Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.028425
Article

Tech Science Press

A Collaborative Approach for Secured Routing in Mobile Ad-Hoc Network

W. Gracy Theresa[1,*], A. Gayathri[2] and P. Rama[3]

[1]Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, 600123, Tamil Nadu, India
[2]Department of Information Technology, Vellore Institute of Technology, Vellore, 632014, Tamil Nadu, India
[3]Department of Computer Science and Engineering, Loyola Institute of Technology, Chennai, 600123, Tamil Nadu, India
*Corresponding Author: W. Gracy Theresa. Email: sunphin.new@gmail.com
Received: 09 February 2022; Accepted: 15 March 2022

Abstract: Mobile computing is the most powerful application for network communication and connectivity, given recent breakthroughs in the field of wireless networks or Mobile Ad-hoc networks (MANETs). There are several obstacles that effective networks confront and the networks must be able to transport data from one system to another with adequate precision. For most applications, a framework must ensure that the retrieved data reflects the transmitted data. Before driving to other nodes, if the frame between the two nodes is deformed in the data-link layer, it must be repaired. Most link-layer protocols immediately disregard the frame and enable the high-layer protocols to transmit it down. In other words, because of asset information must be secured from threats, information is a valuable resource. In MANETs, some applications necessitate the use of a network method for detecting and blocking these assaults. Building a secure intrusion detection system in the network, which provides security to the nodes and route paths in the network, is a major difficulty in MANET. Attacks on the network can jeopardize security issues discovered by the intrusion detection system engine, which are then blocked by the network's intrusion prevention engine. By bringing the Secure Intrusion Detection System (S-IDS) into the network, a new technique for implementing security goals and preventing attacks will be developed. The Secure Energy Routing (SER) protocol for MANETs is introduced in this study. The protocol addresses the issue of network security by detecting and preventing attacks in the network. The data transmission in the MANET is forwarded using Elliptical Curve Cryptography (ECC) with an objective to improve the level of security. Network Simulator – 2 is used to simulate the network and experiments are compared with existing methods.

Keywords: Mobile ad-hoc network (MANET); intrusion detection system; secure energy routing (SER); elliptical curve cryptography (ECC); security

1 Introduction

Mobile Ad-hoc Networks (MANETs) [1] are the communication technologies of the future. MANETs are self-contained networks that do not require any infrastructure to connect. However, if a fixed infrastructure network is present, MANETs can use it to communicate with other devices. As a result of

its cost-effective wireless networking technology and ability to provide mobility anytime and anywhere, the development of mobile ad-hoc networks has accelerated. A MANET is defined by the number of interconnected nodes. If the nodes in the setup are within the coverage area, they communicate with one another. With no fixed infrastructure, a mobile computer device can move in any direction across the coverage area of radio links. Developing applications over MANETs has become possible as the limited range of wireless technologies for mobile computing devices has improved. MANET apps calculate network operations remotely, and their use has increased significantly due to their versatility and self-configuration. Mobile Ad-hoc Networks are self-configuring networks using pre-installed infrastructure. The combination of enhanced processing and communication techniques has opened up a slew of new possibilities for ad-hoc network development. Many software and hardware designs have resulted in various services, but they fail to guarantee security since ad hoc networks lack firewalls and suitable data protection capabilities. Multiple assaults, ranging from selfish to malicious nodes, are vulnerable to the networks [1]. Attacks on wireless networks can be divided into two types: greedy and malicious. Solitary attacks in the networks relate to node non-cooperation in data transmission. This lack of cooperation from the nodes causes the system to rebroadcast the data, consuming additional energy from the nodes in a network. Malicious assaults in the network relate to failure to follow the protocol structure. A malicious attack is when a hacked node is used for nefarious purposes. The difficulties include creating a Secured Intrusion Detection System and deploying nodes to deal with all of these attacks in real time while maintaining network security. MANETs have no fixed architecture due to excessive node mobility, interference, and path loss. As a result, they require a dynamic routing protocol to function properly. MANET has deployed a number of intrusion detection systems based on routing protocols, assuming that no node in the network breaches the protocol's normal functioning and that the nodes fail to defend themselves against attacks by any selfish or malevolent node [2]. A reactive routing system is designed in this proposed work to establish stable Secure-Intrusion Detection System (S-IDS) for nodes. The data transmission routing paths in this proposed security algorithm must be the shortest paths, and the protocol should use less energy when transmitting information, as well as solve security concerns in MANETs. S-IDS will be developed, and the Securing Energy Routing (SER) protocol [3] will be implemented for MANETs, according to the suggested work goals. Each mobile node's energy usage must be divided evenly in the protocol, and energy for each route should be decreased to maximize the network path's lifespan. The proposed ECC-based IDS [4] technique keeps track of the routing information, as well as the intermediate node that receives the data and its next hop. It captures information from the attacker, sends it to the network, and protects future involvement. The protocol is intended to investigate and mitigate the consequences of separate network attacks including black hole attacks. The protocol then assesses the impact of each of these attacks on network efficiency.

This research work article is structured such that the research is based on current research works in Section 2, which defines the research objectives. Section 3 illustrates the proposed methodology, followed by Section 4 with performance analysis and discussion. In Section 5, the proposed research work was concluded with a glance into the prospective improvements.

