ISSN 2347 - 3983
Volume 8. No. 2, February 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter32822020.pdf
https://doi.org/10.30534/ijeter/2020/32822020

# Elliptic Curve Cryptography Based Security Protocol of MANET under Dynamic Cluster Head Selection Environment

**R.Srilakshmi [1], Dr.Jayabhaskar Muthukuru[2]**
[1]Research Scholar, KLEF (Deemed to be University), regulasrilakshmi@gmail.com
[2]Professor, KLEF (Deemed to be University), jayabhaskar@kluniversity.in

## ABSTRACT

Recently, Mobile ad hoc network (MANET) is progressively emerging to be an extensive part in the rise of wireless technology domain. In this network, security has become a major challenge which affects the data communication among the nodes and the cluster head (mobile nodes). Those challenges arise due to the channel vulnerability, dynamically changing network topology, lack of infrastructure and node vulnerability. The major objective of the experimentation is to transmit the message from the sensor node to its correspondent cluster head as well as to protect the message from the hackers. In this paper, Elliptic Curve Cryptography (ECC) based security protocol is proposed to adopt those objectives. This paper intends to introduce a security protocol for MANET even under varying Cluster Head environment. Further, attacks-based analysis and key sensitivity analysis is done to determines the effectiveness of the communication. Also, the performance of the proposed ECC- based security protocol compares with the conventional Advanced Encryption Standard (AES) protocol. The computational time of the proposed method is compared with the methods as reported in the literature, where the computational time of the proposed method superior to the conventional methods. Finally, the overall comparison ascertained that the security of the network by proposed method increases from the standard encryption.

**Key words:** MANET, mobile node, cluster head, communication, security protocol, ECC, attacks

## 1. INTRODUCTION

MANET [13] [14] [15] [16] [17] [18] [19] [20] is an infrastructure-less, self-arranging, multi-hop and inimical formed network prototype of mobile devices [36] [37] linked by in-between nodes [3]. Each node in MANET takes the responsibility of the router, in which it transmits the observed packets to the command centre through wireless channels [1]. Since the nodes are typical of small size, there are constraints on computation speed, memory, energy for transmission, bandwidth, and limited battery existence [4].Due to its self-organizing reconfigurability, the lack of physical security and rapidly deployed ability, wireless communication, and intermediate nodes are suffered from diverse attacks such as masquerading, impersonation, spoofing, interception and modification [1]. To provide secure communication in MANETs, two methodologies could be revealed such as attack-oriented and cryptography.

The earlier developed works on MANET were mostly based on the initial approach. However, those works have failed to introduce advanced solutions to handle the possible hazards and severe attacks [7] [8] [9] [10] [11]. Further, the security of MANET has been developed using the second approach from which the researchers conflicted to adopt the lightweight cryptosystem that could satisfy restriction of resources in MANETs. Under such circumstances, resource-constrained environments use symmetric cryptography (SC) [21] [22] [23] [24] [25] in which the complexity under management of keys in SC induces the developers to apply public key cryptography (PKC) instead [12] [26] [27] [28] [29] [30]. Due to the problems of the discrete logarithm, the computational complexity increases. Thus the high-security Elliptic Curve Cryptography (ECC) [31] [32] [33] [34] [35] has been suggested to diminish the count of computation. Moreover, ECC deals a better performance because it attains the similar protection with smaller key size [6]. Several optimization methods [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] are exploited to solve the problems of ECC.

The main contribution of this paper is to introduce a security protocol for MANET even under varying Cluster Head environment. The ECC based private-public key pairs is generated for each node and a registration phase is proposed during the change of Cluster Head. The hashing based evaluation is performed to validate each sensor. Moreover, the hashing is applied for both key distribution as well as message transmission. In addition, the protocol is developed with multiple authentication stages using ECC to protect the protocol from attacks.

## 2. LITERATURE REVIEW

Srikanta Kumar Sahoo and Manmanth Narayan Sahoo have proposed an Elliptic curve based Hierarchical cluster key management scheme for wireless sensor network (WSN). In this approach, Root cluster head (RCH) has generated a global group key (GGk) and then signs it with own Root cluster group key and sends to each Cluster Head. Cluster Head decrypted GGK and signature by using cluster group key and then sends it to every Sense node (SN). Finally, SN decrypted it and then acquired GGK. Later, the author has compared the

performance of the proposed method regarding the duration of a generation, count of distributed messages, overall key capacity and consumption of energy with Khamy's scheme. Hence, the experimental results showed that it has been quicker than Khamy's scheme. Thus the experimental results showed that the proposed method provides the superior performance regarding storage of keys, count of operations and count of messages transferred during the establishment of keys [1].

To meet security demands as well as the communication overhead of mobile ad hoc network Yang Yang [3] has been suggested a lightweight Identity-Based Broadcast Encryption (IBBE) approach. Since the group membership changes vigorously, the group key has to be efficient. For such case, at the encryption phase, it only adds or excludes that particular member ID to produce a new group key and then the communication overhead also unchanged since encapsulation of group key remains stable. Finally, it has proved the security analysis and compared with the truncated q-ABDHE standard model. The experimental results have shown that it has been achieved high efficiency and gained high security against chosen ciphertext attack.

