MACO-ECDH BASED SECURE DATA TRANSMISSION IN MANETS

Sandeep Lalasaheb Dhende

Research Scholar, Department of Electronics and Telecommunication Engineering,
ZES's Zeal College of Engineering and Research, Pune,
SPPU, Maharashtra, India
sandeepldhende@gmail.com

Suresh D. Shirbahadurkar

Professor, Department of Electronics and Telecommunication Engineering,
ZES's Zeal College of Engineering and Research, Pune,
SPPU, Maharashtra, India
shisd@gmail.com

Abstract

Wireless Mobile Ad Hoc Network (MANET) is a network of mobile nodes that is self-contained. The unique characteristics of mobile ad hoc networks (MANETs), such as dynamic topology and an open wireless medium can expose MANETs to a variety of security vulnerabilities. This has an effect on the protection of data transmitted between network nodes. Due to self-configuration and maintenance capabilities, the MANET faces a range of security problems as it expands its technology. Furthermore, because of the highly complex and resource-constrained existences of MANETs, conventional security solutions for wired networks are ineffective and inefficient. As a result, an effective technique is needed to prevent abnormal nodes following the detection process while also improving QOS parameters. The researchers in this paper use an optimization technique to improve efficient data transmission with high protection in the MANET. The optimal route is selected using modified ant colony optimization (MACO). To improve the transmission security of the MANET, an Elliptic curve Diffie-Hellman (ECDH) can be used. The Elliptic curve Diffie-Hellman (ECDH) method improves its overall efficiency and security. The packet delivery ratio, overhead, end to end delay and throughput are used in the security-based research. Finally, the results show that using optimization techniques, the MANET can achieve a high transmission rate while also improving data protection.

***Keywords*: MANET, Security, MACO, ECDH, Routing**

1. Introduction

MANET is a network made up of a large number of mobile nodes (MN) that can be used for a variety of mechanical, security, and rural applications, such as transportation movement tracking, environmental monitoring, smart offices, and battlefield surveillance [3][6]. Nodes in these networks interact with one another in a multi-hop manner. When a sender sends a data packet to a destination node, it communicates with an intermediate node. As a result, each node in the network plays an equal role [18]. The mobile devices in the respective networks function as routers, allowing users to send and receive data while also controlling and routing the network. Routing allows for the proper path selection within a network. The routing protocol, on the other hand, facilitates contact between routers and processes data packets from source to destination by determining the best path between sender and receiver [18]. When devices are in motion, they have a huge effect on communication and Quality of Service (QoS). Because of its dynamic environment, a MANET is fitted with limited resources such as bandwidth in this regard. The main tools used for QoS evaluation are throughput, latency, and delay deviation. In comparison to fixed wired and wireless networks, QoS in MANETs is found to be extremely complicated [18]. For the MANET, various energy-efficient relaying schemes have been developed, with clustering and data transfer being particularly useful for relay-based sensor networks that require scalability to hundreds, if not thousands, of nodes. In the case of the MANET, the optimal shortest route for communication between the source and destination is selected using MACO and the data transfer is secured using HRM. The routing for quality-of-service (QoS) should take into account a variety of factors, including end-to-end reliability, quality, deferral, and energy efficiency. Few limitations are discovered to be dissimilar, and delicate QoS provisioning can be accomplished. The CHs are in charge of collecting data samples from inside the cluster. The accumulated results are sent from CHs to sink through single- or multi hop paths in a hierarchical order. Because of the lack of correspondence, the reliability issues could have an impact on the details, causing it to be undermined/data misfortune. The main problem with course disclosure is steering

overhead, which results in data loss. Since clustering in the MANET is a non-deterministic polynomial-time-hard problem, a variety of optimization algorithms can be used to solve it. Genetic algorithm (GA), simulated annealing, particle swarm optimization (PSO), artificial bee colony algorithm, and others are examples of optimization algorithms [6].