2 Literature Survey

MANET has a range of design shortcomings in real time. One of the major issues in wireless networks is the routing strategy used by MANETs. MANETs are vulnerable to cyber-attacks as they lack network management services due to lack of network architecture and the centralized access point. Since no preceding stable policies have been implemented, the network nodes must band together to maintain the network service. MANETs are extremely demanding in terms of creating these security measures in place at network nodes [5]. For the infrastructure types of networks, security policy methods have been defined. However, applying this regulation in MANET's implementations is a difficult task.

A novel CL-KESC construction model based on Hyperelliptic Curve Cryptography (HECC) [6] was proposed by Khan et al. (2020). The HECC is a more advanced version of the elliptic curve, with reduced parameter and key sizes. In contrast to the elliptic curve, which requires a key size of 160 bits, the key size can be as small as 80 bits. The proposed technique was found to be superior, particularly in terms of security and performance, as evidenced by the results of the security verification and a comparative analysis of existing counterparts.

Burhan et al. (2020) developed a model that uses game theory's potential modelling [7] component to describe the multiple-collusion attacker situation. It helps with modelling of regular/malicious node tactics and (ii) formulating optimal strategies using optimization principles and unique auxiliary information. The model improves the ability of each normal node, i.e., malevolent node, to perform precise computations on the opponent player's strategy forecast. The simulation results of the proposed mathematical model in MATLAB show that it outperforms the baseline approach in game theory.

Ningrinla et al. (2016) developed an IDS model [8] that reduces the active time of IDSs while maintaining their effectiveness. Researchers characterize the interactions between IDSs as a multiplayer cooperative game in which the players have partially cooperative and partially opposing objectives to validate our suggested strategy. This game is theoretically analyzed and supported by simulation findings.

Suganthi et al. (2021) proposed a new Trust-based Efficient Energy Balanced Less Loss Routing (TER) Protocol [9] for MANETs. By selecting the right intermediate forwarding nodes, this protocol enhances network performance. Using the Efficient Parameter, the Source Node selects only one of its neighbor's as its next hop node (EP). The EP is calculated using the node's remaining energy, distance, Occupied Queue space, and velocity. The node with the most EP is chosen as the subsequent node. This protocol minimizes the quantity of channeling messages, lowering the network's path-finding overhead.

A secure lightweight backbone building strategy [10] was developed by Gauravand et al. (2021). For safeguarding the backbone network, the author used a lightweight distributed strategy, which allows our suggested solution to detect numerous existing attacks without exhausting the nodes' resources.

Bismin et al. (2021) proposed a distinctive method [11] called Chimp-CoCoWa-AODV that merges both Ad-hoc On-Demand Distance Vector (AODV) protocol coupled with chimp optimization algorithm and Collaborative Contact based Watchdog to enhance MANET performance.

The recent research results based on the security aspect of the Mobile Ad-Hoc Network (MANET) had provided diversified range of aspects. The recent researches had concentrated on the particular attacks and some methodologies experiences a major hike in the communication overhead with an objective to provide high level of security in the routing process. Based on the aforementioned study results, the following objectives were framed for the development of the proposed system with a general motive of providing high level of security to the data in the MANET.

- To design a Secure-IDS (S-IDS) system that addresses the concerns related to the establishment of secured path between the MANET nodes.
- To design an IDS system to communicate the data between nodes in a secured manner.
- To develop security scheme using Elliptical Curve Cryptography (ECC) to mitigate the security concern raised due to the selfish/malicious node.

3 Proposed Work

The security concerns in MANET must be resolved by constructing a secure intrusion detection system that addresses issues such as a secure path to nodes for data transmission, minimal node energy consumption, and the development of security schemes [12] that can deal with selfish and malicious attacks on network

nodes. The MANET's intrusion detection system scheme has not been fully deployed. In contrast to wired and wireless networks, the Secure Intrusion Detection System (S-IDS) algorithm has an unique infrastructure and architecture. Since there is no architecture in MANET, node attacks in the networks are unharmed, posing a threat to the S-IDS design requirement. Once all nodes in the network participate in data transmission does the S-IDS achieve great efficiency, and the algorithm eliminates attacks from malevolent nodes.

Fig. 1 illustrates the MANET architecture with the source and destination node, neighbor nodes, and malicious node to illustrate the scenarios for the requirements of the secure intrusion detection system. The S-IDS must take path computation into account as well as provide node protection. When going through the network, the S-IDS algorithm seeks to discover the most efficient and accurate way to sink nodes. Minimum energy usage in the network should also be considered while locating nodes on the shortest paths. This protocol [13] may enable many paths; if one route path malfunctions for any cause, the data will still be transferred to the intended destination within the network via an alternate path. The S-IDS should be created for MANETs to detect suspicious nodes on the network, unless they have been first detected in the network. Malicious nodes lead to network packet loss, as shown in Fig. 2, and the S-IDS must inhibit this node from moving along the network through the data transmission path. The SER protocol implementations in the S-IDS system [14] upgrades node information in a timely manner to protect the nodes in the setup from various types of assaults and keep hostile nodes out of the network's route path.