In 2004, Charikleia Zouridaki et al. [4] have proposed a comprehensive approach to contribute a distributed CA-based PKI in MANETs based on Elliptic Curve Cryptography [4]. According to this scheme, cluster-based key management with mobile CA servers using ECC in which the mobile Certification Authority (CA) has to provide dispersed service for the mobile nodes. It showed that the performance improvement and limited computational power than the standard systems using ECC. Ankush A. Vilhekar and C.D. Jaidhar [6] introduced an efficient modified Authentication Protocol using ECC on MANET for Virtual Subnets. However, it was claimed that protocol with RSA-based cryptosystem was failed to handle the devices with low computations such as PDAs, mobile, smart cards, etc due to the increment of the computational power. Thus the high security with less computation is attained by contributing same scheme with ECC. Thus the experimental results have proved that the number of computations had been reduced than the RSA with the same level of security also produced shorter key size.

Moreover, for large-scale networks, a new certificate less PGP-like trust establishment scheme for MANET has been proposed by Khaled Hamouid and Kamel Adi in the year 2015 [5]. Moreover, the approach has adopted a distinct method using self-certifying ID-based cryptography. This model has granted the mobile nodes to estimate the public-keys of each other from only the nodes identities and their trust levels. The above approach has proved and compared the efficiency, security, and performance of traditional PGP-like schemes. In the same year, an improved certificate-less public key authentication ID-RSA using elliptic curve based algebraic groups has been presented by Shabnam Kasra-Kermanshahi and Mazleena Salleh [2]. More accurately, in RSA security based protocol, the use of bilinear pairing has considered a costly cryptographic map, and it seemed that they are not lightweight enough to be used in MANETs. To overcome this drawback, the above approach has proved the ID-RSA using Elliptic Curve-based algebraic groups. Hence the above experimental approach has been achieved better efficiency when compared with ID-RSA protocol. Fig 1 states the taxonomy of elliptic curve cryptography.

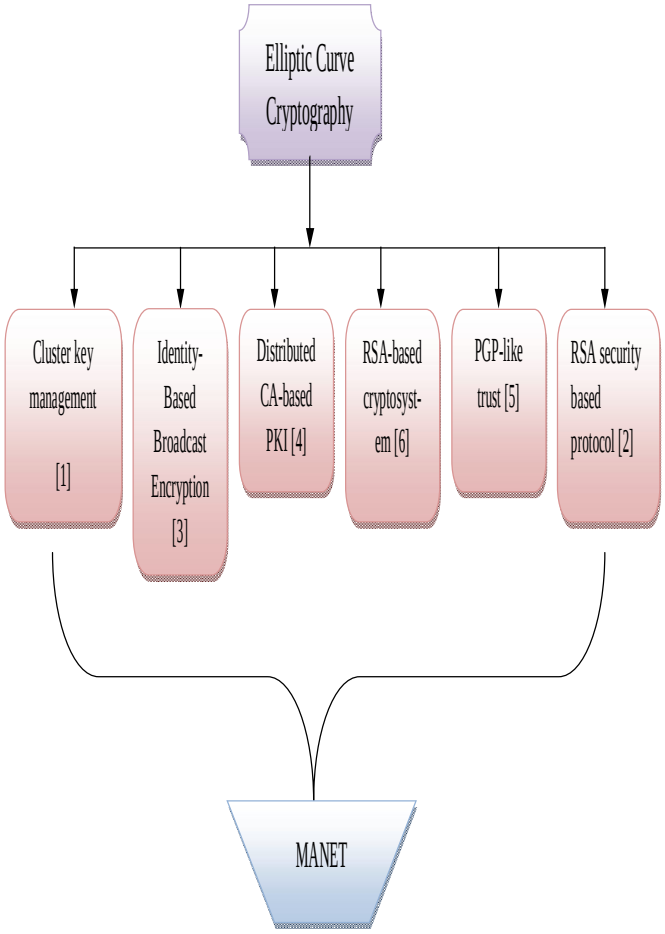


**Figure 1:** Taxonomy of Elliptic Curve cryptography

This section summarizes the findings of the existing literature as well as its challenges. Therefore the existing knowledge of the related works can be easily analyzed.Though ECC can provide a high degree of security over message transmission among multiple members of a network, a limited number of applications on MANETs have been found in the literature. Very few researchers have worked on adopting ECC concepts on MANET [1] [2] [3] [4] [5]. However, the intention of exploiting the ECC has remained in accomplishing the security with limited key size. Since the MANET is infrastructure-less and dynamic, any nodes can become Cluster Head or RCH. Meantime, the Cluster Head and RCH may be alive or dead node after losing its energy. Under such circumstances, the current protocols require major review. The fact is that the state-of-the-art protocols become ineffective. For an instant, a periodic data transmission has been considered in [1] under which the RCH and Cluster Head are powerful and robust against attacks. However, the RCH and Cluster Head are nodes of the MANET, and they may change in the subsequent

periods. Such periodical dynamicity has not been considered, and so the routing protocols remain ineffective. Certificate-less protocols [2] [5] require crucial enhancements under change of Cluster Head and RCH, whereas the rest of the protocols [3] [4] and [6] need to be enhanced under adversarial environment.

