WALAILAK JOURNAL
Applied Sciences
http://wjst.wu.ac.th https://doi.org/10.48048/wjst.2021.8987

A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in MANET

Anubhuti Roda MOHINDRA* and Charu GANDHI

Department of Computer Science, Jaypee Institute of Information Technology, Noida, India

(*Corresponding author's e-mail: anubhuti.mohindra@jiit.ac.in)

Received: 26 September 2019, Revised: 17 June 2020, Accepted: 8 July 2020

Abstract

Providing security to the Mobile Ad-hoc Network (MANET) is one of the demanding and critical tasks in recent days, due to its dynamic nature. For this reason, the various routing protocols and security mechanisms are developed for the traditional networks. Nonetheless, it still lacks the limitation of increased computational complexity, inefficient security, reduced throughput, and increased delay. To solve these problems, this paper developed a new system, namely, Secure Cryptography based Clustering Mechanism (SCCM) for MANET. It comprised the following stages: secure routing, encryption, signature generation, signature verification, and decryption. After forming the network, the connection between the mobile nodes was formed. After that, the secured routing was created between the source and destination by implementing the AOMDV routing protocol. Then, the original packet was converted into an unknown format by employing an Elliptic Curve Cryptography (ECC) encryption mechanism. Consequently, the signature for the encrypted packet was generated and forwarded to the destination via the Region Head (RH) and other gateway nodes. When the destination node received the packet, it performed the signature verification process for verifying whether the packet is valid or invalid. If it were valid, the receiver would accept the data and decrypt it by using the ECC decryption mechanism; otherwise, it would reject the packet and report to the base station. The simulation results evaluated the performance of the proposed security mechanism by using various measures and compared it with other techniques for proving the superiority.

Keywords: Confidentiality, Elliptic Curve Cryptography (ECC), Message authentication, Mobile Adhoc Network (MANET), Secure Cryptography based Clustering Mechanism (SCCM), Schnorr's signature generation mechanism

Introduction

The Mobile Adhoc Network (MANET) is a self-organized system that contains a set of wireless nodes, where each node can act as a router or data transmission source [1]. This type of network does not require a pre-organized network infrastructure, which is deployed in uncontrolled or harsh environments [2]. Moreover, information sharing and distributed collaboration are the major operations of MANET. The major characteristics of a network are shared wireless medium, limited resources, physical vulnerability, and absence of fixed trusted infrastructure [3]. Due to the aforementioned proprieties, the MANET is highly susceptible to the demolition of malicious attacks. Besides, it does not have any centralized infrastructure for monitoring the operations of the node, which leads to node compromise and malfunctioning [4]. Hence, it is easy for the adversaries to launch the attacks on routing function and it hinders the normal communication of the network [5]. The MANET is used in the following applications: conferences, meeting events, battlefield communication, forest fire detection, etc. The general architecture of clustering based MANET is shown in **Figure 1**.

Figure 1 MANET of a smart device [6].

Problem statement

Due to the dynamic nature and distributed control of MANET, it is highly susceptible to attacks [7]. In the traditional security strategies, a trust based framework is offered by the central parties like Trusted Third Parties (TTP) [8]. It is responsible for creating the trusted relationships between the nodes in the network. Normally, the TTP acts like a Certification Authority (CA) that provides the certificates as the trusted indication for the public key authentication. Also, the trust-based relationship between the nodes is created to decide whether the communicating node is highly trusted or not [9]. In the clustering-based frameworks [10], the cluster head acts as a TTP or CA to provide secure communication in inter and intracluster routing [11]. To manage the cluster members in the group, the cluster head requires lightweight key management algorithms [12]. For this purpose, different algorithms are derived from the traditional mechanisms, but they lack in regards to increased computational complexity, network overhead, inefficient security, unreliability, and reduced network throughput [13]. To solve these problems, this paper aims to develop a new clustering-based security mechanism for improving the efficiency of a network.

Objectives

The major objectives of this paper are as follows:

- To ensure secure communication, message confidentiality is ensured at the sender side, and the message authentication is ensured at the receiver side.
- To detect the anonymous activity in inter and intracluster routing, a Secure Cryptography based Clustering Mechanism (SCCM) is developed in this work.
- To enable a secure routing path between source and destination, an Adhoc On-demand Multi-path Distance Vector (AOMDV) protocol is utilized.

Organization

The rest of the sections in the paper are organized as follows: The existing clustering related security frameworks and architectures for MANET are surveyed in section II. A clear description of the proposed methodology is presented with its detailed flow description in section III. The results of existing and proposed security mechanisms are validated and compared in section IV. Finally, the paper is summarized and the enhancement that can be implemented in the future are stated in section V.

Related works

In this section, the existing routing protocols, and cryptography mechanisms related to MANET security are discussed with their advantages and disadvantages.

Rafsanjani and Fatemidokht [14] designed a new routing protocol, namely, FBeeAdHoc for providing secure routing in MANET. Tis paper aimed to investigate the security vulnerabilities and threats against the network. Also, the fuzzy set theory was utilized in this work to identify and detect different types of threats in the network. The attacks that are considered in this work were scout related attacks, forager route related attacks, and forager route information related attacks. Moreover, both the node trust and route trust were evaluated by using the concept of fuzzy logic. However, it is required to improve the performance of the system by implementing the optimization algorithm. Chavan *et al.* [15] examined the performance of AODV and DSDV protocols for detecting the black hole attacks in MANET. In this paper, it was stated that the Ad-hoc On-demand Distance Vector (AODV) protocol outperforms the Destination Sequenced Distance Vector (DSDV) protocol by providing a better throughput, reduced delay, and increased packet delivery ratio. Chang *et al.* [16] developed a Cooperative Bait Detection Approach (CBDS) for detecting the malicious nodes in MANET. The suggested technique integrated the benefits of both proactive and reactive defense architectures. Also, a reverse tracing technique was utilized to detect the malicious nodes by using the bait destination address. The advantage behind this work was that it constructed a comprehensive security framework by protecting the MANET against miscreants. Vhora *et al.* [17] developed a Rank Base Data Routing (RBDR) scheme for detecting packet dropping attacks in MANET. The intention of this paper was to find the malicious routing paths and trusted loop-free routes during the packet transmission. The suggested technique used a record to analyze the malicious behavior of the nodes, which contains the fields of route rank, timer, routing paths, destination sequence number and hop count. However, it failed to prove the effectiveness of this system by evaluating different performance measures.

