ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse87842019.pdf
https://doi.org/10.30534/ijatcse/2019/87842019

Dual Server based Security Protocol in MANET using Elliptic Curve Cryptography: A Cluster Head Selection Scenario

R.Srilakshmi[1],Dr.M.Jaya Bhaskar[2]
[1]Research Scholar, KLEF Deemed to be university,India,regulasrilakshmi@gmail.com
[2]Professor, KLEF Deemed to be university,India,jayabhaskar@kluniversity.in

ABSTRACT

Mobile Ad hoc Network (MANET) is gradually emerging to be the most perspective part in the rising domain of wireless technology. However, the network security becomes more crucial since it affects the data communication between nodes and cluster head. Further, all the challenges are mostly due to the factors like lack of infrastructure, node vulnerability, and channel vulnerability. The aim of this investigation is to send the message to the respective cluster head and also to defend the transmitting message from the intruders. This paper proposes a Elliptic Curve Cryptography (ECC) based security protocol for adopting those objectives even under varying Cluster Head environs. The proposed protocol includes two phases namely Registration phase and Authentication phase. This paper contributes a new working strategy in the authentication phase by introducing two servers: Common server and Master server. In this, the common server is for doing the computing process and the master server is for validating purpose. With the adoption of these two servers, the protocol seems to be stronger with effective authentication. Finally, the attacks-based analysis and key sensitivity analysis is performed to define the effectiveness of the communication. Further, the computational time is also analyzed along with the functionality features to prove the superiority of proposed protocol in terms of security.

Key words: MANET, Security Protocol, ECC, Attacks, Master Server

1.INTRODUCTION

MANETs are the infrastructure-less, self-configuring network of mobile nodes that are linked by wireless links. Every MANET [9] [10] [11] [12] nodes are free to travel independently mostly in all directions. This would make frequent changes in their links. Nodes that present within radio range can directly do the communication process, whereas the nodes that not present in each others' radio range can do the communication through some intermediate nodes, in which the packets get relayed from source to destination. Owing to the pervasive availability of mobile devices, MANETs have been broadly utilized in different applications including defence crisis operations, disaster preparedness and response operations as well.

The utilization of MANETs is the primary criteria as it has the infrastructure-less property. At the time of data receiving, nodes also require suitable cooperation with one another for forwarding the data packets, in that way, it forms the wireless local area network [13] [14] [15] [16]. The mentioned features (forwarding data) often suffer from severe drawbacks in the view of security aspect. In fact, the abovementioned applications inflict certain stringent constriction on the security of network routing, topology, as well as data traffic. For example, the existence and association of network malicious nodes might interrupt the process of routing, which leads to a malfunctioning in network operations.

Numerous research works have been determined on MANETs security. Among them, most of the research work dealt with preclusion and detection models to fight the individual misbehaving nodes. Under this consideration, the efficiency of these models becomes worse if their present several malicious nodes that collude one another for initiating collaborative attack, and that might produce more distressing damages to the network. This is attained through manipulating the routing tables, injecting false route data or altering routes. However, attacks are the major concern and that are not yet prohibited with effective approach. In that case Man in the middle (MitM) attacks can be launched through the manipulation of routing data for passing traffic by malicious nodes. Several routing protocols have been developed for mitigating attacks against MANETs [17] [18] [19] [20], however these cause do not widen guard or protection to other data. Moreover, lagging of infrastructure that added to dynamic topology of MANETs [21] [22] [23] [24] [25] make the network more vulnerable under routing attacks like grayhole as well as blackhole (known as variants of blackhole attacks). These drawbacks of attacks in MANET must be rectified by developing some advanced intelligent models.

This paper introduces a new security protocol including two phases: (i) Registration phase and (ii) Authentication phase. In the authentication phase there has two servers: Common server and Master server. In this, the common server is to do the computing process and the master server is to do the validation process. The adoption of these two servers makes the protocol stronger with effective authentication. The rest of the paper is organized as follows: Section II reviews the literature work. Section III explains the general concept of MANET. Section IV discusses the obtained results and Section IV concludes the paper.

2.LITERATURE REVIEW

A. Related Works

In 2015, Uttam and Raja [1] have proposed a distributed dynamic address configuration approach (based on low-overhead identity) to have secure IP address allocation particularly for authorized nodes of MANET. A fresh node would get the IP address from the conventional neighbor node. After this, every network node could produce the set of distinct IP addresses from there own IP address. This could further assigned for more new nodes. As there has infrastructure lagging, rather than the issues of security, network cause various design limitations including partitioning of network, great packet error rate, and merging of network. The authors have proposed a protocol to rectify these limitations by incurring least overhead since it does not need any message flooding approach on total MANET. Finally, the simulation outcomes have reviewed that the developed algorithm has outperformed other conventional approaches.