In general, the MANET symbolizes the complex disseminated system that consists of diverse wireless mobile nodes. The general architecture model of MANET is shown in fig. 2. The network architecture is categorized into enabling technologies and networking application and middleware, where each category is related to specific network operations. The nodes in the network are grouped into clusters to adopt rapid and reliable data transmission. From each cluster, a cluster head is selected which should receive data from the nodes of its cluster. The main security-related challenges in MANET include channel vulnerability, dynamically changing network topology, lack of infrastructure and node vulnerability. If the network dynamically changes the topology, the node may happen to transmit the data to the cluster head which does not belong to its cluster. Under such circumstance, wrong cluster head may happen to receive the transmitted data and further it receives the data from the nodes belongs to its group. As a result, congestion may cause in the network. On the contrary, if the wrong cluster receives the transmitted data, it may act as the hacker which leads to losing the security of the network which can be termed as node vulnerability. Moreover, the channels between nodes and cluster head may sometimes act as the hacker that comes under the channel vulnerability challenge.

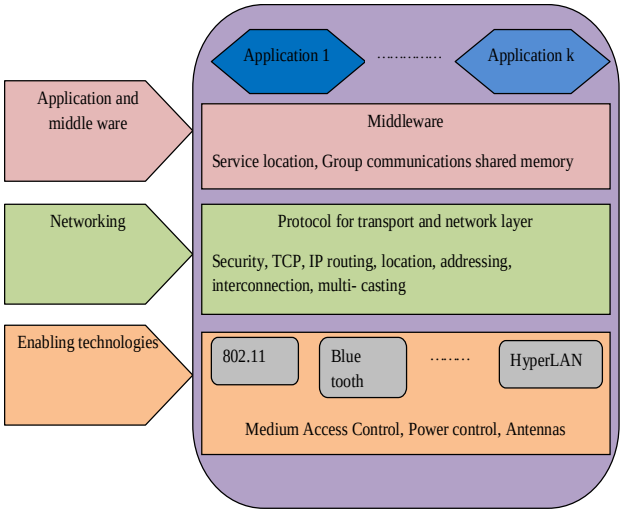


**Figure 2:** Architecture of MANET

## 3. ECC-BASED SECURITY PROTOCOL FOR MANET

"ECC is an approach to public- key cryptography based on the algebraic structure of elliptic curves over a finite field". The advantageous part of ECC is that it only needs smaller keys when compared with the general cryptographic method. The basic operations of ECC are elliptic curve scalar multiplication, elliptic curve doubling, and elliptic curve addition. Let us consider two points A and B, and the pattern of arithmetic operations is shown in Algorithm 1 in which the scalar multiplication is dependent on the elliptic curve addition and doubling operations. Thus the algorithm 1 mathematically represents the elliptic curve scalar multiplication along with the elliptic curve addition and doubling operations.

**ALGORITHM 1**: ELLIPTIC CURVE SCALAR MULTIPLICATION

Input: Integer $n = (1, n_{i-2}, \ldots n_1, \ldots\ldots n_0)$
Output: $B = nA$ /*Elliptic curve scalar multiplication

Initialize: $B \leftarrow A$
For $a = b - 2$ down to 0 do
$B \leftarrow 2B$ /*Elliptic curve doubling
If $n_a = 1$, then
$B \leftarrow A \oplus B$ /*Elliptic curve addition
end
End for
Return $B$

The ECC-based protocol for MANET security contains two primary phases such as registration phase and an authentication phase. The registration phase makes all nodes register to its corresponding cluster head to provide proper services. In this phase, the unique identity of a node $ID$ is determined and concatenates with the hash of that $ID$ and further, they are stored in the smart card $Q_l$. Thus this phase can share the credential as well as to generate the common credentials. On the other hand, authentication phase is to access the resources of the service supplier. Fig. 3 demonstrates the protocol model of proposed ECC-based security.

In this experiment, the unique identity of the cluster head is denoted as $SID$, and unique identity of each node is denoted as $ID$. Here, data $G$ with the message $m$ is passed from the node to the cluster head. In general, the objective of the experiment is to identify whether the node of a specified cluster is passing message only to its cluster head. For this identification, the number of parameters is determined, in which all the required conditions are demonstrated in the protocol diagram. At first in the transmission section, the verifying part starts with computing the condition as given in Eq. (1) and eq. (2) to check it gets hold or not where $x_k$ refers to the public key of the node, $F$ refers to the ciphertext, $P$ refers to the generator of the field, $P^{pub}$ refers to the public key of $CHRC$, $K_1$ refers to the point of cryptography (ECC), $K_{1x}$ refers to the x- coordinate of $K_1$.