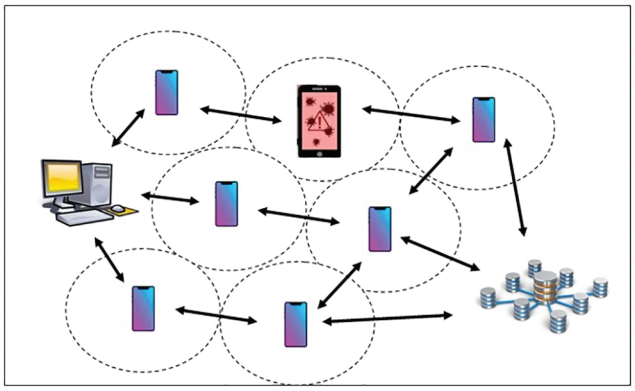

Figure 1: Secured mobile ad-hoc network model

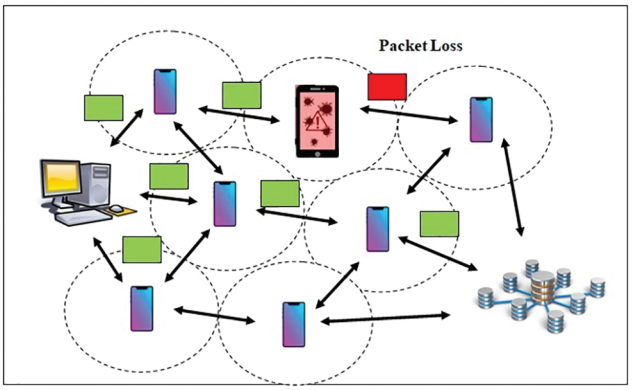

Figure 2: Packet loss due to malicious node in MANET

The Intrusion Detection System (IDS) model is intended to identify attacks and prevent them from occurring by raising an alarm in MANET. Mobile nodes, training datasets, packet analyzers, threshold valves, and attack categorization [15] are all part of the S-IDS paradigm. A node in a MANET tends to travel in any route and sends data in the network; the data transfer causes traffic in the network, and the likelihood of being attacked by an intruder is significant in these instances. To address this problem, the S-IDS model as shown in Fig. 3 is useful since it includes detection and prevention engines that help to minimize network threats.

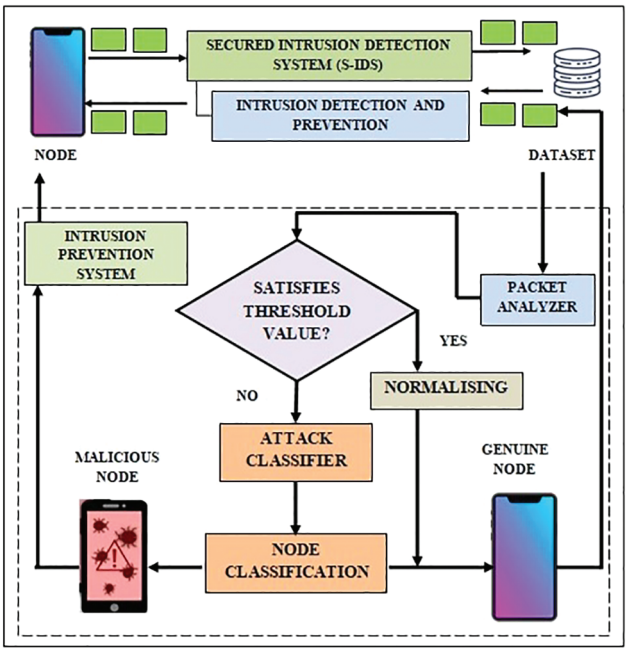

Figure 3: Proposed S-IDS model for securing MANET

The IDS is split into two categories: detection and prevention. The detection system includes a packet that analyses packets based on criteria such as packet arrival time, number of packets per flow, packet count, and packet size. The valves of this are verified with a training data, and the ambiguity of these valves is determined by establishing threshold valves. The categorization of different types of attacks [16] in the network is determined by establishing threshold valves. If an attack is identified, an alarm is set in the intrusion prevention engine to alert the user. The following essential features are required for establishing S-IDSs for MANETs, due to the availability of attacks from malicious nodes in the network:

- S-IDS shall not result in any new MANET attacks.
- The system's nodes must communicate information to their network connections in a transparent manner.
- S-IDS must use the least resources possible to identify assaults and convey this information to its associated nodes as soon as possible after detection in the network.
- S-IDS needs to be fault resilient.