This paper proposes routing protocol for increasing distribution ratios, reducing end-to-end delays, and ensuring more stable transmission. The updated modified ant colony optimization (MACO) method was then used to found out shortest path for communication. The Elliptic curve Diffie-Hellman (ECDH) method was used in the MANET to ensure channel security during data transmission. The Elliptic curve Diffie-Hellman (ECDH) method can improve overall performance and confidentiality. The packet delivery ratio, throughput, overhead, and end to end delay were used in the security-based research. This routing protocol can also be used to improve reliability and lower end to end delay.

The following is how the rest of the paper is organized: Section 2 examines the issue in the light of previous research. Section 3 provides an overview of MACO and Elliptic curve Diffie-Hellman (ECDH) methods. In Section 4, the characteristics chosen for modeling are defined, as well as the results of proposed method compared to select secure routing and data protection protocols. The study results are summarized in Section 5.

2. Literature Survey

In 2019 [3], with the aid of an optimal CH-based signcryption technique, Mohamed Elhoseny and K. Shankar proposed a novel model for a stable security level of the MANET. The MDPSO algorithm was used to find the best CH in this case. For data protection in the MANET, the approximate distance, TV, and energy consumed by each CM were measured. The use of an SRP also ensures data availability, stability, and readability from beginning to end. Furthermore, the proposed model combined the number of attackers with the performance assessment method to examine the number of attackers. With a variable number of nodes in the network, the suggested approach achieved the best results with a PDR of 92.22 percent, an NLT of 111 hours, and EC was reduced by 92 J. Furthermore, the proposed EERP with the signcryption process achieved an accuracy rate of 80–82 percent and a security level of 93 percent.

In 2019 [13], Mariappan Rajashanthi and K. Valarmathi suggested a secure multipath routing scheme based on Quality of Service (QoS) for efficient data transmission, as well as an encryption technique. The suggested strategy's function was connected to available organizations in terms of packet delivery ratio, throughput, end-to-end delay and energy. In comparison to earlier energy-aware routing protocols, the proposed routing protocol consumes very little energy.

In 2018, Liu et al. [9] suggested several security-related data collection regulations and then reviewed newly proposed methods in the field of MANET detection mechanisms. To be more precise, they used the new standards as a series of guidelines to assess current security-related data collection efforts. Some recent literature studies relating to defense data collection in attack detection were checked for accurate security assessment.

In 2017, Rana and Rana [14] addressed efficient routing strategies and consolidated the updated LEACH and ad hoc on-demand multipath distance vector approaches (AOMDV). LEACH was used for cluster generation and also provided information on node energy, while AOMDV was used for multipath routing. In this way, the suggested approach offered low-overhead and low-EC coordination in the MANET.

In 2017 [7], Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN), suggested by Darren Hurley-Smith, Jodie Wetherall, and Andrew Adekunle, safeguards the network and connectivity in MANETs. The main goal is to gain access to a virtually closed network (VCN) that allows for fast and secure communication while maintaining anonymity, honesty, and authenticity. For their respective routing protocols, SUPERMAN has been shown to have lower-cost security than SAODV and SOLSR. One may presume a certain degree of trust within a stable, closed network by creating it.

Sending and receiving messages from nodes is the only way for two users to communicate. The network's framework is built on this foundation; Oh and Lee created it in 2017 [11]. A relative angle was used to set the route direction using the built algorithm. The implemented algorithm's protocol resulted in a higher packet delivery ratio (PDR) and lower EC than the most inferior detection clustering algorithm. In addition, the mobility-based clustering metric in the MANET algorithm was calculated.

In 2018 [10], Mostafaei suggested a distributed-learning automaton-based algorithm to improve the network's performance with several constrained QoS parameters. It took a few QoS routing restrictions into the record in way decision, such as end-to-end unwavering quality and deferral. In terms of end-to-end delay and energy-effectiveness, the results showed that the measurement performed better than the current state of the craftsmanship violent calculations.