Cai *et al.* [18] developed a Group Mobility-based Clustering Algorithm (GMCA) to perform a secure routing in MANET. In this environment, the mobile node was selected as a cluster head that depends on the group of mobile nodes with similar mobility. Also, the Gauss-Markov model was utilized in this paper, which determined the node's movement in the network. Moreover, the velocity between the 2 nodes was estimated by using the mobility factor. However, this work required to improve the mobility metric by implementing an efficient clustering technique, which was the limitation of this work. Loutfi *et al.* [19] presented an energy-aware clustering algorithm for improving the lifetime of the MANET. Here, the number of cluster heads were selected by considering the measures of mobility and node density. Moreover, the Multi-Point Relays (MPRs) were used to reduce the network overhead in the same region with the use of link-state protocol. Here, the key factors of using this protocol were traffic controlling, efficient broadcasting, neighbor sensing, and shortest path calculation. In this paper, it was stated that the performance of the routing protocol was highly dependent on the mobility pattern that is transpiring in the network. Furthermore, 2 different scenarios such as the Random Waypoint Mobility model (RWP), and a fixed number of nodes were considered to evaluate the performance of the suggested technique. Yet, it is required to analyze the impact of differentiated traffic and overlapped clustering in the network.

Saxena *et al.* [20] designed a max-heap tree for enabling energy efficient routing in MANET. This paper intended to increase the lifetime of the network by splitting it into small and self-manageable groups. The cluster head was selected by the use of max-heap, which focused is to increase the scalability and energy metric of the network. The stages that are involved in this system design are general steps of multihop cluster-based protocol.

After forming the cluster, the energy level of each node was analyzed to select the cluster head by constructing the max heap. The disadvantage behind this approach was, it failed to prove the efficient performance of the suggested system. Morshed *et al.* [21] introduced a Cluster-Based Secure Routing Protocol (CBSRP) for enabling a secure routing in MANET. Here, the digital signature was generated to ensure secure communication between the nodes. Moreover, the authentication was enabled between the 2 nodes by using 1-way hashing technique. The cluster-to-cluster signature verification was performed to reduce the computation cost. The major considerations of this work were as follows:

- Designing a cluster model
- Cluster to cluster communication
- Hash key management
- Digital signature generation

The limitation of this work was, it does not use various measures to evaluate the performance of the suggested technique. Jhaveri [22] developed a Reliable AODV (R-AODV) protocol to detect and isolate the black hole and gray hole attacks in the network. Such attacks can disrupt the normal functionality of the network by forwarding bogus information. The suggested routing protocol intended to enable a secure route between nodes. This paper does not evaluate the R-AODV protocol by using some performance measures. Singh and Singh [23] implemented a clustering-based attack detection mechanism for providing security to MANET. Here, the communication nodes were selected based on the location, trust, energy, mobility, and throughput. Also, various clustering techniques such as Lowest Id Clustering (LIC), Highest Connectivity Clustering (HCC), Least Cluster Change (LCC), and Weighted Clustering Algorithm (WCA) were examined to select the most suitable technique. In this paper, it was stated that the clustering algorithm improved the network lifetime and transmission rate by efficiently detecting the malicious nodes in the group. But, this work failed to maintain the stability of the network by implementing an energy-efficient mechanism. Kulkarni and Yuvaraju [24] investigated the challenges and issues of clustering based security in MANET. Here, the trusted based security, and authentication base security mechanisms were estimated for enabling reliable communication in a network. Also, the cluster-based key management scheme was utilized to authenticate all the nodes in the network with the threshold signature. Furthermore, various clustering techniques were discussed with their advantages and disadvantages.

Kaur and Rao [25] implemented a key management scheme for improving the security of MANET with reduced mobility overhead. The main intentions of this work are as follows:

- Small calculations were performed to improve the network security.
- The allocation of resources was decreased to expand mobility.
- The key generation time was reduced with the increased network quality.

Here, the Chinese Remainder Theorem (CRT) was utilized to generate the key for removing the malicious nodes. Panke [26] developed a clustering-based certificate revocation scheme for identifying and detecting the attacks in MANET. In this environment, the nodes were classified into different categories, which include normal, warned, and attacker. Here, the Centralized Authority (CA) maintains the black and warning list for blocking the attacker nodes. If it detects the node as an attacker or warned, it added those nodes into the corresponding list. Moreover, the false accusation and false recovery were considered for detecting the node as an attacker. However, this paper has an increased computational overhead and reduced robustness. Prasanth and Sivakumar [27] implemented an energy-efficient geocast forwarding mechanism for increasing the security of MANET. Here, the common 3 tier security framework was used for performing the pairwise key establishment and authentication. The suggested protocol utilized the geographical information for efficiently forwarding the packets. Also, the multi-hopping scheme was utilized to route the data in a clustered manner. Nevertheless, this paper failed to improve the level of security by enabling efficient and reliable communication in the network. Kannan and Dinesh [28] used a Cluster-based Certificate Revocation with Vindication Capability (CCRVC) for identifying the attackers in MANET. Here, the cluster head identified the false accusation for revoking the certificate. This mechanism protected the legitimate nodes by maintaining the warned list and block list. Moreover, the node was classified as legitimate, malicious, and attacker by using the CCRVC mechanism. The advantage of this mechanism was, it reduced the revocation time by maintaining the legitimate nodes. However, it has increased computational complexity and overhead.