The system establishes a secure intrusion detection system and implements the Secure Energy Routing (SER) Protocol, which monitors and resists network intrusions using a protocol that establishes a path to the source node via network communications. The necessary path is acquired by the nodes through a connection implementation phases when required in the protocol. The network layer and the Media Access Control

(MAC) layer, on the other hand, will be investigated. There have been three categories in the SER protocol for the utilization of node energy in the network. The energy used to transmit and receive data packets, as well as the energy used in the idle state. Energy efficiency [17] cannot be achieved if MANET is overheard. The energy spent to collect and distribute packets shows the system's basic and wasted energy loss. The DSR algorithm has been modified to enhance the SER protocol. The energy factor is considered to be a need for finding the shortest path. Reducing energy force causes a node in the remaining nodes to experience an expense. The objective is to extend the lifetime of an ad hoc network. The total energy consumption incurred by the MANEL node is mathematically represented in Eq. (1).

$$E_T = \sum_{i=1}^{R-1} E(n_i, n_{i+1}) \tag{1}$$

where, n_i is the present node to transfer the data to the successive node n_{i+1}. The term "i" represents the number of routes that the node is transferring the data to reach the dataset. The MANET tends to determine the optimal number of paths between the source node to the destination node using the mathematical representation in Eq. (2).

$$E_{TO} = min(E_T) \tag{2}$$

The cost function of the MANET node is determined by the energy capacity of individual MANET node. The cost function is mathematically represented in Eq. (3).

$$f_c(t) = \frac{1}{E_C} \tag{3}$$

The energy capacity of the individual node in the MANE is determined using the residual energy and the energy consumed by the node to transfer the data from one node to another. This energy capacity also relies on the size of the data to be transferred which is mathematically illustrated in Eq. (4).

$$E_c = E_R + \int_0^{n-1} (L_p + D_p) dt \tag{4}$$

The MANET chooses the routing path such that it consumes minimal energy to transfer the data from one node to the another which is represented in Eq. (5).

$$R_p = Min(R_t | t = (n-1)) \tag{5}$$

3.1 Route Discovery Phase

When a connection from source to destination is identified in the SER protocol, the route discovery process launches a Route Request (RREQ) packet with a requested route to the destination.

- When a new packet is received with reduced cost, the cost is updated to the new minimum, and the necessary information to the path is stored in RREQ.
- In addition, if new RREQ costs are large, prior data will preserve them, ensuring that nothing is changed.

At that point, the destination node broadcasts Route Replay (RREP), which removes the RREQ and lowers the connection cost. The destination generates RREP in the existing reactive protocol after receiving the initial RREQ. After that, the shortest path is chosen, and the various RREQs are discarded. It is possible that the SER protocol has the authority to choose the path by sending a Path Confirm (RCON) to the destination. To have a deeper understanding of how the secure energy routing protocol

creates a channel in the network by transmitting RREQs to its neighboring members. The source node transmits RREQ to its neighboring node to obtain information about node energy and route accessibility for the destination, as shown in Fig. 4.

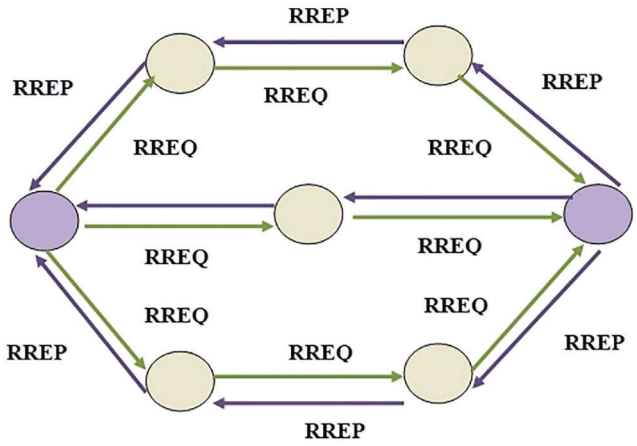

Figure 4: Resource request initiated and received by source node

The source nodes will receive RREP from the other nodes in the network, and the process repeats until all nodes in the network have been completed, as shown in Fig. 4. The information in the packets will be the shortest path from the source to the destination in the network. As described in Fig. 5, the SER protocol has the advantage of deciding the proper route path with the lowest energy-aware metric.

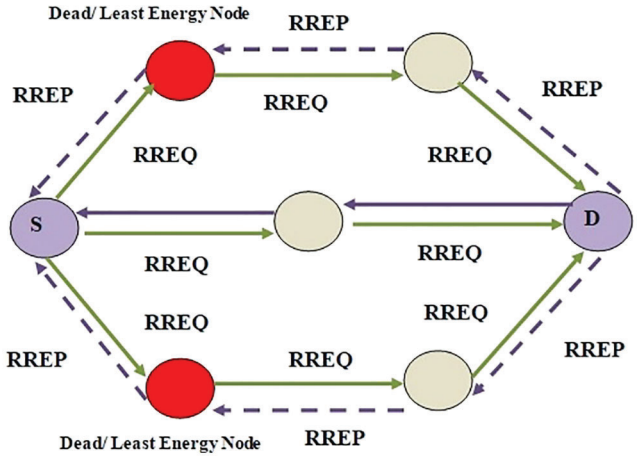

Figure 5: Best path selection process

MANETs are vulnerable to attacks as they lack network management services, due to their absence of network architecture and the lack of a centralized access point that distinguishes trusted and untrusted nodes. Because no past stable policies have been implemented, the network nodes must band together to maintain the network service. MANETs are also demanding in terms of creating these security measures in place at network nodes. MANETs are subject to a variety of attacks. Because such attacks jeopardies the network's performance. Avoiding attacks is often the first step in ensuring connectivity between networked nodes. Fig. 5 emphasizes the detection and prevention of selfish and malicious nodes in a

network by setting an alarm in the proposed S-IDS. The source node transmits RREQ to all of its affiliated nodes, which subsequently respond with RREP to the source node through the route path from destination. The source then reverses pathways and sends an RCON to validate the destination route path. This step is repeated until all nodes in the network have been completed. The secure energy routing protocol for MANET follows the route path discovery with the minimal energy threshold valve section. The MANET's safeguarding energy routing protocol against assaults addresses concerns such as routing protocols, energy consumption, safeguarding routing paths, and exposing a malicious node to the network, as well as monitoring performance in the face of attacks. The SER protocol has been developed and tested. The algorithm for performing the secure routing in MANET using the proposed Secure-Intrusion Detection System is illustrated in Tab. 1.