In 2014, Jian-Ming *et al.* [2] have stated that the detection of malicious nodes that launches grayhole was the great dispute. The authors have designed a dynamic source routing (DSR)-based routing approach for resolving these issues, and it was named as cooperative bait detection scheme (CBDS). This model has integrated the benefits of both reactive and proactive defense architectures. Further, this CBDS approach has implemented a reverse tracing mechanism for helping in attaining the suggested goal. The outcomes of simulation have reviewed that the proposed CBDS was more effective when compared to other security protocols with respect to routing overhead and packet delivery ratio.

In 2014, Vijaya *et al*. [3] have analyzed the behavior and effect of JellyFish attack on TCP-related MANETs. The authors have implemented and assessed all the 3 attack variants like JF-delay, JF-reorder, as well as JF-drop through the process of simulation work. The corresponding attacks have exploited the behavior of stopped loop protocols including TCP and have disturbed the process of communication without violating the protocol rules; hence the identification process becomes more complex. Subsequently, traffic was disrupted and that leads to degradation of throughput. The simulation outcome has reviewed the performance of proposed model under EXata-Cyber simulator with respect to throughput of network, network overhead and delay. Further, direct trust-based detection (DTD) was also developed for removing the JellyFish node.

In 2016, Darren *et al.* [4] have stated that the utilization of communication security protocols that basically proposed for wireline as well as WiFi networks could show heavy burden on the restricted MANET resources. In order to resolve the issue, the authors have developed a new framework SUPERMAN. This was actually the framework that modelled for allowing the network as well as routing protocols on effective performance of their functions, along with authentication of node, node access control, and mechanism of communication security. At last, the proposed framework was compared to other conventional methods to identify the betterments in terms of suitability of network.

In 2013, Tahsin and Michel [5] have addressed the matter of delay overhead that occurred by the introduction of cryptography, which provides straight impact of the performance of video streaming. This developed model has been encouraged by the feasibilities of adaptive security along with multimedia services. The authors have made the impact of identifying when, why and how to setup the adaptation. They have developed a QaASs (QoS aware Adaptive Security approach), which was a adaptive approach that contradict the impact of delay overhead through the adaptation of cryptography properties and multimedia properties. finally, the simulation work has proven the superiority of proposed model.

In 2015, Marjan and Hamideh [6] have stated that the designing of secure routing protocol was a greatest challenging aspect. Many nature-inspired routing approaches like BeeAdHoc has been used to introduce the routing protocol of MANET. In this work, the authors have evaluated the vulnerabilities of security under BeeAdHoc and have developed a security model namely FBeeAd-Hoc, that uses the fuzzy set theory as well as digital signature. Theuy have used a toolbox TRUTIME for simulation work. Finally, the investigation outcome has revealed the performance of proposed work in terms of encounting various threats. The proposed model has attained better performance over the conventional method.

In 2016, Malik *et al.* [7] have proposed a Flooding Factor based Framework for Trust Management (F3TM) in MANETs. Here, the authors have used a True flooding model for finding the identify attacker nodes, which was on the basis of evaluation of trust value. They have developed a Route Discovery Algorithm for discovering an effective and secure path for data forwarding. This was done via Grey Wolf algorithm that has validated the network nodes. Moreover, the enhanced Multi-Swarm Optimization was utilized for optimizing the found delivery path. Finally, the simulation work has been takes place in ns2 for assessing and comparing the F3TM performance with the conventional approaches: CORMAN and PRIME in terms of packet delivery ration, delay, overhead as well as throughput.

In 2014, Saju and philip [8] have developed a self-organized key management model for MANET. The developed architecture comprises of single coordinator node, ordinary mobile nodes as well as servers. Here, the coordinator acts like mediator in message transmission between the servers as well as normal nodes. Subsequently, they have employed a multi-path certificate exchange model in which the nodes' public key was certified through manifold nodes. The nodes that subjected the certificates were evaluated through the Eigen Vector Reputation Centrality.

Table 1: Features and Challenges of different MANET security protocol

Author [citation]	Methodology	Features	Challenges
Uttam and Raja [1]	Low-overhead identity based distributed dynamic address configuration scheme	• Less addressing latency. • More robust and scalable	• Advancement is needed in removing latency. • Suffers a lot in addressing conflicts
Jian-Ming *et al.* [2]	Cooperative Bait Detection Scheme (CBDS)	• Reduces the Routing Overhead. • Packet Delivery ratio is effective	• Could not investigate the feasibility of the approach. • Integration investigation is complex.
Vijaya *et al*. [3]	DTD algorithm	• Increases the throughput • Reduces the delay	• Less accurate. • Improper overhearing
Darren *et al.* [4]	SUPERMAN	• Increases the confidentiality • Do reliable communication	• Real time implementation is difficult. • Suffers in Complex insecure environment
Tahsin and Michel [5]	Runtime adaption mechanism	• Greatly works in real time environment. • Maintains the security level.	• Problems occur in adapting multiple parameters. • Cannot solve multivariable optimization problem.
Marjan and Hamideh [6]	FBeeAdHoc	• Can counter various threats. • Improves the network performance	• Optimization is required to get optimal membership function. • Selfish node detection is complex.
Malik *et al*. [7]	Enhanced Multi-Swarm Optimization	• Identifies the malicious nodes. • More scalable	• Advancement is needed for better accuracy rate
Saju and philip [8]	Self organized Key Management technique	• Increases the confidentiality. • worth in multipath approach	• Should include the certification revocation approach