Satav *et al.* [29] had proposed a modified AOMDV routing table. The proposed structure consists of a path status parameter for labeling status of the path. Simulation result proves that proposed method offers numerous alternate reliable path for secure communication. This plan solves the effect of single

and collaborative black hole nodes. This method attains 100 % of PDR but there is increase in storage and computational cost. Alkhamisi and Buhari [30] to enhance network security, this research proposed Trusted based Secured Ad hoc On-Demand Multipath Distance Vector (TS-AOMDV) which depends on the routing behavior of nodes. TS-AOMDV aims at discovering and isolating attacks like a gray hole, black hole, and flooding attacks in MANET. With the support of trusted dependent routing and IDS (intrusion detection system), discovering and isolation of attack was performed in 2 steps such as Data forwarding and route discovery. IDS enables full routing security by monitoring data and control packets that involved in route discovering and data forwarding step. To enhance performance measures for routing, IDS combines measured statistics with AOMDV protocol for the prediction of attacks. This enables the proposed method to offer better routing performance and security in MANET. Makhlouf and Guizani [31] introduced an efficient and secure AOMDV routing protocol for vehicular communication. Security measures include the prediction of malicious vehicles and malicious behavior that aren't authenticated. To guarantee authentication and integrity for a route, replay packets were utilized to retrieve secure and best path. For node adjustment, RREP packets were utilized. The proposed method proves its efficiency in terms of average end-end delay for high-speed vehicle.

From the survey, the merits and demerits of both existing and proposed mechanisms are investigated, but the traditional clustering-based security mechanisms lack the following limitations:

- Reduced network performance
- Consumed a large amount of network bandwidth
- Unresolved security issues
- Gradually reduced number of nodes.

To solve these problems, this paper aims to develop a new clustering-based security mechanism for detecting the harmful attacks in MANET.

Materials and methods

In this section, a detailed description of the proposed methodology is presented with its flow illustration. The motive of this paper is to increase the security of MANET by implementing the signature generation and cryptographic mechanisms. The working procedure of the proposed SCCM system is illustrated in **Figure 2**, which has the following phases:

- Neighbor discovery
- Key generation
- Secure routing
- Packet encryption
- Signature generation
- Signature verification and decryption.

Originally, the network is designed with a varying number of mobile nodes, and the link between those nodes are created by sending the HELLO packets. Then, the location of each node is shared between the neighboring nodes to enable the secured data transmission. In this environment, the region is formed by grouping the mobile nodes into a cluster, in which the Region Head (RH) is elected based on its energy, bandwidth, mobility, and lifetime. Here, the region members register themselves to the RH, and the key generation and sharing processes are performed in each region. Once the service request is initiated, the secure routing path is established between the source and destination nodes. Before transmission, the original packet is encrypted into an unknown format by using the Elliptic Curve Cryptography (ECC) technique. After that, the signature is generated for the encrypted data by the use of schnorr's signature generation technique. Then, the encrypted packet is forwarded to the destination through the RH and other gateway nodes. When the destination receives the packet, it again regenerates the signature for decrypting the original data. During this process, the proper verification is performed, if the received is correct, the destination can accept it; otherwise, it discards the message and it reports to

the base station. The major advantages of this system are, it enabled both message confidentiality and authentication.

Region head selection

After discovering the neighbors, the region [32] is formed by grouping the nodes as clusters for improving the routing performance in the network. It increases the data transmission rate and reduces the communication overhead in the network. In a region, a node serving as a local coordinator is selected as RH and the remaining nodes operate as member nodes. In the proposed work, one-hop regions are formed so that the nodes are located proximate to the RH.

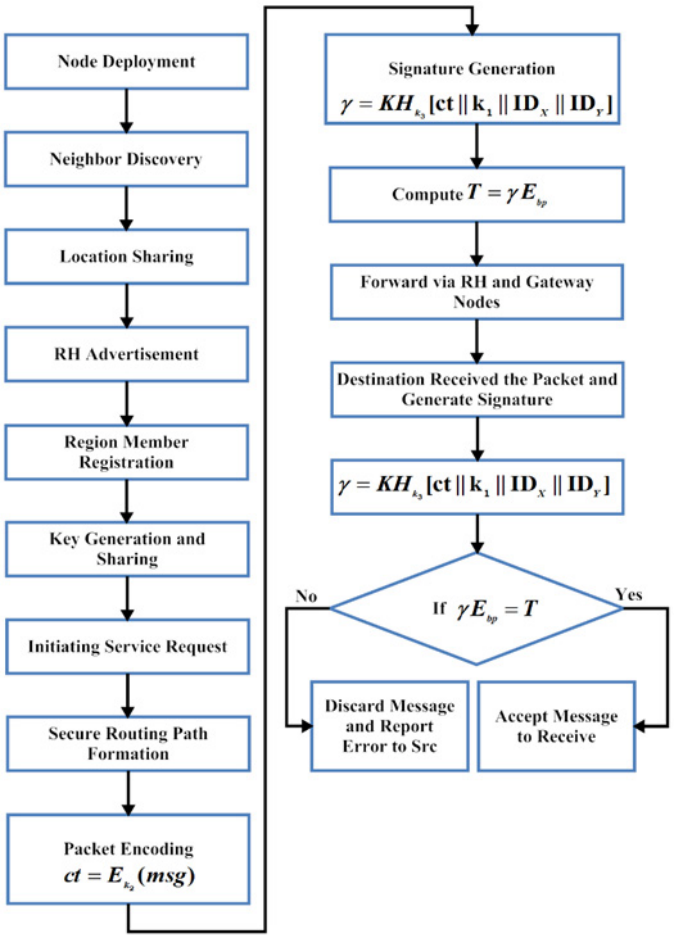

Figure 2 Flow of the proposed system.