To determine the best location of the group particles, the basic swarm optimization was updated. In the case of a stable network structure, one particle is expected to determine the G-best position, and the remaining particles can look for further domains to verify that the best position is G-best, not the current one. In this article, a new MDPSO algorithm for CH selection is developed to solve the shortcomings of current versions of

PSO algorithms. The majority of previous research has concentrated on either energy efficiency or reliability; however, in this article, both energy-efficient clustering and reliability are combined in a single MANET model.

2.1 *Security issues in the current system*

Security is a broad word that refers to a network administrator's rules and processes for preventing and tracking illegal access, exploitation, modification, or a denial of service to the network and its resources [3]. Because of the MANET's importance, security is a top priority. It has inherent weaknesses. These flaws are inherent in nature.

It is an integral part of the MANET structure and cannot be removed. Several of the security concerns that exist in existing systems are listed as seen below.

1) MANET dependable security refers to some protective systems for a highly secured network and includes two key processes: security service and assaults.
2) The MANET nodes are unable to properly define the network's physical border.
3) The CH process selects the cluster's leader node, which serves as a coordinator for the cluster's data transmission process and security.
4) When a node in a cluster wants to connect with another node that belongs to a different cluster, the cluster gateway is used to complete the communication between the two nodes. As a result, cluster gateway should be included in the communication.
5) To ensure authentication, the gateway in each cluster verifies the device selection.
6) Data encryption plans should be used to protect data privacy [16]. Additionally, if the cryptographic keys are not encoded and kept in the node, hacked nodes may pose a danger to secrecy [5], [19].

3. Methodologies

The technique of sending data from a source to a destination without the need of a wired media is known as wireless communication. Some of the WSN's and MANET's features are almost identical. The MACO (Modified Ant Colony Optimization) and ECDH (Elliptic curve Diffie-Hellman) were employed in the MANET to provide reliable data transfer and improve QoS.

The ECDH method explored for the path security procedure in the MANET. Only the secured path can be taken for the data transfer in the MANET using this security approach. In addition, in the next parts, the technique and graphical depiction of the proposed study are explained.

3.1 Modified ant colony optimization (MACO)

The improved throughput rates are required for MANET applications to satisfy user needs and to provide smooth support for user requests. Due to various design difficulties and constraint fulfilment, traditional protocols fail to meet users need. Enhancing throughput becomes a critical problem in order to satisfy user needs and application support. Throughput is the most important criteria in the Modified ACO optimization method. ACO is used to increase network throughput by determining the best paths to the destination [12].

The modified ACO increases the link's packet transmission rate, resulting in a fair route selection solution. Forward ant is started by the source node at random to visit all of the accessible nodes in the route [13]. During their traversal, the ants leave a little quantity of pheromone on the visited links. When the ants arrive at their destination, they update the pheromone of all nodes visited throughout the traversal. A node's throughput is treated as a pheromone in this case. The throughput function is used to update a node's pheromone [4] [8].
Equation 1 is used to calculate f (t).

$$f(t) = max \sum_{i=1}^{k} \frac{p(i)}{t(i)} \quad (1)$$

Where k denotes the packet transmission limit, p(i) is the number of packets successfully transferred, and t(i) denotes the packet transmission time.

An ant (A) is a collection of routes that link all nodes. MACO's fitness function shown in equation 2, also known as the objective function, is as follows:

$$fitness\ of\ ant = \sum_{i=1}^{n-1} d(i,j) \quad \forall j = n \ \Delta \ j = i + 1 \quad (2)$$

The pheromone is updated in a cyclic way during the course of each traversal of a link l. Equation 3 is used to calculate the likelihood of an ant ‘m' visiting node ‘j' from node i.

$$\rho_{ij}^{k}(t) = \frac{[\tau_{ij}(t)]^{\alpha} \cdot [\mu_{ij}(t)]^{\beta} \cdot [\theta_j(t)]^{\gamma}}{\sum_{k \in N} [\tau_{ij}(t)]^{\alpha} \cdot [\mu_{ij}(t)]^{\beta} \cdot [\theta_j(t)]^{\gamma}} \quad (3)$$

The pheromone concentration in link ij is τ_{ij}, θ_j is the energy of the node, control parameters are α, β and γ, and the throughput heuristic value μ_{ij} is f (t).