B. Review

Table I shows the features and challenges of some conventional security models in MANET. In this, Low-overhead identity based distributed dynamic address configuration scheme [1] can address only less latency and the method is highly robust and scalable. However, the model suffers a lot while addressing conflicts. CBDS [2] could minimize the routing overhead and has efficient packet delivery ratio. The problem with this model is, it could not evaluate the possibility under all fields. DTD [3] has high throughput and could minimize the delay. Yet the model has the drawback of improper overhearing with less accuracy rate. SUPERMAN [4] promises for high confidentiality and it does the reliable communication as well. However, the model is more complex in real time implementation and also it suffers a lot under insecure environment. Runtime adaption mechanism [5] highly works in real time environment with suitable environment maintenance. Yet, the adaptation of multiple parameters creates more problems. FBeeAdHoc [6] has the ability to counter many threats and enhances the performance of network. Enhanced Multi-Swarm Optimization [7] could find the malicious nodes and it is more scalable. However, advancement is required in attaining better accuracy rate. Self organized Key Management technique [8] is worth enough in multipath approach but it must include the certification revocation approach.

3.MANET ARCHITECTURE: GENERAL CONCEPT

Generally, the MANET represents the most complex distributed system, which includes various wireless mobile nodes. Figure 2 illustrates the general art of MANET. This architecture is categorized into enabling models and networking application and middleware, in which each and every category is associated to the distinct network operations. In order to adopt quick and reliable data transmission, the nodes that exist in network are trooped or grouped in to clusters. In each cluster, a CH is chosen that must receive the transmitted data from the nodes of its own cluster. Further, the MANET suffers from different security-challenges including channel liability, dynamic changes in network topology, lack of infrastructure and node liability. In case, if there obtains any changes in topology, the node transmits the data to CH that does not belong to its particular cluster. In such scenario, wrong CH tends to receive the transmitted data and moreover it receives the data that transmitted by the node belongs to its cluster. As a result, there cause congestion in the network. In contrast to this, if the transmitted data is received by the wrong cluster, it might act as the hacker that leads to security issues in network. This is what named to be node vulnerability. Also, in some cases, the channels among nodes and CH might act as hacker, which comes under the challenge of channel vulnerability.

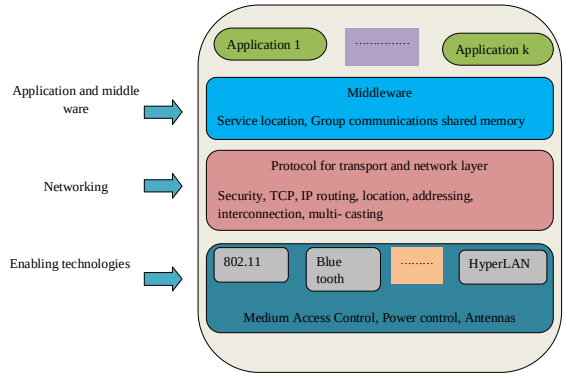

Figure 1: General Architecture of MANET

C. Public key Cryptography: ECC based security protocol

This is a public- key cryptography approach that is on the basis of algebraic structure of elliptic curves under a finite field. The most beneficiary part of this ECC is that it only requires smaller keys when compared over other general cryptographic approaches. Further, the basic ECC operation is elliptic curve scalar multiplication, elliptic curve doubling, and elliptic curve addition. Considering two points A and B, and the Algorithm 1 shows the pattern of arithmetic operations, where the scalar multiplication is dependent to elliptic curve addition as well as doubling operations. Hence, the mathematical representation of elliptic curve scalar multiplication with elliptic curve addition and doubling operations is given in Algorithm 1.

ALGORITHM 1: ELLIPTIC CURVE SCALAR MULTIPLICATION
Input: Integer $m = (1, m_{i-2}, ...m_1, ...m_0)$
Output: $B = mA$ /*Elliptic curve scalar multiplication
Initialize: $B \leftarrow A$
For $a = b - 2$ down to 0 do
$B \leftarrow 2B$ /*Elliptic curve doubling
If $m_a = 1$, then
$B \leftarrow A \oplus B$ /*Elliptic curve addition
end
End for
Return B

The mentioned ECC based protocols comprises of two major phases like registration phase and the authentication phase. In the registration phase, all the nodes make registration to their respective CH for providing proper services. Here, the determination of node's unique identity ID is done and concatenates with the hash of that ID. Further, the hashed ID is stored in smart card C_l. Hence, the phase could share the credential and generates the common credentials. Similarly, authentication phase is for accessing the resources of the service supplier.