Table 1: Algorithm for secure route discovery using S-IDS in MANET

Algorithm: Process of Secure route discovery using S-IDS in MANET
// Initialize the process
for (x=1 to n)
{
if("x" is the source mobile ad-hoc network node)
path[P] = x
elseif (a is the neighbor node)
path[P] = x+a (determine the energy capacity)
else
path[P] = Null
}
Transmit RCON to{path 1[P1], path 2[P2],….path n[Pn]}
//update the routing path, path[P]
Repeat
{
Wait(vector path [P] received from neighbor "a")
for (x=1 to n)
{
if(path [P] encompasses source node "x")
discard [P]
else
path [P] = {path [P_n], x+a}
}
if(possible of alternate path)
check path energy {path 1[P1], path 2[P2],….path n[Pn]}
}
end if
end

3.2 Secure Transmission Phase using Elliptical Curve Cryptography

The discovery of secured shortest path between the source and destination is followed by encrypting the data packet before transmission, with an objective to be rigid against attacks like black hole attack which is most common in MANET. The Blackhole Attack is a type of attack in which the malicious nodes respond to the RREQ with a fraudulent RREP and then masquerades as the routing node with the most recent route by creating a greater sequence number. The attacker node in this attack attracts packets but does not transmit any of them to the destination, instead dropping them all. The data sent by the nodes do not reach their intended destination as a result of this attack. The issue emerges when a number of attacker nodes block all other paths, and the attacker node functioning as a router disguise itself as a valid one. Fig. 6 depicts a MANET in which the packet sent by the source, S, and intended for D is intercepted by M, a blackhole attacker node acting as a router with a higher sequence number.

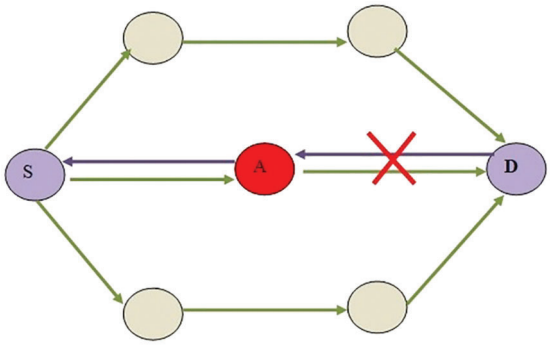

Figure 6: Malicious Node "A" intercepting the data communication

Elliptic Curve Cryptography is a secure and efficient public key cryptographic technology with a shorter key size than other public key cryptographic algorithms. Furthermore, it is based on the discrete logarithm issue, which claims that if K = nxB, it is simple to deduce K given n and G, but difficult to expose n given K and B. As a result of ECC, retrieving the private key from the given secret key and public key will be difficult for the blackhole attacker node. Elliptic Curve Cryptography (ECC) is a term that refers to a set of cryptographic tools and protocols that leverage the discrete logarithm problem to provide security. ECC is based on elliptic curves and their accompanying sets of integers and equations. The phases of ECC's work are as illustrated in Tab. 2.

The Tab. 2 illustrates the encryption process performed at the Sender "S" end and the decryption process in the destination "D". Thus, by performing encryption and decryption process using Elliptical Curve Cryptography (ECC), the data is transferred with high level of security.

4 Results and Analysis

In the NS-2, the Secure Energy Routing (SER) protocol is implemented, and the research is compared to the DSR protocol, the Ad-hoc On-Demand Vector (AODV) routing protocol, and the Destination Sequenced Distance Vector (DSDV) routing protocol. The NS-2 simulator, version 2.64, has been used to simulate the SER, DSR, AODV, and DSDV protocols, and network traces were obtained with mobility records. The simulation's execution model is shown in Tab. 3. Packet Delivery Ratio (PDR) and End-to-End Delay with changing node speed (m/s) and packet size were chosen as performance metrics for evaluating the protocols (Bytes).

Table 2: Algorithm for Elliptical Curve Cryptography (ECC) for secured data transmission in MANET

Algorithm: Elliptical Curve Cryptography (ECC) for secured data transmission in MANET

Key Generation Phase:

1. Define the public element
   a) The elliptic curve cryptography with prime parameters "a", "b" and "p" is defined as in Eq. (6).
   b) $Y^2 \bmod (p) = (x^3 + ax + b) \bmod (p)$ (6)
   c) "B" is the base point in elliptical curve.