Equation 4 is used to calculate the pheromone concentration as it decreases over time.

$$\tau_{ij} = (1 - \rho) * \tau_{ij} + \sum_{n=1}^{m} \Delta_{ij}{}^{n} \quad (4)$$

Where, Δ_{ij}^{m} is the change in pheromone amount in the link ij, updated by the m^{th} ant, and (1-ρ) is a decreasing pheromone constant. The following generation of ants migrates to their goal via increasing pheromone concentration nodes.

This cycle is continued until the condition of stagnation is fulfilled. The road that emerges after a period of stasis is regarded as the best path for communication. This procedure is carried out for each data transmission. This step signals the start of the network's transmission process.

3.2 Elliptic curve Diffie-Hellman (ECDH) Technique

Using a finite number of nodes, a mobile Ad-hoc network can be constructed. The Elliptic curve Diffie-Hellman technique is used to determine whether or not a path is secure. Find the source and destination nodes in the MANET that want to communicate with each other to transfer data packets. The AODV routing protocol is used with MACO to identify the shortest path between these nodes. The shortest way from source to destination will be chosen using MACO, but it does not have to be the secured path. The Diffie-Hellman method is used to verify this path [19]. First and foremost, a conduit from source to destination is constructed in this method. After that, the data packets are transferred using communication channel. ECDH is a variant of the Diffie-Hellman algorithm for elliptic curves. It is actually a key-agreement protocol, more than an encryption algorithm. This basically means that ECDH defines (to some extent) how keys should be generated and exchanged between parties. How to actually encrypt data using such keys is up to us.

The problem it solves is the following: two parties (the usual Alice and Bob) want to exchange information securely, so that a third party (Attacker) may intercept them, but may not decode them. This is one of the principles behind TLS, just to give you an example.

Here's how it works:

First, Alice and Bob generate their own private and public keys. We have the private key dA and the public key HA=dAG for Alice, and the keys dB and HB=dBG for Bob. Note that both Alice and Bob are using the same domain parameters: the same base point G on the same elliptic curve on the same finite field.

Alice and Bob exchange their public keys HA and HB over an insecure channel. The attacker would intercept HA and HB, but won't be able to find out neither dA nor dB without solving the discrete logarithm problem.

Alice calculates S=dAHB (using her own private key and Bob's public key), and Bob calculates S=dBHA (using his own private key and Alice's public key). Note that S is the same for both Alice and Bob, in fact: S=dAHB=dA(dBG)=dB(dAG)=dBHA

The attacker, however, only knows HA and HB (together with the other domain parameters) and would not be able to find out the shared secret S. This is known as the Diffie-Hellman problem, which can be used to ensure the security of the path and further communication can be proceed.

4. Simulation parameters and results

The proposed method is validated by modelling the findings in Network Simulator 2 (NS2) and comparing it to an existing method.

Parameters	Value
Number of Nodes	30, 60, 90, 120 and 150
Area Size	1500 m ✕ 1500 m
Transmission Range	250 m
Data Types	CBR
Packet Size	512Bytes
Antenna	Omni directional
Type of Queue	Drop Tail
Routing protocol	AODV
Number of Malicious Nodes	6

Table 1. Parameters for simulation

Table 1 shows the many parameters that are taken into account during simulation. The number of nodes is counted between 30 and 150.

4.1 Performance metrics

The effectiveness of the routing protocol, MACO with ECDH technique is revealed through the analysis based on the metrics, such as packet delivery ratio (PDR), throughput, routing overhead, and delay.