The Algorithm I - RH selection procedure

Step 1: The source node initiates communication by transmitting the Hello packet to detect the neighbor node Identity (ID).

Step 2: One hop neighbors send a reply after receiving the Hello packet. When the neighbor ID is detected, the status of the neighbor node is checked.

Step 3: Check the status of the neighbor node only if the neighbor node is located within the cluster range. Otherwise, the nodes are not reachable.

Step 4: After the selection of nodes, check the relay factor of the selected neighbor and calculate the link status of the node.

Step 5: Then, check the signal status for the selected neighbor nodes.

Step 6: Check the energy level for the selected neighbor nodes.

Step 7: Check the mobility of all selected nodes.

Step 8: Finally send the acknowledgment to RH.

Step 9: When the weight value of RH is reduced from the threshold value, the RH is re-elected.

Step 10: Finally, update and activate the RH.

Secure data routing

In this work, the AOMDV protocol is used to perform the secure routing between the source and destination. Here, an alternate path is selected during data transmission, only if there is any fault or failure like a blackhole attack found in the selected path. A blackhole attack is a kind of DDoS attack which performs packet dropping activity. Due to this kind of malicious activity routing overheads are increased. In such cases, the protocol uses the alternate path for further transmission. It efficiently avoids the data loss and end-to-end delay of the network by computing multiple loops free and link disjoint paths. This type of protocol is specifically designed for the highly dynamic ad-hoc networks, where the route breaks and link failures are frequent. Also, it uses the route update rule for establishing and maintaining the fault-free and multiple paths between the sender and receiver nodes. In this environment, 2 different types of path disjoint mechanisms such as node disjoint and link disjoint are utilized. In which, the node disjoint mechanism has only the path between source and destination, and the link disjoint mechanism has some common nodes, but it does not have any common links. Moreover, it selects a common path based on the time of routing by building multiple paths. AOMDV multipath algorithm attains and resolve blackhole attack issue by choosing an alternate route. The purpose for utilizing AOMDV are:

- Least inter-nodal organization overheads in AOMDV.
- Numerous are disjoint.
- The whole path is disjoint and loop-free.
- There is no need to find a new route.
- Reactive routing protocol establish the path only if there is a need to transmit a packet to a neighborhood.
- AOMDV chooses the only ideal path from the existing path.
- Selection of optimal path depends on less congested path and nearest path property.

Secure route selection

The routing structure of AOMDV includes various parameters, such as IP address for destination node, a sequence number for destination node, hop count, path list, and expiration route. Path list includes IP for next hop, hop_count_1, path_status, Launch_time.

Algorithm II - Secure route selection

Step 1: Form a mobile ad-hoc network with sufficient N nodes.

Step 2: Proposed SCCM routing protocol is designed with an additional parameter.

Step 3: Source node checks availability first and reliable updated path availability from the routing table.

$if\ (P_s == R_P \quad \&\& \quad PCT == current)$

{

- Choose the path from the routing table
- Send the packet through that selected path

}

else

{

- Perform route finding process for reliable path

}

Step 4: Forming, verifying, and updating the reliability of all the paths for single/multiple cooperative black hole attack detection on the trajectory.

$for(\ i := 1 : i < P_L; i++)$

{

$PR_V(pat(i))$

}

A dummy packet is sent from source to destination node to validate and update trajectories status.

$If\ (ACK_{received}\ == Yes)$

{

update P_s as a reliable path

}

else

{

update P_s as an unreliable path

}

Step 5: SCCM chooses the most reliable and secure path among the existing path.

$PR_V -$ validation of the reliability of the path

$P_L -$ path list

PCT – Path creation time

$P_s -$ path status

R_P – Reliable path

$ACK_{received}$ acknowledgment received from source to destination

Encryption

After establishing the secured path between the source and destination, the ECC technique is implemented to encrypt the original data into an unknown format. It is one of the widely used cryptographic techniques in network security, which offers fast computation and reduced resource consumption. Also, this technique establishes equivalent security with minimized cost. The strength of this algorithm is, it fully depends on the key and alphabetical table. Also, it provides a better solution for the data by enabling the secure transmission of keys between the communicating entities. Furthermore, different characteristics are symbolized in this technique as the coordinates of the curves. The group of the structure of ECC is formed by the curve that has a finite number of integer points with determinate points. In this work, the main reason for using ECC encryption is, it creates complexity in the encrypted data, so the unauthenticated user cannot easily access the data.

Signature generation

After encrypting the data, the schnorr's signature generation algorithm is utilized to generate the signature for the encrypted data. It is a kind of key generation mechanism that integrates both digital signature schemes and public-key encryption schemes. It analyzes the discrete logarithmic problem for generating the digital signature, which increases the security of the network. This signature generation has the following steps:

- Setup
- Key generation at the sender side
- Key generation at the receiver side
- Signcryption
- Unsigncryption

In this technique, the source verifies the public key of the packet by using the certificate. Then, the integer is randomly selected, based on this the keys that are used for generating the ciphertext are computed. Also, the one-way keyed hash function is utilized to generate the encrypted text, and it is forwarded to the destination with the generated signature. The working procedure of ECC based encryption and signature generation algorithms are illustrated as

Algorithm III - Encryption and signature generation

Step 1: Source verifies the public key of Py by using its certificate;

Step 2: *Randomly select an integer* v, *where* $v \geq P_O$

Step 3: *Compute* $k_1 = hash(vE_{bp})$

Step 4: *Compute* $(k_2, k_3) = hash(vPy)$

Step 5: *The symmetric encryption algorithm is used to generate cipher text* $ct = E_{k_2}(msg)$

Step 6: *Use the one-way keyed hash function to generate,* $\gamma = KH_{k_3}[ct \,||k_1\, ||ID_X||ID_Y)$

Step 7: *Computes* $s = \frac{v}{\gamma + v_x} mod\ p$

Step 8: *Compute* $T = \gamma E_{bp}$

Step 9: *Sends the signature added ciphertext* (ct, T, s) *to the receiver;*

Signature Verification and Decryption

After receiving the data by the destination, the packet can be decrypted by using the ECC decryption technique. Also, it regenerates the signature by using the same schnorr's key generation algorithm. During this process, the verification is performed to ensure that the packet is valid or not. If it is valid, the receiver can accept the data; otherwise, it rejects and reports to the base station.