Here, the distinct CH identity is specified as CID, and the distinctive identity of each node is indicated as ID. In this, data D with me message is transmitted from the node to the CH. Generally, the major aim of this experiment is to find whether the node in distinctive cluster is transmitting message to its CH. To make this identification, more parameters are defined, where all the needed conditions are illustrated in the protocol diagram. Initially, in the transmission section, the verifying part initiates with the evaluation of condition as determined in Eq. (1) and Eq. (2), which checks whether it gets hold or not where x_k denotes the node's public key, P indicates the ciphertext, G denotes the generator of the field, the public key of $CHRC$ is denoted by PU^{pub}, K_1 indicates the point of cryptography (ECC), K_{1x} specifies the x-coordinate of K_1 .

$$ha_1 = HA(ID_l \| CID_k \| z_k \| me_1 \| x_l \| T \| K_1) \quad (1)$$

$$ha_2 = HA(P_1 \| T \| ha_1 \| CID_k \| x_k \| z_k \| me_2) \quad (2)$$

$$x_l = v_l \oplus HA(G_l^w \| \sigma_1) \quad (3)$$

$$z_l = HA(x_l \| ID_l \| HA(G_l^w \| \sigma_1)) \quad (4)$$

$$T = jG \quad (5)$$

$$K_1 = jPU^{pub} \quad (6)$$

$$j = HA(j_l \| x_l \| me_1) \quad (7)$$

$$P_1 = E_{K_{1x}}[ID_l, CID_k, z_l, me_1] \quad (8)$$

ECC encrypts the message in node, and it is defined in Eq. (9). Eq. (10) and (11) defines E_1 and E_2 ciphertexts, where α_1 indicates the random number. In this, the E_1 arithmetic operation is associated with elliptic curve scalar multiplication and E_2 arithmetic operation is associated to elliptic curve addition.

$$P_2 = E_1 + E_2 \quad (9)$$

$$E_1 = \alpha_1 G \quad (10)$$

$$E_2 = me_2 + \alpha_1 PU^{pub} \quad (11)$$

Hence, the data that has to be transferred from the node to the corresponding CH is produced as $D = \{P_1, T, ha_1, P_2, ha_2\}$. At last, in the CH, the passed message is decrypted using ECC as in Eq. (12), where G^{pri} refers to the private key.

$$me_2 = E_2 - E_1 * G^{pri} \quad (12)$$

D. *Correctness of Protocol*

Proof 1: This proof gives the correction protocol of encryption protocol. As mentioned in the protocol, Eq. (6) specifies the K_1 representation.

$$K_1 = K_2$$

Whereas, the representation of T is defined in Eq. (5)

$$jPU^{pub} = xT$$

$$jPU^{pub} = xjG$$

$$jPU^{pub} = j(xG)$$

$$jPU^{pub} = jPU^{pub}$$

Thus proved K_1 is equivalent to K_2

Proof 2: This section explains the correction protocol of decryption process. According to Eq. (12)

Eq. (11) is the representation of N_2 and Eq. (10) shows the representation of N_1.

$$me_2 = E_2 - E_1 * G^{pri}$$

$$me_2 = me_2 + \alpha_1 PU^{pub} - \alpha_1 G * PU^{pri}$$

$$me_2 = me_2 + \alpha_1 PU^{pub} - \alpha_1 PU^{pub} \Rightarrow me_2 = me_2$$

E. Registration Phase

This phase aims in eliminating the registration of new node with the actual status of the legal node. The χ, which is the identity-verifier table that aids in matching the registration of new node with legal nodes. For example, here, the node E_l selects CID_l and send the registration request $\{CID\}_l$ to the CH registration centre $CHRC$. After receiving this, $CHRC$ verifies whether the hash value of $HA(CID_l \| x)$ matches with any of the entries in the table χ. If the hash value gets matched, then the $CHRC$ declines the request and declare the considered request as invalid. Else, $CHRC$ arbitrarily produces a number y_l and do the evaluation of authentication parameter $x_l = HA(CID_l \| x \| y_l)$. Further, $CHRC$ formulates the z_l on CID_l in correspondence with y_l that is the form $z_l = HA(CID_l \| x \| y_l \| CID_l)$ and saves $\{HA(CID_l \| x), y_l\}$ into the table χ. Finally, $CHRC$ transmits this information to the corresponding node E_l and proclaims the information that should be publically accessible to all the legal nodes. The protocol of registration phase is given in Figure 2.