$$ha_1 = H(ID_l \| SID_k \| z_k \| m_1 \| x_l \| S \| K_1) \quad (1)$$

$$ha_2 = H(F_1 \| S \| ha_1 \| SID_k \| x_k \| z_k \| m_2) \quad (2)$$

$$x_l = v_l \oplus H(P_l^w \| \sigma_1) \quad (3)$$

$$z_l = H(x_l \| ID_l \| H(P_l^w \| \sigma_1)) \quad (4)$$

$$S = jP \quad (5)$$

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

$$j = H(j_l \| x_l \| m_1) \quad (7)$$

$$F_1 = E_{K_{1x}}[ID_l, SID_k, z_l, m_1] \quad (8)$$

The message is get encrypted in the node by ECC which can be represented as given in Eq. (9). The ciphertexts $N_1$ and $N_2$ are determined based on Eq. (10) and eq. (11) Where $\alpha_1$ represents the random number. The arithmetic operation of $N_1$ is related to elliptic curve scalar multiplication and $N_2$ is related to elliptic curve addition.

$$F_2 = N_1 + N_2 \quad (9)$$

$$N_1 = \alpha_1 P \quad (10)$$

$$N_2 = m_2 + \alpha_1 P^{pub} \quad (11)$$

$$m_2 = N_2 - N_1 * P^{pri} \quad (12)$$

Thus the data that has to be passed from the node to the concerned cluster head is formed as $G = \{F_1, S, ha_1, F_2, ha_2\}$. Finally, in the cluster head, the passed message is decrypted by ECC suing eq. (12) where $P^{pri}$ refers to the private key.

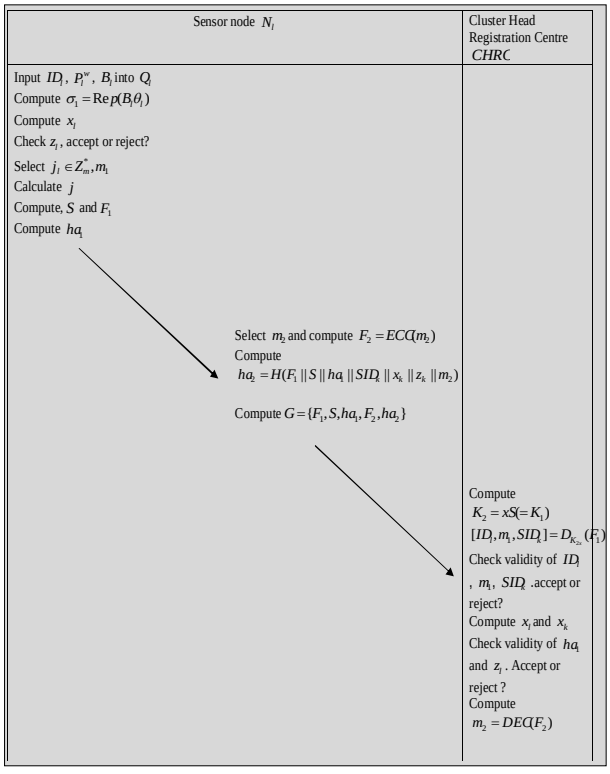


**Figure 3:** Protocol model of proposed ECC-based security

### 3.1 Correctness of protocol

Proof 1: The correction protocol of the encryption protocol is given in this proof. As given in the protocol,

The Representation of the $K_1$ is given in Eq. (6)

$K_1 = K_2$

Whereas, the representation of $S$ is given in Eq. (5)

$$jP^{pub} = xS$$

$$jP^{pub} = xjP$$

$$jP^{pub} = j(xP)$$

$$jP^{pub} = jP^{pub}$$

Hence proved $K_1$ is equivalent to $K_2$

Proof 2: The correction protocol of the decryption process is given this section. As per eq. (12)

The representation of $N_2$ is given in Eq. (11) and $N_1$ is given in Eq. (10).

$$m_2 = N_2 - N_1 * P^{pri}$$

$$m_2 = m_2 + \alpha_1 P^{pub} - \alpha_1 P * P^{pri}$$

$$m_2 = m_2 + \alpha_1 P^{pub} - \alpha_1 P^{pub} \Rightarrow m_2 = m_2$$

### 3.2 Registration Phase

This phase helps to eliminate the new node registration with the actual status of the legal node. The identity-verifier table denoted by $\chi$ help to match the new node registration with legal nodes. For instance, in this phase, the node $N_l$ selects $SID_l$ refers to the assumed to send the registration request $\{SID\}_l$ to the cluster head registration centre $CHRC$. To the next from receiving the request, the $CHRC$ checks whether the hash value of $H(SID_l \| x)$ matches with any one of the entries in the table $\chi$. If the value of hash gets a match, then the $CHRC$ refuses the request and assert the concerned request as invalid. In another case, $CHRC$ randomly generates a number $y_l$ calculate authentication parameter $x_l = H(SID_l \| x \| y_l)$. Also, $CHRC$ computes the $z_l$ on $SID_l$ in correspondence with $y_l$ which is the form $z_l = H(SID_l \| x \| y_l \| SID_l)$ and stores the $\{H(SID_l \| x), y_l\}$ into the table $\chi$. At last, $CHRC$ sends this information to the concerned node $N_l$ and declares the information that should be publically accessible to all legal nodes. The registration phase of the nodes in MANET in this experimentation is shown in Table 2. Fig. 4 illustrates the protocol of Registration phase.