4.2 Comparative analysis

The ACO, genetic algorithm (GA), particle swarm optimization (PSO), and MDPSO were used for comparative analysis [3]. Figure 1 shows the difference in the packet delivery ratio (PDR) with respect to the number of nodes. When compared to existing approaches such as ACO with signcryption, PSO with signcryption, GA with signcryption, MDPSO with signcryption, PSO with ECDH, GA with ECDH, and ACO with ECDH, the proposed MACO with ECDH achieves improved PDR, throughput, delay, and overhead. The achieved throughput for the approaches is shown in Table 3. The figures from (1) to (4) and tables from (2) to (5) show the PDR, throughput, overhead, and delay analysis.

Number of Nodes	ACO with Signcryption	PSO with Signcryption	GA with Signcryption	MDPSO with Signcryption	PSO with ECDH	GA with ECDH	ACO with ECDH	Proposed MACO with ECDH
30	85	89	91	91	92	94	95	96
60	85	85	86	86	93	93	94	95
90	85	86	86	90	94	95	95	96
120	85	86	89	93	95	95	95	96
150	86	88	88	92	95	96	96	97

Table 2. PDR analysis (in %) (Higher PDR is better)

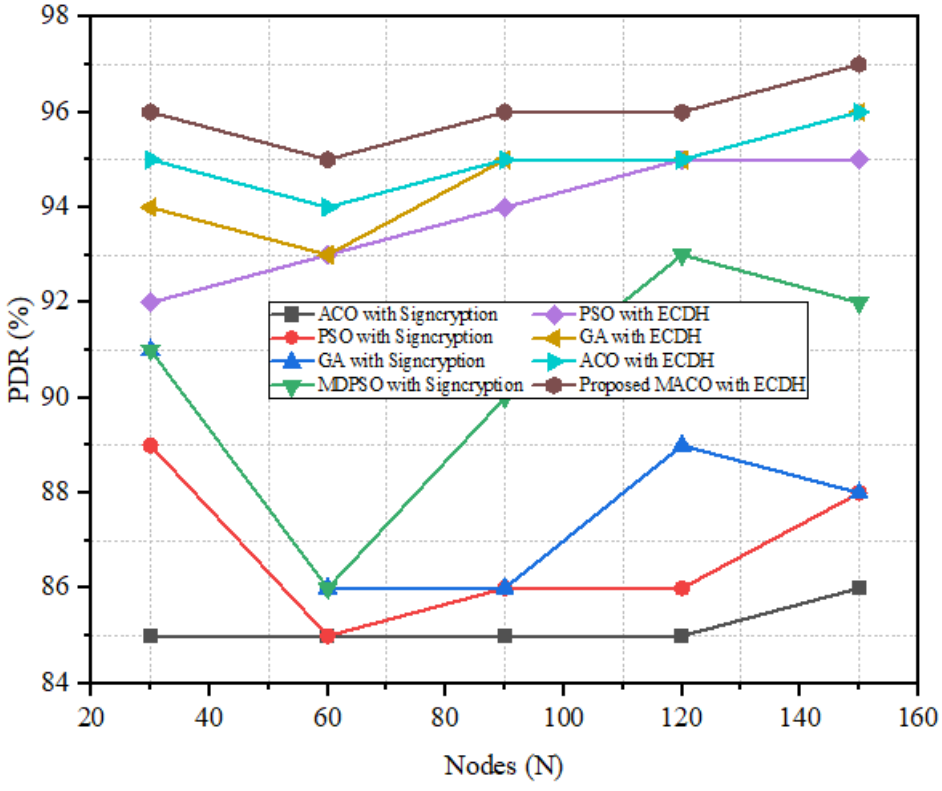

Fig. 1. Analysis based on PDR (Higher PDR is better)

The PDR analysis is done in relation to the number of nodes (in table 2), and it is seen that the PDR % improves slightly as the number of nodes increases. Although the PDR reduces as the number of nodes increases owing to link failure, the secure path selection method increases the PDR by extending the network's link lifetime. When 150 nodes communicate in the network, the suggested MACO with ECDH achieved a PDR of 97 percent, which is the highest PDR percentage ever achieved, thanks to the invention of the secure path selection mechanism.