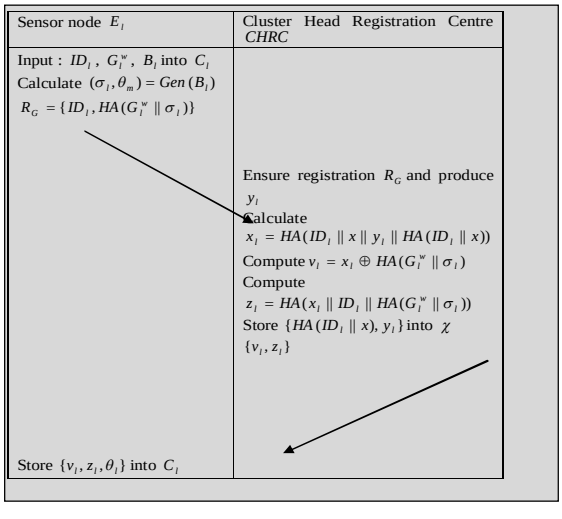

Figure 2: Registration phase protocol

Let Ec_p refers to the noun- the singular elliptic curve, where p the huge prime, Ω is the symmetric- key cryptography and i indicates the order. Let the pre-constructed smart card C_l with public parameters that is in the form $\{p, Ec_p, G, PU^{pub}, i, \Omega, HA(.)\}$. Moreover, here in this phase, the smart card is attained by each and every node. This makes possible by granting the abovementioned public parameters to E_l, and subsequently, a component of built-in fingerprint scan is embedded into the card reader. In this, the node E_l transmits the request to $CHRC$ and gain the smart card and subsequently it is makes the registration with $CHRC$. The registration phase includes some steps and that as follows:

Step 1: At first, the node E_l inserts the smart card C_l into the card reader. Then, the node's distinctive identity, password and biometric, ID_l, G_l^w, and B_l are obtained. The node E_l starts to evaluate the $(\sigma_l, \theta_m) = Gen(B_l)$, and transmits the request to register with $CHRC$.

Step 2: Subsequently, $CHRC$ verifies whether the hash value $HA(ID_l \| x)$ matches to any of the entries in χ, and all these happens after receiving the request message. Here, $CHRC$ discards the request if the hash value matches with the entries, and hence the considered node is confirmed as the invalid one. Else, $CHRC$ starts to evaluate $x_l = HA(ID_l \| x \| y_l \| HA(ID_l \| x))$,

$v_l = x_l \oplus HA(G_l^w \| \sigma_l)$, $z_l = HA(x_l \| ID_l \| HA(G_l^w \| \sigma_l))$. Subsequently, the table gets updated with new entry $\{HA(ID_l \| x), y_l\}$. The $CHRC$ transmits $\{v_l, z_l\}$ to the node E_l.

Step 3: After getting $\{v_l, z_l\}$, E_l node saves $\{v_l, z_l, \theta_l\}$ into the smart card C_l.

F. Authentication and Message Transmission Phase

This phase is the most important phase that can make reliable communication under insecure channel. Further, this paper introduces some new strategy to transmit the message with the assurance of authentication. For this, the proposed authentication protocol introduces two servers: common server and master server, which is shown in Fig 2. Both this server works on taking final decision. Here, the computing process is done by common server and the master server proceeds the validation process. The corresponding steps that are followed in this authentication phase are given below:

Step 1: After receiving the login message D_1, arbitrarily selects the nonce me_1. Subsequently, evaluate P_2, ha_2. Once the values are computed, E_l sends the message D to common server via public channel.

Step 2: Subsequently, the common server tends to evaluate the $K_2 = xT(= K_1)$ and hence defines ID_l, CID_k, z_k and me_1. These are performed by decrypting P_1 using K_{2x} where

K_{2x} indicates the x- coordinate of ECC point K_2. All the evaluated results are transmitted to master server, where it validates it.

Step 3: Master server checks the freshness of me_1 and also checks the validity of both ID_l and CID_k by verifying $HA(ID_l \| x)$ and $HA(SID_k \| x)$ respectively in χ. Nevertheless, master server terminates the sitting if those verified parameters are seemed to be valid. Else, the server recovered the y_k and y_l with respect to ID_l and CID_k from χ. The validated status is send back to common server.

Step 4: Further, the common server evaluates the $x_l = HA(ID_l \| x \| y_l \| HA(ID_l \| x))$ and $x_k = HA(SID_k \| x \| y_l)$. Then, it is send to master server.

Step 5: The master server validates whether $ha_1 = HA(ID_l \| CID_k \| z_k \| me_1 \| x_l \| T \| K_1)$ and $z_k = HA(x \| y_k \| x_k \| CID_k)$ holds or not. Further, the master server ends the session if those do not hold and if the received record (CID_k, z_k) is valid, it sends back to common server.

