the round is 100, the QOS of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 9.9130%, 15.4167%, 25.5357%, and 26.4623%, respectively in the presence of 50 nodes and DOS attacks. It is noted that the QOS of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the QOS in %.

Table2. Comparative discussion of the methods in the presence of 50 nodes

50 nodes and black-hole attacks				
Methods	**RLT**	**UAKMP**	**M-GILP**	**Proposed ECSH-Multilevel authentication**
Delay (ms)	471.997	402.068	344.677	266.705
Detection rate (%)	6.4	7.2	8	11.2
PDR (%)	13.9333	30.4000	32.4476	35.4779
QOS (%)	10.450	22.552	23.077	25.899
50 nodes and DOS attacks				
Methods	**RLT**	**UAKMP**	**M-GILP**	**Proposed ECSH-Multilevel authentication**
Delay (ms)	556.389	506.558	435.666	213.781
Detection rate (%)	6.4	8.8	10.4	15.2
PDR (%)	14.5391	22.7778	35.2381	35.7895
QOS (%)	9.9130	15.4167	25.5357	26.4623

Table 3 shows the comparative discussion of the methods based on the delay, PDR, detection rate, and QOS with respect to the round-100 and for two types of attacks in the presence of 100 nodes. When the round is 100, the delay of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 477.914 ms, 450.956 ms, 346.785ms, and 200.945 ms, respectively in the presence of 100 nodes and black hole attacks. It is noted that the delay of the existing methods is higher compared with the ECSH-Multilevel authentication protocol that acquired the minimal value of the delay in ms. When the round is 100, the detection rate of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 2.4%, 4.8%, 5.6%, and 8.8%, respectively in the presence of 100 nodes and black hole attacks. It is noted that the detection rate of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the detection rate in percentage. When the round is 100, the PDR of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 7.2381%, 20.5714%, 24.2336%, and 26.7063%, respectively in the presence of 100 nodes and black hole attacks. It is noted that the PDR of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the PDR in %. When the round is 100, the QOS of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 4.8857%, 14.5714%, 15.9854%, and 19.1071%, respectively in the presence of 100 nodes and black hole attacks. It is noted that the QOS of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the QOS in %.

Similarly, the analysis of the methods using DOS attacks is demonstrated in the same table 3. When the round is 100, the delay of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 609.181 ms, 449.746 ms, 388.876 ms, and 135.922 ms, respectively in the presence of 100 nodes and DOS attacks. It is noted that the delay of the

existing methods is higher compared with the ECSH-Multilevel authentication protocol that acquired the minimal value of the delay in ms. when the round is 100, the detection rate of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 4 %, 5.6%, 7.2 %, and 8%, respectively in the presence of 100 nodes and DOS attacks. It is noted that the detection rate of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the detection rate in percentage. When the round is 100, the PDR of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 8.381%, 14.783%, 20.000%, and 21.739%, respectively in the presence of 100 nodes and DOS attacks. It is noted that the PDR of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the PDR in %. When the round is 100, the QOS of the methods RLT, UAKMP, M-GILP, and ECSH-Multilevel authentication is 6.2857%, 10.2857 %, 15.0000%, and 16.3043%, respectively in the presence of 100 nodes and DOS attacks. It is noted that the QOS of the existing methods is lower compared with the ECSH-Multilevel authentication protocol that acquired the maximal value of the QOS in %.

Table3. Comparative discussion using 100 nodes in the presence of black-hole and DOS attacks

100 nodes and black-hole attacks				
Methods	**RLT**	**UAKMP**	**M-GILP**	**Proposed ECSH-Multilevel authentication**
Delay (ms)	477.914	450.956	346.785	200.945
Detection rate (%)	2.4	4.8	5.6	8.8
PDR (%)	7.2381	20.5714	24.2336	26.7063
QOS (%)	4.8857	14.5714	15.9854	19.1071
100 nodes and DOS attacks				
Methods	**RLT**	**UAKMP**	**M-GILP**	**Proposed ECSH-Multilevel authentication**
Delay (ms)	609.181	449.746	388.876	135.922

Detection rate (%)	4	5.6	7.2	8
PDR (%)	8.381	14.783	20.000	21.739
QOS (%)	6.2857	10.2857	15.0000	16.3043

5. Conclusion

The proposed ECSH multilevel authentication protocol assures secure communication in IoT through the application of Encryption, Chebyshav, hashing function, and session passwords. The security of the IoT communication is enabled through the effective registration and authentication phases based on the security and performance factors. The analysis of the methods based on the performance metrics is performed using 50 and 100 nodes in the presence of 50 and 100 nodes. It is evident from the analysis that the proposed ECSH multilevel authentication protocol outperformed the existing methods with a minimal delay, maximal PDR, detection rate, and QOS. The minimal delay of 135.922 ms is acquired by the proposed ECSH multilevel authentication protocol when the DOS attack is available with a total of 100 nodes. On the other hand, the maximal detection rate, PDR, and QOS is acquired by the proposed ECSH multilevel authentication protocol when the simulation environment possesses 50 nodes with DOS attacks, which is 15.2%, 35.7895%, and 26.4623%, respectively. The future extension of the research is based on any of the enhanced protocols that further lower the delay and enhance the performance.