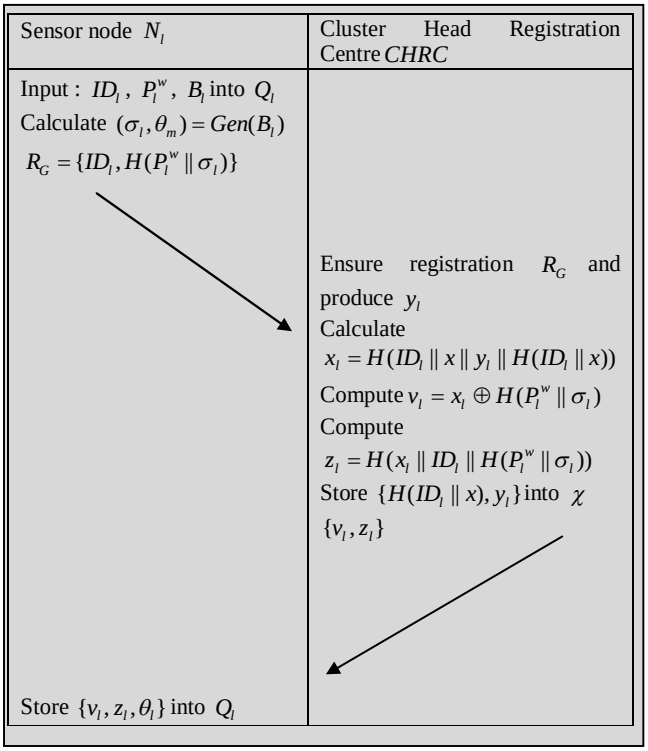


**Figure 4:** Protocol model of the registration phase

Let the noun- the singular elliptic curve is denoted as $Ec_p$ where $p$ be the large prime, $\Omega$ be the symmetric- key cryptography and $i$ be the order. Consider the pre-constructed smart card $Q_l$ with public parameters which is in the form $\{p, Ec_p, P, P^{pub}, i, \Omega, H(.)\}$ .Also in this phase, the smart card is obtained by each node. It is made possible by providing the aforementioned public parameters to the node $N_l$, and a built-in fingerprint scan component is embedded into the card reader. Here, the node $N_l$ sends the request to $CHRC$ and gain the smart card and further it is registered to the $CHRC$. The steps of registration are depicted below.

Step 1: Initially, the node $N_l$ inserts the smart card $Q_l$ into the card reader. Obtain the unique identity of the node $ID_l$, password $P_l^w$, and personal biometric $B_l$. Then the concerned node $N_l$ begins to calculate the $(\sigma_l, \theta_m) = Gen(B_l)$ and sends the request for registration to $CHRC$.

Step 2: Consequently, $CHRC$ verifies whether the hash value $H(ID_l \| x)$ matches with any of the entries in the table $\chi$ after receiving the request message. Here, $CHRC$ rejects the request if the hash value matches with the entries, and thus the concerned node is declared as the invalid one. Otherwise, $CHRC$ begins to calculate $x_l = H(ID_l \| x \| y_l \| H(ID_l \| x))$, $v_l = x_l \oplus H(P_l^w \| \sigma_l)$, $z_l = H(x_l \| ID_l \| H(P_l^w \| \sigma_l))$. Consequently, the table is updated with fresh entry $\{H(ID_l \| x), y_l\}$. Ultimately, $CHRC$ sends $\{v_l, z_l\}$ to the node $N_l$.

Step 3: The node $N_l$ stores $\{v_l, z_l, \theta_l\}$ into the smart card $Q_l$ after getting $\{v_l, z_l\}$.

### 3.3 Authentication and Message Transmission phase

The reliable communication under the insecure channel is made possible in this phase. The required steps of the authentication phase are illustrated below.

Step 1: Randomly choose the nonce $m_1$ after getting the login message $G_1$. Then, compute $F_2$, $ha_2$. After computing those values $N_l$ sends the message $G$ to $CHRC$ via public channel.

Step 2: Subsequently, the $CHRC$ tends to calculate the $K_2 = xS(= K_1)$ and thus determines $ID_l$, $SID_k$, $z_k$ and $m_1$. These are done by decrypting $F_1$ using $K_{2x}$ where $K_{2x}$ refers to the x- coordinate of the ECC point $K_2$. Further, $CHRC$ verifies the freshness of $m_1$ and also verify the validity of both $ID_l$ and $SID_k$ by checking $H(ID_l \| x)$ and $H(SID_k \| x)$ respectively in $\chi$. However, $CHRC$ terminates the sitting if these verified parameters seem to be valid. Otherwise, $CHRC$ recovered the $y_k$ and $y_l$ in correspondence with the $ID_l$ and $SID_k$ from $\chi$. Further, $CHRC$ calculates the $x_l = H(ID_l \| x \| y_l \| H(ID_l \| x))$ and $x_k = H(SID_k \| x \| y_l)$. It is also essential to check whether the form $ha_1 = H(ID_l \| SID_k \| z_k \| m_1 \| x_l \| S \| K_1)$ and $z_k = H(x \| y_k \| x_k \| SID_k)$ hold or not. However, $CHRC$ ends the session, if these do not get hold. On the other hand, the received record $(SID_k, z_k)$ is valid. Further, $CHRC$ computes $m_2$ and checked the condition $ha_2$ to authenticate the node $N_l$. However, $CHRC$ terminates the session, if the authentication is found to be failed. Otherwise, $CHRC$ begins to calculate $x_{l,k}$, $F_3$ and $ha_3$. In the end, $CHRC$ sends the message data $G_3 = \{F_3, ha_3\}$ via a public channel.