Step 6: The common server evaluates me_2 and checks the condition ha_2 to authenticate the node E_l. However, the server terminates the session if the authentication is identified to be failed. Else the common server begins to evaluate $x_{l,k}$, P_3 and ha_3. Finally, the common server transmits the message data $D_3 = \{P_3, ha_3\}$ via a public channel. The protocol model of proposed ECC based security is shown in Figure 3.

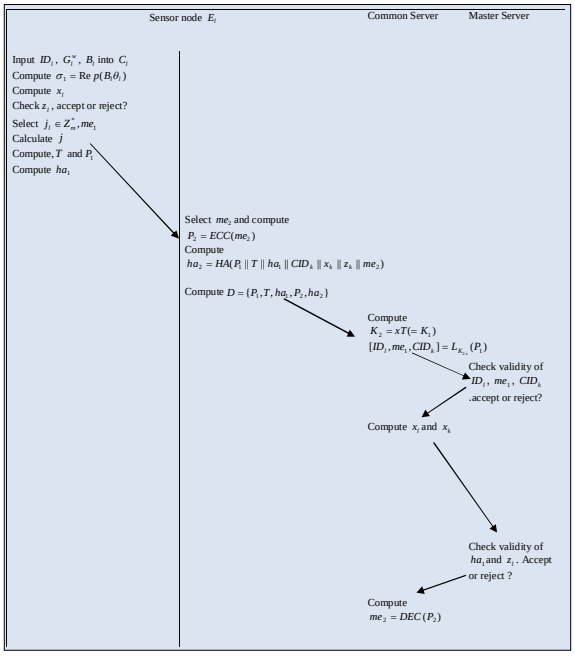

Figure 3 : Master Server based ECC protocol

4.RESULTS AND DISCUSSION

G. Simulation Setup

The MANET network with specific nodes and cluster head is simulated in MATLAB R2015a. The respective nodes are fixed in the area of $100m \times 100m$. In this investigation, the message transmission from one node to the cluster head is performed. Moreover, the hashing based formulation is performed for validating each sensor. The security of the transmitted messages is also analyzed by the determination of four types of attacks. Next to this, the performance of the proposed ECC is compared with the conventional AES based model for certifying the superiority of proposed method.

H. Compuattional Efficiency

Table 2 shows the comparison of proposed protocol over other conventional protocols. In this, the proposed protocol along with master server has attained high computational time of 19.1904 (ms) since it has more steps in case of validation and evaluation. However, the conventional protocols requires only less computation time to execute. Henceforth, it is concluded that the proposed protocol could resist various attacks, but the time taken for this is high over the conventional protocols.

Table 2: Computational Efficiency of Proposed and Conventional Protocols

Methods	**Computational time (ms)**
Srikanta and Manmanth [26]	26.67
Shabnam and Mazleena [27]	31.12
Yang Yang [28]	11.11
Charikleia *et al*. [29]	37.78
ECC-based security protocol [30]	8.8904
Proposed master Server based ECC protocol	11.1604

I. Key Sensitivity Analysis

In order to do the analysis of key sensitivity, the transmitted message's original key is altered ten times and performs the process of decryption. The analysis finds the capability of proposed protocol by changing the key. Table 3 shows the key sensitivity analysis of transmitted messages. The conventional AES based protocol could recover the value closer to the original value, and the total messages get decrypted by changing keys. The ECC- based security protocol outperforms the AES based protocol, as it could decrypt the text and sometimes it restores the value with vast deviation from the original value. Moreover, the proposed protocol outperforms both the conventional methods since it could decrypt the text and could restore the values with very large deviation when compared to other methods.

Table 3: Key Sensitivity Analaysis of transmitted Meassage

AES- based security protocol	Status	ECC-based security protocol	Status	Proposed Master Server based ECC protocol	Status
64	Yes	0	No	0	Yes
25	Yes	0	No	0	Yes
31	Yes	0	No	0	Yes
72	Yes	0	No	0	Yes
3	Yes	1	Yes	0	Yes
119	Yes	1	Yes	0	Yes
53	Yes	0	No	0	Yes
119	Yes	1	Yes	0	Yes
94	Yes	0	No	0	Yes
45	Yes	0	No	0	Yes

J. Robustness Against Attack

In this investigation, four attacks like Known Plain Text Attacks (KPA), Cipher Text Only Attack (COA), Cipher Plain Text Attacks (CPA) and Chosen Cipher Text Attack (CCA) are defined for assuring the security of the transmitted messages. In order to identify the robustness of MANET over these attacks, the message is changed and obtains ten equivalent messages. Next to this, the ciphertext of 10 messages is created. KPA is the correlation among message and the respective ciphertext, while COA is the correlation among decrypted message and the ciphertext. Consequently, some parts of the plain message get altered and attain the corresponding ciphertext. CPA is the correlation among altered text and the ciphertext whereas CCA is the correlation among altered ciphertext and the decrypted text. The security features of the protocol against the potential attacks are shown in Table 4. In case of KPA, the ECC – based security protocol is 95% better than AES while in the case of COA, ECC is 33% superior to AES. Furthermore, ECC is 81% better from AES while considering CPA and the performance of ECC is enormously better from AES whereas CCA is taken into account.