Sender "S" key generation phase:

2. Sender "S" may select any random number as a private key "N_S" such that N_S<n Determine public key "P" using the mathematical model represented in Eq. (7).

$$P = N_S * B \tag{7}$$

Destination "D" key generation phase:

3. Destination "D" selects any random number as a private key "N_D" such that N_D<n
4. Determine public key "M" using mathematical equation represented in Eq. (8).

$$M = N_D * B \tag{8}$$

Secret Key Generation phase:

5. Secret key: Sender "S": $P_{1K} = N_S * M$
6. Secret key: Destination "D": $P_{2K} = N_D * P$
7. The relation between the key is to satisfy the following equation

$$Ns * M = Ns*(N_D*B) = N_D*(N_S*B) = N_D*P \tag{9}$$

Encryption phase using ECC:

8. Consider information packet [I_1] is sent from Source "S" to Destination "D"
9. Sender "A" opts a random number "k" to choose a private key "N_S" and determines the public key "P" using Eq. (7).
10. Opt the B value, "the base point" from the elliptic curve E(a,b)
11. Encrypt the data packet [I_1] to produce the cipher text [C_1] using Eq. (10).

$$C_1 = \{kB,\ I_1 + kN_D\} \tag{10}$$

12. The cipher text (C_1) is decrypted to retrieve the plain text (I_1).
13. Multiply the Cipher text (C_1) with private key of Destination "D" as represented in Eq. (11).

$$C = C_1 * N_D \tag{11}$$

14. Perform subtraction from the C to retrieve the plain text (I_1) as mentioned in Eq. (12).

$$C_1 * I_1 + kM - N_D(kB) = I_1 + k(N_D B) - N_D(kB) = I_1 \tag{12}$$

15. Repeat the process for all data packets (I_n)
16. End process

Table 3: Simulation parameters

Parameter	Simulation specifications
Simulation tool	NS-2 (2.64)
Network coverage area	1000 × 1000 m
Number of MANET nodes	100
Initial energy of nodes	200 Joules
Range of transmission	250 m
Bandwidth	2 Mbps
Network protocols	SER, AODV, DSDV and DSR
Data rate	1024 bytes

The Fig. 7 depicts the Network Animator which represents the graphical notation of data transfer from source node to the destination node.

$$PDR = \frac{\sum_{x}^{N} Total\ packet\ Received}{\sum_{X}^{N} Total\ Packet\ transmitted} \tag{13}$$

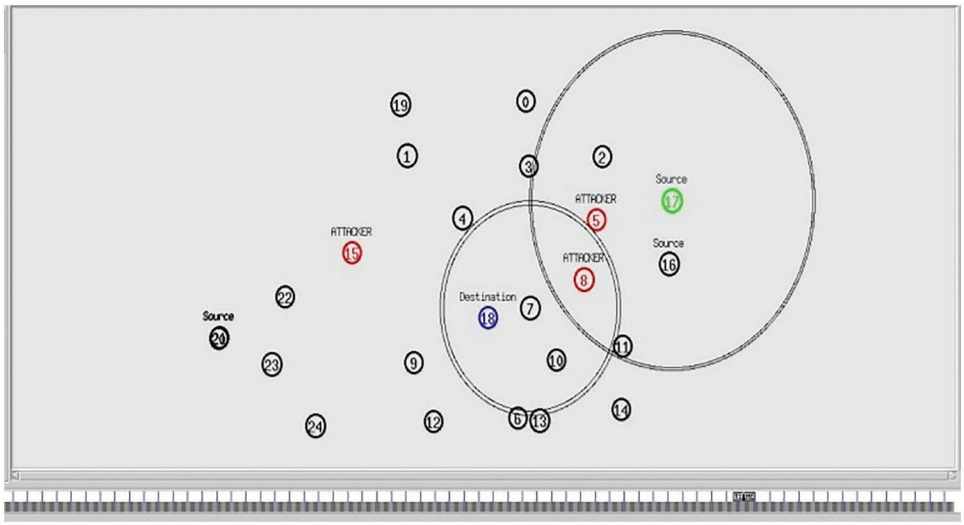

Figure 7: Network animated MANET

The Packet delivery ratio is compared with the node speed under two cases namely with and without the occurrence of attack in the MANET.

The Tab. 4 represents the comparative values of the proposed SER protocol when there is no attack is recorded in the MANET.

The Tab. 5 is the measured performance values of the proposed and existing protocols in the presence of attacks which provide a reduced percentage of Packet Delivery Ratio and an elevated level of End to End delay.