## 4. PERFORMANCE ANALYSIS

### 4.1 Simulation and Procedure

The MANET network with specified nodes and cluster head is simulated in MATLAB R2015a. The specified nodes are fixed in the area of $100m \times 100m$. The transmission of messages from one node to the cluster head is performed in this experimentation. Here, hashing based evaluation is performed

to validate each sensor. Furthermore, the security of the transmitted messages is analyzed through the determination of four types of attacks. To the next of this analysis, the performance of the proposed ECC is compared with the conventional AES based approach to certifying the effectiveness of the proposed method.

### 4.2 Robustness against attacks

The four attacks such as Known Plain Text Attacks (KPA), Cipher Text Only Attack (COA), Cipher Plain Text Attacks (CPA) and Chosen Cipher Text Attack (CCA) are determined in this experimentation to ensure the security of the transmitted messages. To find the robustness of MANET against the attacks, the message $m_2$ is altered and obtains ten equivalent messages. To the next, the ciphertext of 10 messages is created. KPA is the correlation between the message and the corresponding ciphertext whereas the COA is the correlation between the decrypted message and the ciphertext. Subsequently, the few parts of the plain message are altered and obtain the corresponding ciphertext. On the other hand, CPA is the correlation between the altered text and the ciphertext whereas CCA is the correlation between the altered ciphertext and the decrypted text. The security features of the protocol against the potential attacks are shown in Table 1. In case of KPA, the ECC – based security protocol is 95% better than AES while in the case of COA, ECC is 33% better than AES. Furthermore, ECC is 81% superior to AES while considering CPA and the performance of ECC is enormously better than AES while CCA is taken into account.

**Table 1:** Security Features of the Protocols against Potential 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 |

**Table 2:** Key sensitivity analysis of the transmitted messages

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

**Table 3:** Computational efficiency of the proposed method with conventional methods

| Methods | Computational time (ms) |
|---|---|
| Srikanta and Manmanth [1] | 26.67 |
| Shabnam and Mazleena [2] | 31.12 |
| Yang Yang [3] | 11.11 |
| Charikleia et al. [5] | 37.78 |
| ECC-based security protocol | 8.8904 |

### 4.3 Key Sensitivity Analysis

To perform the key sensitivity analysis, the original key of a transmitted message is changed ten times and performs the decryption process. The analysis identifies the ability of the method while changing the key. The key sensitivity analysis of the transmitted messages is shown in Table 2. In the case of conventional AES method, the decryption process recovers the value nearly close to the original value, and entire messages are get decrypted while changing keys. However, the proposed ECC- based security protocol outperforms, as it does not decrypt the text and some time, the decryption is possible, and it restores the value with vast variation from the original value.

### 4.4 Computational Efficiency

Table 2 shows the comparison of the computational efficiency of the proposed ECC- based security protocol against the methods reported in the literature. The computational time is determined based on the contribution of scalar multiplication in the current methods. As per the paper [38], the required time per scalar multiplication is 2.2226 ms. By this way, the overall computational time in Srikanta and Manmanth [1] is 26.67ms, Shabnam and Mazleena [2] is 31.12ms, Yang Yang [3] is 11.11ms, Charikleia et al. [5] is 37.78 ms and the proposed ECC- based security protocol is 8.8904ms which is better than entire conventional methods.

## 5. CONCLUSION

MANET is generally considered to be a multi-hop wireless network consists of numerous mobile nodes. The general security challenges include channel vulnerability, dynamically changing network topology, lack of infrastructure and node vulnerability. Those security-based challenges during the transmission of a message from a single node to the equivalent cluster head and protecting messages from the hackers are considered in this experimentation. This paper has presented the novel ECC – based security protocol in MANET to overcome the challenges above. Further, the proficiency of the proposed algorithm was endorsed by analyzing four different types of attacks and sensitivity of key. Consequently, the performance of the proposed method was compared with the conventional AES method to find the ability of the adopted algorithm. Then the computational time of the proposed method was compared with the conventional methods as

reported in the literature. As compared to the conventional protocol, proposed ECC- based security protocol performs better by achieving higher security.

**REFERENCES**


[1] 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. https://doi.org/10.1007/978-81-322-1665-0_38

[2] 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.

[3] 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.

[4] Charikleia Zouridaki, Brian L. Mark, Kris Gaj, Roshan K. Thomas, "Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography", Springer Berlin Heidelberg, pp 232-245, 25-26 June, Greece, 2004.

[5] 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.

[6] Ankush A. Vilhekar, C. D. Jaidhar, "Modified Authentication Protocol Using Elliptic Curve Cryptosystem for Virtual Subnets on Mobile Adhoc Networks", Springer Berlin Heidelberg, pp 426-432, 1-3 August, China, 2011.