Table 4: Security Features of Protocols over Attacks

Methods	KPA	COA	CPA	CCA
AES-based security protocol	0.66667	0.12395	0.19535	0.016329
ECC-based security protocol	0.029586	0.082355	0.03691	-0.15414

K. Comparison of Functionality Features

The functional analysis of proposed method over other conventional methods is given in Table 5. It is proven that the functionality analysis of the proposed protocol scheme is better over other conventional protocols. All the features mentioned in the Table V can be fulfilled by the proposed protocol. This is because the validation and evaluation of proposed protocol is stronger with the master server, whereas the conventional protocols lack in this. Resultant to this, the proposed protocol is suitable for real time applications when compared to the conventional protocols.

Table 5: Functional Feature Analysis of Proposed Protocol over others

Features	Vanga [31]	ECC based security protocol	Proposed Master-Server Based ECC protocol
Free from denial of service attack	Yes	Yes	Yes
Requires identity-verification table	Yes	Yes	Yes
Server spoofing attack resistance	Yes	Yes	Yes
Stolen verifier attack resistance	Yes	Yes	Yes
Drawback in password change phase	No	No	Yes
Password guessing attack resistance	Yes	Yes	Yes
Known session-specific temporary information attack resistance	Yes	Yes	Yes
Stolen/lost smart card attack resistance	Yes	Yes	Yes
Provides strong user anonymity	Yes	Yes	Yes
Provides perfect forward secrecy	Yes	Yes	Yes
Provides mutual authentication	Yes	Yes	Yes
Impersonation attack resistance	Yes	Yes	Yes
Reply attack resistance	Yes	Yes	Yes
Provision for revocation and re-registration	Yes	Yes	Yes
Privileged insider attack resistance	Yes	Yes	Yes
Wrong password login	No	Yes	Yes
Provides SK-security	Yes	Yes	Yes
Man-in-the-middle attack resistance	Yes	Yes	Yes

5.CONCLUSION

It is well known that the MANET is concerned to be the multi-hop wireless network including various mobile nodes. The common security issues comprise of node vulnerability, channel vulnerability and dynamically changing network topology. In this experimentation, the mentioned security-based challenges while message transmission from a single node to the equivalent cluster head and the protection of messages from the hackers is also concerned. This paper has introduced a new ECC – based security protocol in MANET with two phases namely Registration phase and Authentication phase. Further, this paper has contributed a new working model in the authentication phase with the introduction of two servers: Common server and Master server. Here, the computing process has been performed by common server and the validation was done by master server. By adopting these two servers, the proposed protocol had seemed to be stronger

with effective authentication. Finally, the proposed protocol has compared over other conventional protocols in terms of security.

REFERENCES

[1] U. Ghosh and R. Datta, "A Secure Addressing Scheme for Large-Scale Managed MANETs," in IEEE Transactions on Network and Service Management, vol. 12, no. 3, pp. 483-495, Sept. 2015. https://doi.org/10.1109/TNSM.2015.2452292

[2] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, March 2015. https://doi.org/10.1109/JSYST.2013.2296197

[3] VijayLaxmi, ChhaganLal, M.S.Gaur and DeepanshuMehta, "JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET," Journal of Information Security and Applications, vol. 22, pp. 99-112, June 2015. https://doi.org/10.1016/j.jisa.2014.09.003

[4] D. Hurley-Smith, J. Wetherall and A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks," in IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2927-2940, Oct. 1 2017.

[5] Tahsin Arafat Reza and MichelBarbeau, " QaASs: QoS aware adaptive security scheme for video streaming in MANETs", Journal of Information Security and Applications, vol. 18, no.1, pp. 68-82, 2013.

[6] MarjanKuchaki Rafsanjani and HamidehFatemidokht, "FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs", AEU - International Journal of Electronics and Communications, vol. 69, no. 11, pp. 1613-1621, 2015. https://doi.org/10.1016/j.aeue.2015.07.013

[7] Malik N.Ahmed, Abdul HananAbdullah, HassanChizari and OmprakashKaiwartya, " F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs", Journal of King Saud University - Computer and Information Sciences, vol. 29, no.3, pp. 269-280, July 2017.

[8] Saju PJohn and PhilipSamuel, " Self-organized key management with trusted certificate exchange in MANET", Ain Shams Engineering Journal, vol. 6, no. 1, pp. 161-170, March 2015.