Number of Nodes	ACO with Signcryption	PSO with Signcryption	GA with Signcryption	MDPSO with Signcryption	PSO with ECDH	GA with ECDH	ACO with ECDH	Proposed MACO with ECDH
30	3586	3705	3737	3984	4189	4213	4269	4313
60	3632	3651	3735	3829	3981	3910	3914	4085
90	3591	3706	3869	4052	4252	4286	4278	4305
120	3586	3600	3610	3729	3980	4193	4285	4489
150	3604	3617	3794	4083	4112	4167	4298	4384

Table 3. PDR analysis (in %) (Higher PDR is better)

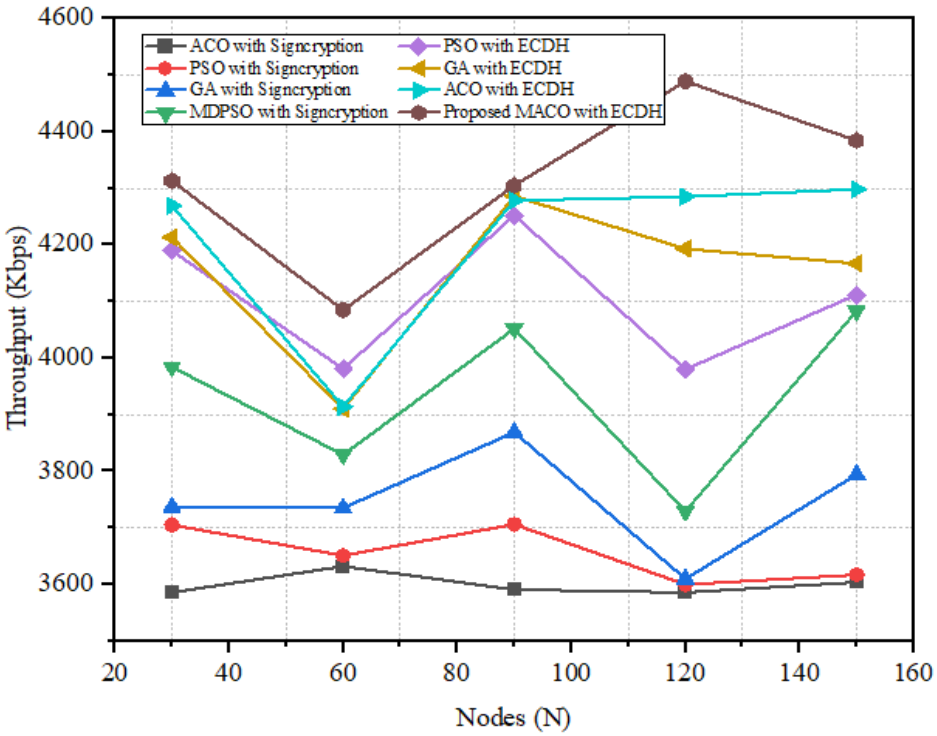

Fig. 2. Throughput analysis (Higher throughput is better)

Figure 2 shows the throughput analysis of the approaches based on the total number of nodes. When the network's transmission overhead is high due to the total number of users, the approaches' throughput suffers. When the total nodes are 150, the suggested MACO with ECDH achieves a throughput of 4384 kbps, which is higher than existing approaches, demonstrating the usefulness of the proposed method.