[7] Hu, Y., Perrig, A., Johnson,D.: Packet leashes: a defense against wormhole attacks in wireless ad hoc networks. Proceedings of IEEE INFORCOM, San Francisco, CA, USA, 2002.

[8] Capkun, S., Buttyan, L., Hubaux, J.: Sector: secure tracking of node encounters in multi-hop wireless networks. Proceedings of the ACM workshop on security of ad hoc and sensor networks, 2003. https://doi.org/10.1145/986858.986862

[9] Yi, S., Naldurg, P., Kravets, R.: Security-aware ad-hoc routing for wireless networks. Report No. UIUCDCS-R-2002-2290, UIUC, 2002.

[10] Sanzgiri, K., Dahill, B., Levine, B., Shields, C., Belding-Royer, E.: A secure routing protocol for ad hoc networks. Proceedings of IEEE international conference on network protocols (ICNP), New York, NY, USA, pp. 78–87, 2002.

[11] Hu, Y., Johnson, D., Perrig, A.: SEAD: secure efficient distance vector routing in mobile wireless ad-hoc networks. Proceedings of the 4th IEEE workshop on mobile computing systems and applications (WMCSA'02), Washington, DC, USA, pp. 3–13, 2002.

[12] Oliveira, L.B., Dahab, R.: Pairing-based cryptography for sensor networks. Presented at IEEE international symposium on network computing and applications, Cambridge, Coimbatore India, July 2006.

[13] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, no. 3, pp. 1089-1098, March 2013.

[14] Uichin Lee, Joon-Sang Park, Seung-Hoon Lee, Won W. Ro, Giovanni Pau, and Mario Gerla, "Efficient Peer-to-Peer File Sharing Using Network Coding in MANET", Journal of Communications and Networks, Vol. 10, no. 4, pp. 422-429, December 2008.

[15] Karim El Defrawy and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE Transactions on Mobile Computing, Vol. 10, no. 9, pp. 1345-1358, September 2011.

[16] Dongkyun Kim, Hanseok Bae, and C. K. Toh, "Improving TCP-Vegas Performance Over MANET Routing Protocols", IEEE Transactions on Vehicular Technology, Vol. 56, pp. 372-377, no. 1, January 2007. https://doi.org/10.1109/TVT.2006.883744

[17] Giovanni Di Crescenzo, Renwei Ge and Gonzalo R. Arce, "Securing Reliable Server Pooling in MANET Against Byzantine Adversaries", IEEE Journal on Selected Areas in Communications, Vol. 24, no. 2, pp. 357-369, February 2006.

[18] Jack L. Burbank, Philip F. Chimento, Brian K. Haberman, and William T. Kasch, "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology", IEEE Communications Magazine, vol. 44, no. 11, pp. 39-45, November 2006.

[19] Daniel Hiranandani, Katia Obraczka and J.J. Garcia-Luna-Aceves, "Manet Protocol Simulations Considered Harmful: The Case for Benchmarking", IEEE Wireless Communications, vol. 20, no. 4, pp. 82-90, August 2013.

[20] Kumar Viswanath, Katia Obraczka and Gene Tsudik, "Exploring Mesh and Tree-Based Multicast Routing Protocols for MANETs", IEEE Transactions on Mobile Computing, Vol. 5, no. 1, pp. 28-42, January 2006.

[21] Ren C. Luo, Long-Yeu Chung and Chang-Hua Lien, "A Novel Symmetric Cryptography Based on the Hybrid Haar Wavelets Encoder and Chaotic Masking Scheme", IEEE Transactions on Industrial Electronics, Vol. 49, no. 4, pp. 933-944, August 2002.

[22] Luca Breveglieri, Israel Koren and Paolo Maistri, "An Operation-Centered Approach to Fault Detection in Symmetric Cryptography Ciphers", IEEE Transactions on Computers, Vol. 56, no. 5, pp. 635-649, May 2007.

[23] Sean O'Melia and Adam J. Elbirt, "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 18, no. 11, pp. 1505-1518, November 2010.

[24] Adam J. Elbirt, Member and Christof Paar, "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography", IEEE Transactions on Parallel and Distributed Systems, Vol. 16, no. 5, pp. 468-480, May 2005.

[25] Gildas Avoine, Muhammed Ali Bingol, Xavier Carpent, and Siddika Berna Ors Yalcin, "Privacy-Friendly Authentication in RFID Systems: On Sublinear Protocols Based on Symmetric-Key Cryptography", IEEE Transactions on Mobile Computing, Vol. 12, no. 10, pp. 2037-2049, October 2013.

[26] Leif Uhsadel, Markus Ullrich, Amitabh Das, Dusko Karaklajic, Josep Balasch, Ingrid Verbauwhede and Wim Dehaene, "Teaching HW/SW Co-Design With a Public Key Cryptography Application", IEEE Transactions on Education, vol. 56, no. 4, pp. 1-6, March 2013.

[27] Lawrence O'Gorman and Irina Rabinovich, "Secure Identification Documents Via Pattern Recognition and Public-Key Cryptography", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, no. 10, pp. 1097-1102, October 1998.