Algorithm IV - Signature verification and decryption

//The destination receives the encrypted and signed text (ct, T, s), based on this it decrypts the ciphertext 'ct' by performing a decryption algorithm with secret key k. It also verifies the signature.

Step 1: Verifies source's public key Px by using its certificate.

Step 2: Computes $k_1 = \text{hash}(sT + sPx)$

Step 3: Computes $(k_2, k_3) = \text{hash}(v_y sT + v_y sPx)$

Step 4: Uses the one-way keyed hash function to generate $\gamma = KH_{k_3}[ct || k_1 || ID_X || ID_Y)$

Step 5: Uses a decryption algorithm to generate plain text $m = D_{k_2}(c)$

Step 6: Destination accepts the message 'm', if $\gamma E_{bp} = T$.

Otherwise, it rejects the message.

$k_1 = \text{hash}(sT + sPx)$

$\gamma = KH_{k_3}[ct || k_1 || ID_X || ID_Y)$

Accept m if and only if $\gamma E_{bp} = T$

The key benefits of this work are as follows:

- Increased network throughput and security
- Reduced latency
- Highly efficient

Results and discussion

In this section, the performance of existing and proposed security mechanisms are evaluated by using various performance measures that include control packet overhead, Packet Delivery Ratio (PDR), average end-to-end delay, False Acceptance Rate (FAR), and throughput. The existing techniques [28] considered in this analysis are Flooding Factor-based Trust Management (F3TM) [33], Cooperative Opportunistic Routing in MANET (CORMAN) [34], and Protocol for Routing in Interested-defined Mesh Enclaves (PRIME) [35]. Here simulation was carried out on NS2 2.29 network simulator, a broadly utilized simulator across the world with open source code. With plentiful component libraries, NS2.29 simulate protocols of MANET, mobile wireless network, etc. result generated by NS2.29 is considered broadly as veracious and acceptable. This is the main reason to choose NS2.29. The simulation settings of the proposed environment is depicted in **Table 1**.

Table 1 Experimental settings.

Parameters	Value
Simulation time	100 s
Topology size	1,200 × 1,000 m²
Number of nodes	> 100
Pause time	3 - 5 s
Max speed	10 m/s
Traffic type	CBR
Packet size	1,024 bytes
Wireless channel capacity	2Mbps
Routing protocol	Modified AOMDV
Transmission range	< 250 m (thresh 150 m)
Mobility model	Random waypoint
Wireless standard	802.11b

Control packet overhead

The control packet overhead is defined as the ratio of the total number of generated control packets to the total number of the received data packets by the node in the network. It is also termed as the amount of time required to transfer the message or data by the node. It is estimated based on the functions of link maintenance, latency, and node discovery. It is calculated as follows:

$$Control\ Packet\ Overead = \frac{Control\ Packets\ Generated}{Data\ Packets\ Received} \quad (1)$$

Typically, the generated control packets and received data packets are helpful to find the overhead ratio of the network. Based on this, the attacker's presence in the network is identified and blocked. **Figure 3** evaluates the control packet overhead of both existing and proposed protocols concerning the number of attackers. When compared to the other techniques, the proposed SCCM efficiently reduced the control packet overhead with the decrease in generated control packet and an increase in received data packets by transferring the message based on RH selection.

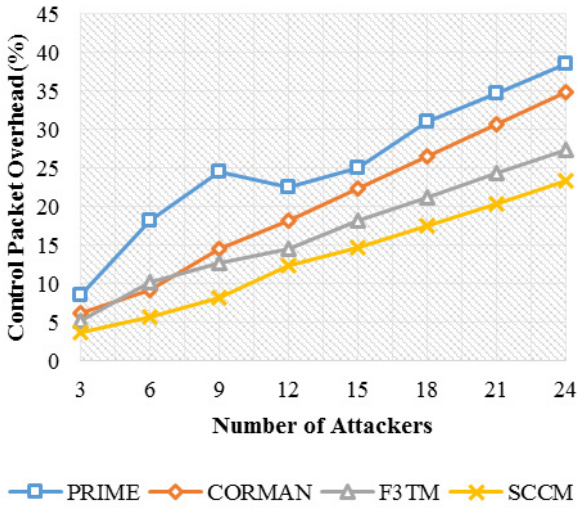

Figure 3 Control packet overhead [33].

Packet delivery ratio

The PDR is estimated based on the fraction of the number of packets that are transmitted by a traffic source and the number of packets received by a traffic sink. Also, it is used to evaluate the efficiency and correctness of the routing protocols by estimating the loss rate. **Figures 4** and **5** show the PDR of the existing and proposed protocols for the number of attackers and number of nodes. The PDR is calculated as follows,

$$PDR = \frac{Received\ Packets}{Transmitted\ Packets} * 100 \quad (2)$$

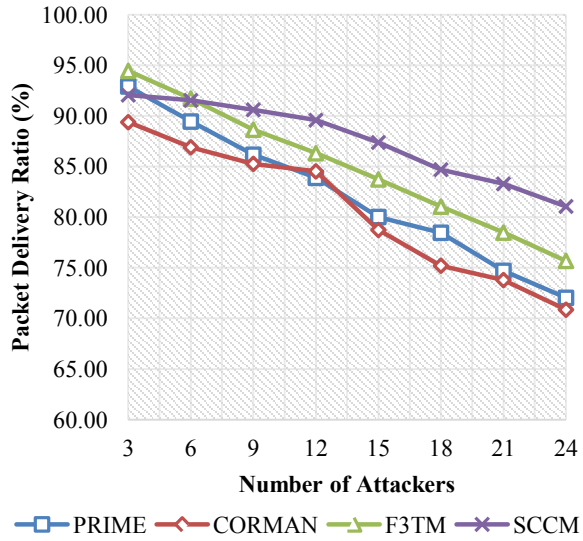

Figure 4 PDR vs the number of attackers [33].