Number of Nodes	ACO with Signcryption	PSO with Signcryption	GA with Signcryption	MDPSO with Signcryption	PSO with ECDH	GA with ECDH	ACO with ECDH	Proposed MACO with ECDH
30	0.04	0.036	0.035	0.033	0.027	0.021	0.021	0.020
60	0.048	0.044	0.043	0.043	0.038	0.029	0.020	0.018
90	0.043	0.041	0.039	0.034	0.031	0.027	0.026	0.023
120	0.04	0.038	0.038	0.033	0.025	0.026	0.021	0.020
150	0.049	0.044	0.042	0.04	0.023	0.022	0.019	0.018

Table 4. Overhead analysis (Minimal overhead is better)

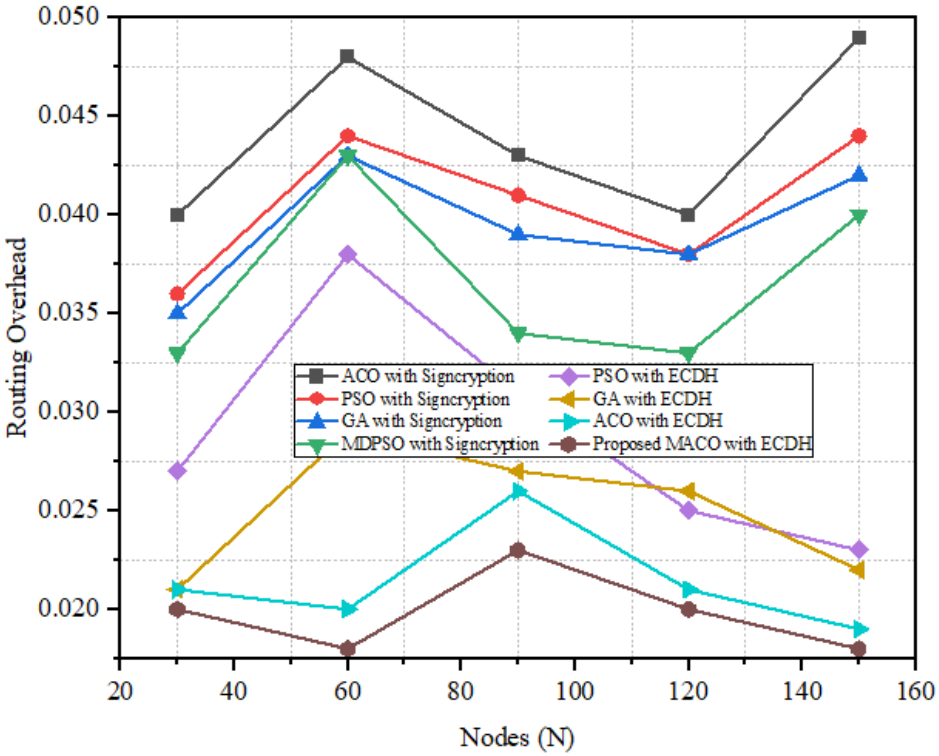

Fig. 3. Overhead analysis (Minimal overhead is better)

Similarly, an overhead analysis is carried out, which examines the network's computing complexity as node communication grows. The overhead is small when the total nodes are 30, but it increases as the number of simulated nodes in the network grows. However, when compared to existing approaches, the proposed model has a low computational overhead, implying that the proposed method schedules communication along the most efficient way.