[9] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta and P. Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems," in IEEE Systems Journal, vol. 5, no. 2, pp. 176-188, June 2011.

[10] M. Burmester and B. de Medeiros, "On the Security of Route Discovery in MANETs," in IEEE Transactions on Mobile Computing, vol. 8, no. 9, pp. 1180-1188, Sept. 2009.

[11] D. Q. Nguyen, M. Toulgoat and L. Lamont, "Impact of trust-based security association and mobility on the delay metric in MANET," in Journal of Communications and Networks, vol. 18, no. 1, pp. 105-111, Feb. 2016.

[12] T. R. Andel and A. Yasinsac, "Surveying security analysis techniques in manet routing protocols," in IEEE Communications Surveys & Tutorials, vol. 9, no. 4, pp. 70-84, Fourth Quarter 2007.

[13] A. Anand, H. Aggarwal and R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks," in Journal of Communications and Networks, vol. 18, no. 6, pp. 938-947, Dec. 2016.

[14] N. Mohammed, H. Otrok, L. Wang, M. Debbabi and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," in IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan.-Feb. 2011. https://doi.org/10.1109/TDSC.2009.22

[15] P. Papadimitratos and Z. J. Haas, "Secure data communication in mobile ad hoc networks," in IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 343-356, Feb. 2006.

[16] M. Ramkumar and N. Memon, "An efficient key predistribution scheme for ad hoc network security," in IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 611-621, March 2005.

[17] M. N. Lima, A. L. dos Santos and G. Pujolle, "A survey of survivability in mobile ad hoc networks," in IEEE Communications Surveys & Tutorials, vol. 11, no. 1, pp. 66-77, First Quarter 2009.

[18] S. Bu, F. R. Yu, X. P. Liu and H. Tang, "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks," in IEEE Transactions on Wireless Communications, vol. 10, no. 9, pp. 3064-3073, September 2011. https://doi.org/10.1109/TWC.2011.071411.102123

[19] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys," in IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, pp. 386-399, Oct.-Dec. 2006.

[20] R. H. Jhaveri, N. M. Patel, Y. Zhong and A. K. Sangaiah, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT," in IEEE Access, vol. 6, pp. 20085-20103, 2018. https://doi.org/10.1109/ACCESS.2018.2822945

[21] T. R. Reshmi and K. Murugan, "Light weight cryptographic address generation (LW-CGA) using system state entropy gathering for IPv6 based MANETs," in China Communications, vol. 14, no. 9, pp. 114-126, Sept. 2017.

[22] M. S. Khan, D. Midi, M. I. Khan and E. Bertino, "Fine-Grained Analysis of Packet Loss in MANETs," in IEEE Access, vol. 5, pp. 7798-7807, 2017.

[23] N. Schweitzer, A. Stulman, R. D. Margalit and A. Shabtai, "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 16, no. 8, pp. 2174-2183, Aug. 1 2017.

[24] S. Kim, "Effective certificate revocation scheme based on weighted voting game approach," in IET Information Security, vol. 10, no. 4, pp. 180-187, 7 2016.

[25] U. Ghosh and R. Datta, "A Secure Addressing Scheme for Large-Scale Managed MANETs," in IEEE Transactions on Network and Service Management, vol. 12, no. 3, pp. 483-495, Sept. 2015. https://doi.org/10.1109/TNSM.2015.2452292

[26] Srikanta Kumar Sahoo, Manmanth Narayan Sahoo, "An Elliptic-Curve-Based Hierarchical Cluster Key Management in Wireless Sensor Network," Proceedings of the International Conference on Advanced Computing, Networking, and Informatics, pp 397-408, vol 243. Springer, New Delhi, 18 December, India, 2013.

[27] Shabnam Kasra-Kermanshahi, Mazleena Salleh, "An Improved Certificateless Public Key Authentication Scheme for Mobile Ad Hoc Networks Over Elliptic Curves", Springer International Publishing, vol 355. Springer, Cham, pp 327-334, 21 June, 2015.

[28] Yang Yang, "Broadcast encryption based non-interactive key distribution in MANETs", Journal of Computer and System Sciences, vol. 80, no. 3, pp 533–545, May 2014. https://doi.org/10.1016/j.jcss.2013.06.009

[29] Khaled Hamouid, Kamel Adi, "Efficient certificateless web-of-trust model for public-key authentication in MANET", Computer Communications, vol. 63,no C, pp 24–39, 1 June, 2015.

[30] Regula Srilakshmi and Jayabhaskar Muthukuru, " Elliptic Curve Cryptography Based Security Protocol of MANET under Dynamic Cluster Head Selection Environment", in communication.

[31] Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami, " A Secure Biometrics-Based Multi-Server Authentication Protocol using Smart Cards", IEEE Transactions On Information Forensics And Security, 2015. https://doi.org/10.1109/TIFS.2015.2439964