From the evaluation, it is observed that if the number of attackers in the network can increase, the PDR of the network can be decreased. When compared to the other techniques, the proposed SCCM provides a better PDR by efficiently blocking the attackers in the network. Also, the AOMDV uses multiple paths for forwarding the packets, if there is any failure in the current, it uses an alternate path for further communication, which increased the PDR.

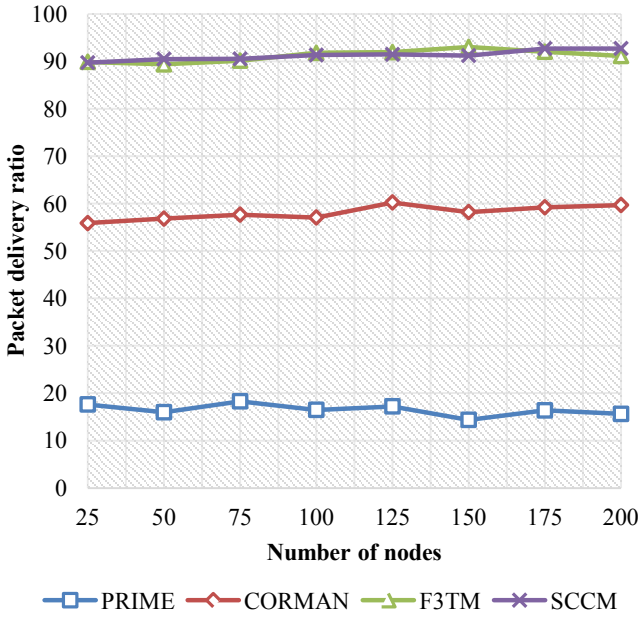

Figure 5 PDR vs the number of nodes [33].

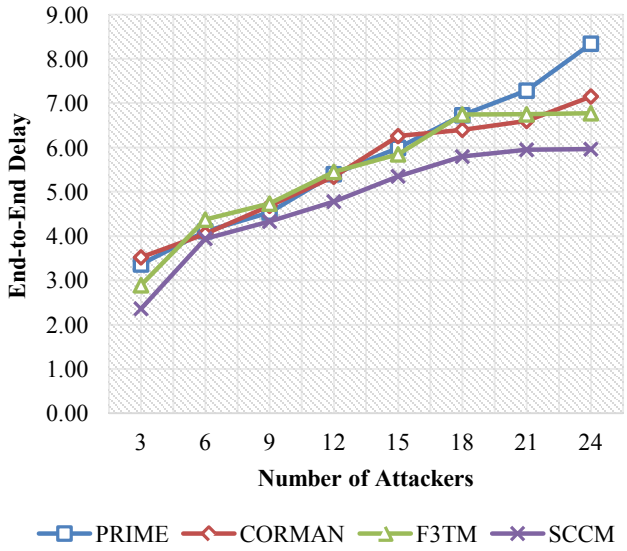

Figure 6 Average end-to-end delay vs the number of attackers [33].

Average end-to-end delay

Average delay is defined as the required amount of time that a packet takes to travel from the source to the destination. It is estimated as follows:

$$Transmission\ delay = \frac{Sum\ of\ all\ packets\ delay}{Total\ number\ of\ received\ packets} \quad (3)$$

Figures 6 and **7** shows the transmission delay of both existing and proposed protocols for the number of attackers and number of nodes. In this analysis, it is proved that the proposed SCCM provides a minimum transmission delay when compared to the other techniques. Because, in the proposed environment, each routing path contains some transmission medium like a gateway, which is used to direct the packets based on the properties of nodes.

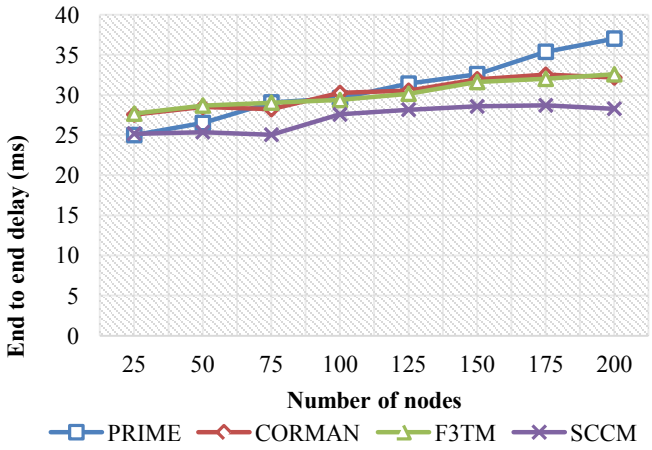

Figure 7 End to end delay vs the number of nodes [33].

False acceptance rate

False Acceptance Rate (FAR) is defined the false positive proportion that represents how many nodes are misidentified as attackers. If the algorithm has a lower false-positive rate, it will give better performance. The FAR is calculated as follows,

$$FAR = \frac{number\ of\ onest\ users\ misidentified}{number\ of\ nodes\ identified\ as\ attackers} \quad (4)$$

Figure 7 shows the FAR of both existing and proposed techniques, concerning the varying simulation time. From this analysis, it is evaluated that the proposed technique high detection rate, when compared to the other techniques.