Table 4: Performance analysis of MANET in the absence of attack

Node speed (ms^{-1})	Routing protocols	Total packets sent	Packets received	Dropped packets	PDR (%)	End to end delay (ms)
0	SER	13000	12657	343	97.36	17
	AODV	13000	11035	1965	84.88	19
	DSDV	13000	11369	1631	87.45	21
	DSR	13000	10325	2675	79.42	23
2	SER	15454	14256	1198	92.25	23
	AODV	15454	13258	2196	85.79	27
	DSDV	15454	12489	2965	80.81	28
	DSR	15454	13110	2344	84.83	31
5	SER	18596	17123	1473	92.08	27
	AODV	18596	16148	2448	86.84	29
	DSDV	18596	16015	2581	86.12	33
	DSR	18596	15945	2651	85.74	36
10	SER	25476	21030	4446	82.55	41
	AODV	25476	20348	5128	79.87	45
	DSDV	25476	19991	5485	78.47	47
	DSR	25476	19248	6228	75.55	51

Table 5: Performance analysis of MANET in the detection of attack

Node speed (ms^{-1})	Routing protocols	Total packets sent	Packets received	Dropped packets	PDR	End to end delay (ms)
0	SER	13000	11526	1474	88.66	21
	AODV	13000	10025	2975	77.12	25
	DSDV	13000	10698	2302	82.29	27
	DSR	13000	10459	2541	80.45	24
2	SER	15454	12658	2796	81.91	29
	AODV	15454	11203	4251	72.49	31
	DSDV	15454	10258	5196	66.38	36
	DSR	15454	11258	4196	72.85	41
5	SER	18596	14902	3694	80.14	36
	AODV	18596	14801	3795	79.59	41
	DSDV	18596	14256	4340	76.66	51
	DSR	18596	14586	4010	78.44	48
10	SER	25476	19514	5962	76.60	51
	AODV	25476	17586	7890	69.03	69
	DSDV	25476	16587	8889	65.11	71
	DSR	25476	14024	11452	55.05	75

The Fig. 8 depicts the graphical representation of comparative performance of the proposed SER with the state of art protocols. It is clearly evident that the proposed SER protocol outperforms in terms of Packet Delivery Ratio when no attack is detected in the MANET.

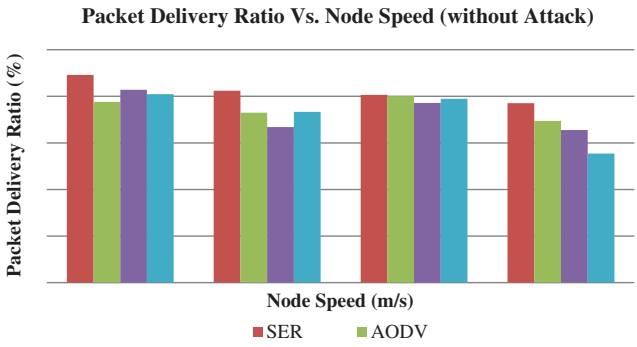

Figure 8: Comparison of packet delivery ratio with node speed (without attacks)

Fig. 9 shows a graphical representation of the proposed SER's performance in comparison to existing protocols. When an assault is discovered in the MANET, it is clear that the suggested SER protocol outperforms in terms of Packet Delivery Ratio.

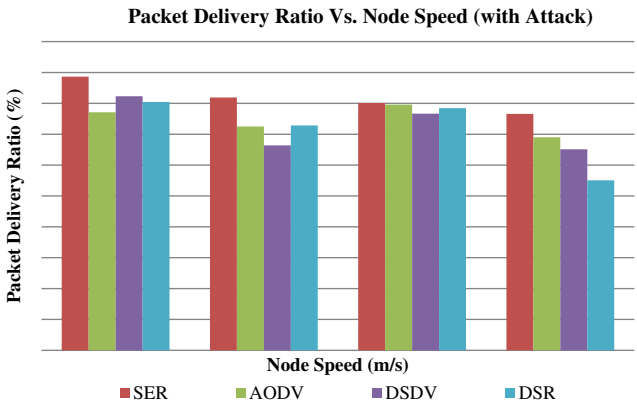

Figure 9: Comparison of packet delivery ratio with node speed (with attacks)

Fig. 10 indicates that while there is no harmful activity, throughput rises to around 355 kbps, but drops to around 240 kbps when malicious nodes are present. The values are increased to 310 kbps with ECC implementation in the simple SER protocol.

As demonstrated in Fig. 11, when blackhole attacker nodes are present in the MANET, the packet delivery ratio declines to around 0.10 with three attackers. When the proposed approach is used, the packet delivery ratio improves significantly to above 0.20, even when attacker nodes are present in the network. With no malicious nodes in the environment, the Packet Delivery ratio is unquestionably the greatest. It gradually lowers as the number of malicious nodes grows. As time is needed by the encryption process with ECC, the average end-to-end delay increases progressively with increasing malicious nodes. The normalized routing load increases in proportion to the number of blackhole attacker nodes present in the circumstance, albeit it varies depending on the quantity of packets transmitted.