Declarations

Funding: None

Conflicts of interest/Competing interests: None

Availability of data and material: None

Code availability: None

Authors' contributions: All authors contributed to the design and implementation of the research, to the analysis of the results and to the writing of the manuscript.

References

[1] Jie Yuan and Xiaoyong Li," A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices based on Multi-source Feedback Information Fusion", IEEE Access, vol. 6, pp. 23626 – 23638, April 2018.

[2]Mohammad Wazid, Ashok Kumar Das, VangaOdelu, Neeraj Kumar, Mauro Conti, and Minho Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks", IEEE Internet of Things Journal, vol. 5 , no. 1 , pp.269 – 282, February 2018.

[3]Yanbing Liu, Yao Kuang, Yunpeng Xiao, and Guangxia Xu, "SDN-based Data Transfer Security for Internet of Things", IEEE Internet of Things Journal, vol. 5 , no. 1 , pp. 257 – 268, February 2018.

[4] Muhammad Naveed Aman, Kee Chaing Chua, and BiplabSikdar, "Mutual Authentication in IoT Systems using Physical Unclonable Functions", IEEE Internet of Things Journal, vol.4 , no.5 , pp.1327 – 1340, October 2017.

[5] Amjad Ali Alamr, Firdous Kausar, Jongsung Kim and ChanghoSeo, "A secure ECC-based RFID mutual authentication protocol for internet of things", The Journal of Supercomputing, vol.74, no. 9, pp. 4281–4294 ,September 2018.

[6]Xiong Li, JianweiNiu, Md ZakirulAlam Bhuiyan, Fan Wu, Marimuthu Karuppiah, and Saru Kumari, "A Robust ECC based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things", IEEE Transactions on Industrial Informatics,vol. 14 , no. 8 , pp. 3599 - 3609,August 2018.

[7]Zhiwei Wang, "A Privacy-Preserving and Accountable Authentication Protocol for IoT End-Devices with Weaker Identity", Future Generation Computer Systems, vol. 82, pp.342-348, May 2018.

[8]Ruhul Amin, Neeraj Kumar, G.P. Biswas , R. Iqbal and Victor Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment", Future Generation Computer Systems, vol. 78, no. 3, pp. 1005-1019, January 2018.

[9] MahaBouaziz and Abderrezak Rachedi," A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology", Computer Communications, vol. 74, pp. 3-15, January 2016.

[10] Thomas Watteyne, Antonella Molinaro,Maria Grazia Richichi and Mischa Dohler," From MANET To IETF ROLL Standardization: A Paradigm Shift in WSN Routing Protocols", IEEE Communications Surveys & Tutorials, vol. 13, no.4, pp. 688 – 707, September 2010.

[11]Terence K.L. Huia, R. Simon Sherratt and Daniel Díaz Sánchez," Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies", Future Generation Computer Systems, vol. 76, pp.358-369, November 2017.

[12] David Airehrour, Jairo A. Gutierrez and Sayan Kumar Ray, "SecTrust-RPL: A Secure Trust-Aware RPL Routing Protocol for Internet of Things", Future Generation Computer Systems, March 2018.

[13] Zheng-Yang Ai, Yu-Tong Zhou and Fei Song," A Smart Collaborative Routing Protocol for Reliable Data Diffusion in IoT Scenarios",vol.18,no.6, June 2018.

[14] Amol V. Dhumane and Rajesh S. Prasad, "Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT," Wireless Networks, pp.1-15, 2017.

[15] Seyed Mahmood Hashemi and Jingsha He, “LA-Based Approach for IoT Security,” Journal of Robotics, Networking and Artificial Life, vol.3, no. 4,pp. 240-248,March 2017.

[16]G. Hatzivasilis and C. Manifavas, “Building trust in ad hoc distributed resource-sharing networks using reputation-based systems,” In proceedings of 16th Panhellenic Conference on Informatics, October 2012.

[17] George Hatzivasilis, Ioannis Papaefstathiou and Charalampos Manifavas,” SCOTRES: Secure Routing for IoT and CPS”, IEEE Internet of Things Journal , vol. 4,no. 6, pp. 2129 – 2141,Dec. 2017.

[18]P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, “Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications,” In Proceedings of IEEE WCNC, pp. 2728- 2733, Istanbul, Turkey, April 2014.

[19] PawaniPorambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Mika Ylianttila, "PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications", International Journal of Distributed Sensor Networks, July 2014.

[20] Kubra Kalkan and Sherali Zeadally, “Securing Internet of Things (IoT) with Software Defined Networking (SDN),” IEEE Communications Magazine, pp.1-7, 2017.