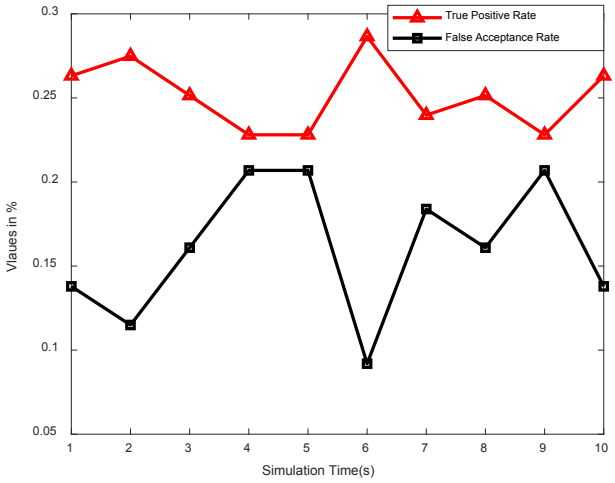

Figure 8 False acceptance rate.

Throughput

The throughput is defined as the average rate of successful data delivery over the communication channel. **Figure 8** shows the analysis of throughput for both existing and proposed methods for the number of attackers. The throughput of the network is calculated as follows:

$$Trougput = \frac{Number\ of\ data\ packets\ recceived\ (bits)}{Simulation\ time\ period\ (secs)} \quad (5)$$

During this calculation, the time window is estimated for measuring the throughput based on the successfully delivered packets per unit of time. In this evaluation, it is proved that the proposed SSVC technique has increased throughput when compared to the other techniques.

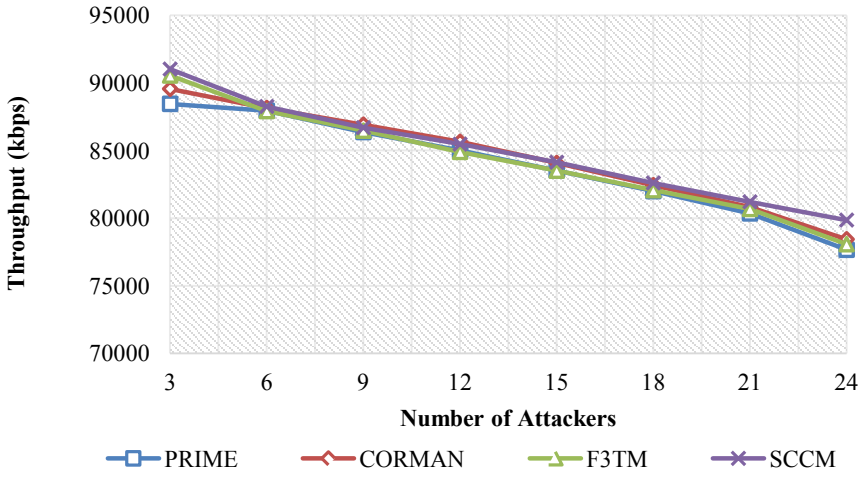

Figure 9 Throughput [33].

Conclusions

This work proposed an efficient mechanism, namely, SCCM for providing security to MANET with increased throughput. Message confidentiality and message authentication are the major considerations of this work. Here, the AOMDV routing protocol is used to select multiple paths during transmission to avoid packet loss and reduce the delay. Then, the ECC based encryption mechanism is utilized to encrypt the original packet before transmitting it to the receiver. Also, the Schnorr algorithm is employed to generate the signature for the encrypted data, which improves privacy. Once the destination receives the packet, it verifies whether the packet is valid or not. If it is valid, it regenerates the signature using the Schnorr algorithm and applies the ECC decryption mechanism for decrypting the data. During the simulation, various performance measures are used to test the results of the proposed SCCM technique. Moreover, some of the existing techniques are compared with the proposed technique for proving the efficacy. From the examination results, it is illustrated that the proposed SCCM provides better results compared to the other techniques.

Future work

In the future, this effort can be enhanced by considering the energy conservation of the network.

References

[1] JG Ponsam and R Srinivasan. A survey on MANET security challenges, attacks and its countermeasures. *Int. J. Emerg. Trends Tech. Comput. Sci.* 2014; **3**, 274-9.
[2] MM Alani. MANET security: A survey. *In*: Proceedings of 2014 IEEE International Conference on Control System, Computing and Engineering, Batu Ferringhi, Malaysia. 2014, p. 559-64.
[3] K Dhanalakshmi, B Kannapiran and A Divya. Enhancing manet security using hybrid techniques in key generation mechanism. *In*: Proceedings of 2014 International Conference on Electronics and Communication Systems, Coimbatore, India. 2014, p. 1-5.
[4] R Mohandas and K Krishnamoorthi. MANET security betterment by enhanced multiple key management scheme. *Wireless Pers. Comm.* 2017; **94**, 2173-88.
[5] SD Mohanty, V Thotakura and M Ramkumar. An efficient trusted computing base for MANET security. *J. Inform. Secur.* 2014; **5**, 192.
[6] T Alam. Middleware implementation in cloud-MANET mobility model for internet of smart devices. *Int. J. Comput. Sci. Netw. Secur.* 2017; **17**, 86-94.
[7] P Nikam and V Raut. Improoved MANET security using Elliptic curve cryptography and EAACK. *In*: Proceedings of 2015 International Conference on Computational Intelligence and Communication Networks, Jabalur, India. 2015, p. 1125-9.
[8] D Dawoud, L Richard, S Ashraph, S Kasmir and V Raja. *Trust establishment in mobile ad hoc networks: Key management.* Mobile Ad Hoc Networks: Application. *In:* X wang (Ed.). In Tech, Shanghai, 2011, 153-93.
[9] R Agrawal and S Sahu. Secured routing over manet using Enhanced Secured Routing (ESR). *In*: Proceedings of 2013 International Conference on Control, Computing, Communication and Materials, Allahabad, India. 2013, p. 1-6.
[10] RS Shaktawat, D Singh and N Choudhary. An efficient secure routing protocol in MANET Security-Enhanced AODV (SE-AODV). *Int. J. Comput. Appl.* 2014; **97**, 34-41.
[11] MK Nazir, RU Rehman and A Nazir. A novel review on security and routing protocols in MANET. *Comm. Netw.* 2016; **8**, 205-18.
[12] R Singh, P Singh and M Duhan. An effective implementation of security based algorithmic approach in mobile adhoc networks. *Hum. Cent. Comput. Inform. Sci.* 2014; **4**, 7.
[13] N Shukla, S Gupta and A Virmani. Mobile Ad-Hoc Network (MANET): Security issues regarding attacks. *Int. J. Comput. Appl.* 2013; **975**, 8887.
[14] MK Rafsanjani and H Fatemidokht. FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs. *AEU Int. J. Electron. Comm.* 2015; **69**, 1613-21.