[28] Farshid Delgosha and Faramarz Fekri, "Public-Key Cryptography Using Paraunitary Matrices", IEEE Transactions on Signal Processing, Vol. 54, no. 9, pp. 3489-3504, September 2006

[29] Andrew M. Odlyzko, "Public Key Cryptography", AT&TTechnical Journal, pp. 17-23, September/October 1994.

[30] James Goodman and Anantha P. Chandrakasan, "An Energy-Efficient Reconfigurable Public-Key Cryptography Processor", IEEE Journal of Solid-State Circuits, Vol. 36, no. 11, pp. 1808-1820, November 2001. https://doi.org/10.1109/4.962304

[31] S.C. Kak, "Secret-hardware public-key cryptography", IEEE Proceedings, Vol. 133, no. 2, pp. 94-96, March 1986.

[32] Zhe Liu, Hwajeong Seo, Johann GroBschadl and Howon Kim, "Efficient Implementation of NIST-Compliant Elliptic Curve Cryptography for 8-bit AVR-Based Sensor Nodes", IEEE Transaction on Information Forensics and Security Latex Class Files, Vol. 11, no. 12, pp. 1-13, December 2014.

[33] Reza Azarderakhsh, Kimmo U. Järvinen, and Mehran Mozaffari-Kermani, "Efficient Algorithm and Architecture for Elliptic Curve Cryptography for Extremely Constrained Secure Applications", IEEE Transactions on Circuits and Systems—I: Regular Papers, Vol. 61, no. 4, pp. 1144-1155, April 2014.

[34] William N. Chelton and Mohammed Benaissa, "Fast Elliptic Curve Cryptography on FPGA", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 16, no. 2, pp. 198-205, February 2008.

[35] Debiao He and Sherali Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography", IEEE Internet of Things Journal, vol. 2, no. 1, pp. 1-13, 2013 .

[36] Kabita Agarwal and Arun Agarwal,"The Next Generation Mobile Wireless Cellular Networks – 4G and Beyond", American Journal of Electrical and Electronic Engineering, vol. 2, no.03, pp.92-97, 2014.

[37] Arun Agarwal, Gourav Misra and Kabita Agarwal, "The 5th Generation Mobile Wireless Networks- Key Concepts, Network Architecture and Challenges", American Journal of Electrical and Electronic Engineering, vol.3, no.02, pp.22-28, 2015.

[38] H. Kilinc and T. Yanik, "A survey of sip authentication and key agreementschemes," IEEE Communications Surveys & Tutorials, vol. 16,no. 2, pp. 1005 – 1023, 2014.

[39] B.S.Sunil Kumar, A.S.Manjunath, S.Christopher,"Improved entropy encoding for high efficient video coding standard",Alexandria Engineering Journal, vol. 57, no. 1, pp. 1-9, March 2018.

[40] P. N. Kota , Dr. A.N. Gaikwad,"Optimized Scrambling Sequence To Reduce Papr In Space Frequency Block Codes Based MIMO-OFDM System",Journal of advanced research in Dynamical and control system, pp, 502-525, 2017.

[41] Bhatnagar, Kavita & Gupta, Subhash,"Extending the Neural Model to Study the Impact of Effective Area of Optical Fiber on Laser Intensity", International Journal of Intelligent Engineering and Systems, vol. no. 10(4), pp.274-283, 2017.

[42] GN Balaji, TS Subashini, N Chidambaram,"Detection of heart muscle damage from automated analysis of echocardiogram video",IETE Journal of Research vol. no 61 (3), 236-243.

[43] S. S. Bramhe, A. Dalal, D. Tajne and D. Marotkar, "Glass Shaped Antenna with Defected Ground Structure for Cognitive Radio Application," International Conference on Computing Communication Control and Automation, Pune, pp. 330-333,2015. https://doi.org/10.1109/ICCUBEA.2015.69

[44] KSSR Yarrapragada, BB Krishna,"Impact of tamanu oil-diesel blend on combustion, performance and emissions of diesel engine and its prediction methodology", Journal of the Brazilian Society of Mechanical Sciences and Engineering, 1-15.

[45] Ninu Preetha Nirmala Sreedharan, Brammya Ganesan, Ramya Raveendran, Praveena Sarala, Binu Dennis, Rajakumar Boothalingam R. "Grey Wolf optimisation-based feature selection and classification for facial emotion recognition", IET Biometrics, 2018.

[46] Amit Sarkar, T. Senthil Murugan, "Cluster head selection for energy efficient and delay-less routing in wireless sensor network", Wireless Networks, pp 1–18, 2017.

[47] AM Wagh, SR Todmal,"Eyelids, Eyelashes Detection Algorithm and Hough Transform Method for Noise Removal in Iris Recognition", International Journal of Computer Applications, vol. 112, no. 3, 2015.

[48] M Iyapparaja, M Tiwari, "Security policy speculation of user uploaded images on content sharing sites", IOP Conference Series: Materials Science and Engineering, vol. 263, no. 4, pp. 042019, 2017. https://doi.org/10.1088/1757-899X/263/4/042019