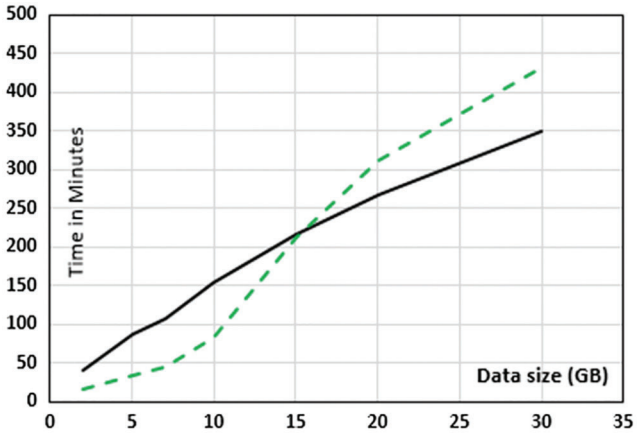

Figure 10: Comparison of processing time with throughput

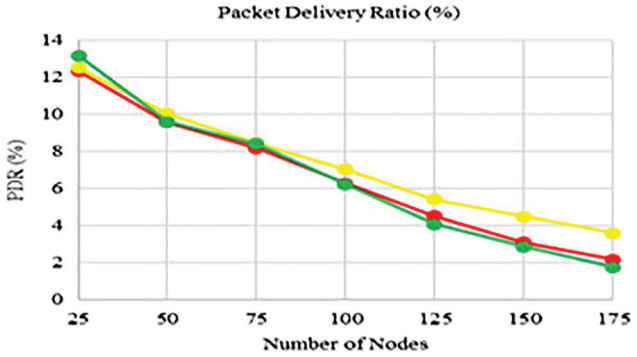

Figure 11: Comparison of processing time with packet delivery ratio

5 Conclusion

The Secure Energy Routing (SER) protocol for MANETs was developed as a result of the Secure Intrusion Detection System (SIDS) architecture. The SER protocol has been developed and tested. The protocol implementation took into account the unique challenges of energy routing and created a SID system to avoid network attacks. The execution of the Securing Energy Routing (SER) protocol for mobile ad-hoc networks, in order to avoid different types of active and passive network attacks that are available in the network, has improved the solution to the security issue by building a secure intrusion detection system for the protocol. The proposed method of securing the data transmission using Elliptical Curve Cryptography (ECC) outperforms the data transmission process in a highly secured manner. The proposed SER protocols have been tested on traffic with a constant bit rate. This traffic type can be expanded to Pareto and Exponential traffic to analyze and better understand wireless communication routing algorithms.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. M. Saifuddin, A. J. B. Ali, A. S. Ahmed, S. S. Alam and A. S. Ahmad, "Watchdog and pathrater based intrusion detection system for MANET," in *4th Int. Conf. on Electrical Engineering and Information & Communication Technology*, China, vol. 4, no. 2, pp. 168–173, 2018.

[2] S. S. Zalte and V. R. Ghorpade, "Intrusion detection system for manet," in *3rd Int. Conf. for Convergence in Technology (I2CT)*, India, vol. 11, no. 7, pp. 1–4, 2018.

[3] R. PremKumar and R. Manikandan, "Distributed hybrid sybil attack detection framework for mobile ad hoc networks," *Materials Today: Proceedings*, vol. 15, no. 21, pp. 23–42, 2021.

[4] D. Prabakaran and S. Ramachandran, "Multi-Factor authentication for secured financial transactions in cloud environment," *Computers, Materials & Continua*, vol. 2, no. 5, pp. 1781–1798, 2022.

[5] M. V. Rajesh, "Intensive analysis of intrusion detection methodology over mobile ad-hoc network using machine learning strategies," *Materials Today: Proceedings*, vol. 9, no. 3, pp. 12–22, 2021.

[6] M. A. Khan, "An efficient and provably secure certificateless key-encapsulated sign encryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, no. 12, pp. 36807–36828, 2020.

[7] K. Burhan, A. Farhat, O. Rashida, R. Bisma and M. Roohie, "A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile ad-hoc networks," *IEEE Access*, vol. 11, no. 9, pp. 1–13, 2020.

[8] M. Ningrinla, D. Raja and D. Sajal, "A novel approach for efficient usage of intrusion detection system in mobile ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 27, pp. 12–32, 2016.

[9] R. Suganthi, I. Poonguzhali, J. Navarajan, R. Krishnaveni and N. Saranya, "Trust based efficient routing (TER) protocol for manet," *Materials Today: Proceedings*, vol. 22, no. 1, pp. 23–50, 2021.

[10] A. Gauravand and A. K. Singh, "Light weight approach for secure backbone construction for MANETs," *Journal of King Saud University - Computer and Information Sciences*, vol. 19, no. 12, pp. 908–919, 2021.

[11] S. Bismin and P. Salini, "Detection and isolation of selfish nodes in MANET using collaborative contact based watchdog with CHIMP-AODV," *IEEE Access*, vol. 21, no. 3, pp. 22–45, 2021.

[12] D. Shona and M. S. Kumar, "Efficient ids for manetusing hybrid firefly with a genetic algorithm," in *Int. Conf. on Inventive Research in Computing Applications (ICIRCA)*, USA, vol. 6, no. 10, pp. 191–194, 2018.

[13] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[14] S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing blackhole attacks in MANETS using modified sequence number in AODV routing protocol," in *8th Int. Electrical Engineering Congress (iEECON)*, India, vol. 21, no. 13, pp. 1–4, 2020.

[15] S. Manikandan and M. Chinnadurai, "Virtualized load balancer for hybrid cloud using genetic algorithm," *Intelligent Automation and Soft Computing*, vol. 32, no. 3, pp. 1459–1466, 2021.

[16] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[17] M. Jan, W. Ian and S. Winston, "Security threats and solutions in MANETS: a case study using AODV and SAODV," *Journal of Network and Computer Applications*, vol. 35, no. 14, pp. 1249–1259, 2012.