[15] A Chavan, D Kurule and P Dere. Performance analysis of AODV and DSDV routing protocol in MANET and modifications in AODV against black hole attack. *Proc. Comput. Sci.* 2016; **79**, 835-44.
[16] JM Chang, PC Tsou, I Woungang, HC Chao and CF Lai. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Syst. J.* 2014; **9**, 65-75.
[17] S Vhora, R Patel and N Patel. Rank Base Data Routing (RBDR) scheme using AOMDV: A proposed scheme for packet drop attack detection and prevention in MANET. *In*: Proceedings of 2015 IEEE International Conference on Electrical, Computer and Communication Technologies, Coimbatone, India. 2015, p. 1-5.
[18] M Cai, L Rui, D Liu, H Huang and X Qiu. Group mobility based clustering algorithm for mobile ad hoc networks. *In*: Proceedings of 2015 17th Asia-Pacific Network Operations and Management Symposium, Busan, South Korea. 2015, p. 340-3.
[19] A Loutfi, M Elkoutbi, JB Othman and A Kobbane. An energy aware algorithm for OLSR clustering. *Ann. Telecomm.* 2014; **69**, 201-7.
[20] M Saxena, N Phate, K Mathai and M Rizvi. Clustering based energy efficient algorithm using max-heap tree for MANET. *In*: Proceedings of the 4th International Conference on Communication Systems and Network Technologies, Bhopal, India. 2014, p. 123-7.
[21] MM Morshed and MR Islam. CBSRP: Cluster based secure routing protocol. *In:* Proceedings of the 3rd IEEE International Advance Computing Conference, Ghaziabad, India. 2013, p. 571-6.
[22] RH Jhaveri. MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based MANETs. *In*: Proceedings of the 3rd International Conference on Advanced Computing and Communication Technologies, Rohtak, India. 2013, p. 254-60.
[23] M Singh and G Singh. A secure and efficient cluster head selection algorithm for MANET. *J. Netw. Comm. Emerg. Tech.* 2015; **2**, 49-53.
[24] SB Kulkarni and BN Yuvaraju. Challenges and Issues of Cluster Based Security in MANET. *IOSR J. Comput. Eng.* 2016*;* **18**, 1-5.
[25] I Kaur and A Rao. A framework to improve the network security with less mobility in MANET. *Int. J. Comput. Appl.* 2017; **167**, 10-24.
[26] T Panke. Clustering based certificate revocation scheme for malicious nodes in MANET. *Int. J. Sci. Res. Publ.* 2013; **3**, 1-5.
[27] K Prasanth and P Sivakumar. Energy efficient improvement geocast forwarding in manet based on a clustered structure. *J. Eng. Sci. Tech.* 2015; **10**, 1224-38.
[28] G Hahn, T Kwon, S Kim and J Song. *Cluster-based certificate chain for mobile ad hoc networks*. *In:* Proceedings of the 2006 Computational Science and Its Applications. Springer, Berlin, 2006, p. 769-78.
[29] PR Satav, PM Jawandhiya and VM Thakare. Secure route selection mechanism in the presence of black hole attack with AOMDV routing algorithmin. *In*: Proceedings of 4th International Conference on Computing Communication Control and Automation, Pune, India. 2018, p. 1-6.
[30] AO Alkhamisi and SM Buhari. Trusted secure adhoc on-demand multipath distance vector routing in MANET. *In*: Proceedings of the IEEE 30th International Conference on Advanced Information Networking and Applications, Crans-Montana, Switzerland. 2016, p. 212-9.
[31] AM Makhlouf and M Guizani. SE-AOMDV: Secure and efficient AOMDV routing protocol for vehicular communications. *Int. J. Inform. Secur.* 2019; **18**, 665-76.
[32] AR Mohindra and C Gandhi. An energy-efficient clustering approach for collaborative data forwarding in heterogeneous MANET. *Int. J. Comm. Syst.* 2017; **30**, e3366.
[33] MN Ahmed, AH Abdullah, H Chizari and O Kaiwartya. F3TM: Flooding factor based trust management framework for secure data transmission in MANETs. *J. King Saud Univ. Comput. Inform. Sci.* 2017; **29**, 269-80.
[34] Z Wang, Y Chen, and C Li. CORMAN: A novel cooperative opportunistic routing scheme in mobile ad hoc networks. *IEEE J. Sel. Area. Comm.* 2012; **30**, 289-96.

[35] R Jaiswal and S Sharma. Relative cluster entropy based wormhole detection using AOMDV in adhoc network. *In*: Proceedings of the 4th International Conference on Computational Intelligence and Communication Networks, Mathura, India. 2012, p. 747-52.