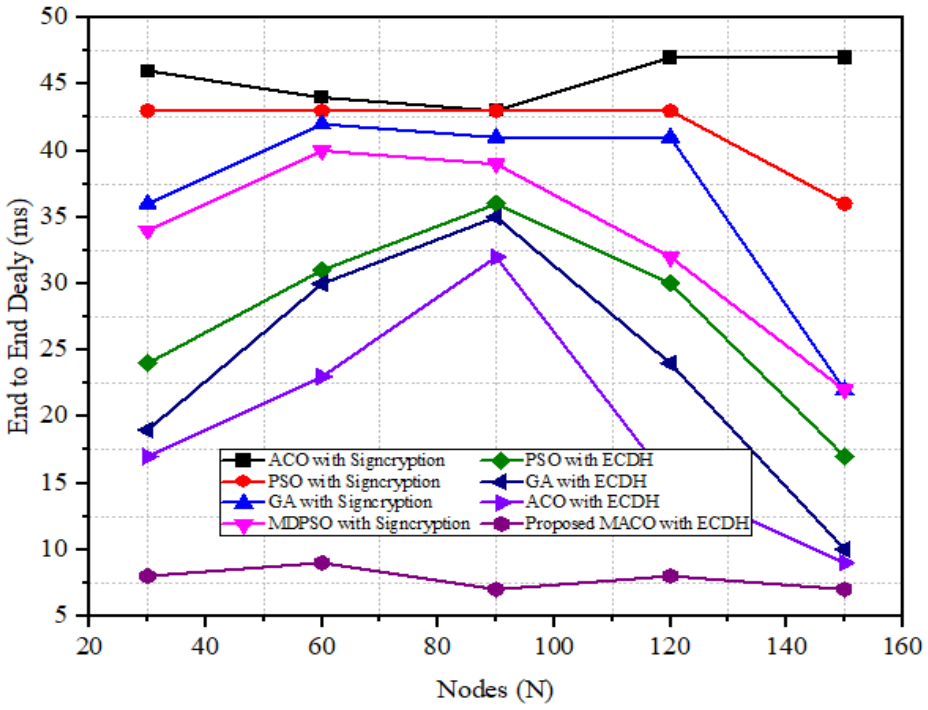

Fig. 4. Delay analysis (Minimal delay is better)

Similarly, the delay analysis in Figure 4 stresses that the network's effective performance is dependent on the shortest possible data communication time between nodes. For example, when a network of 150 nodes is simulated utilizing the suggested MACO with ECDH, the network communication delay is determined to be around 7ms, demonstrating the significance of the proposed approach in exhibiting effective performance.

Number of Nodes	ACO with Signcryption	PSO with Signcryption	GA with Signcryption	MDPSO with Signcryption	PSO with ECDH	GA with ECDH	ACO with ECDH	Proposed MACO with ECDH
30	46	43	36	34	24	19	17	8
60	44	43	42	40	31	30	23	9
90	43	43	41	39	36	35	32	7
120	47	43	41	32	30	24	15	8
150	47	36	22	22	17	10	9	7

Table 5. Delay analysis (in ms) (Minimal delay is better)

In short, the best approach is the one that has the least amount of delay, the least amount of communication overhead, the highest throughput, and the highest PDR. For a minimum delay of 5ms and a minimal overhead of 0.02 with 30 and 90 nodes, the suggested MACO with ECDH surpasses the existing approaches. The suggested MACO with DCDH, on the other hand, achieves a maximum PDR of 97 percent (with 150 nodes) and a throughput of 4471 kbps (with 120 nodes).

Conclusion

The researchers developed a novel model for a security level of the MANET in this study using a MACO with ECDH technique. The MACO technique determines the most efficient communication path. The Elliptic curve Diffie-Hellman algorithm is utilized in the MANET for data security. To assess whether the path between the source and destination nodes is safe, the Elliptic curve Diffie-Hellman algorithm is utilized. The proposed model examined the number of attackers by combining the number of attackers with the performance evaluation technique. Furthermore, the MACO with ECDH technique recommended yielded all-improved results. In the future, backup routing in ad hoc networks (AODV) with an ECDH technique could be investigated for identification of malicious nodes in the MANET. Furthermore, the efficiency of MANETs with security could be improved by merging bioinspired and security algorithms.

Conflicts of interest

“The authors have no conflicts of interest to declare”

References

[1] Alotaibi M. (2019): Security to wireless sensor networks against malicious attacks using Hamming residue method, J Wireless Com Network.
[2] Elhoseny M., et al. (2018): Hybrid optimization with cryptography encryption for medical image security in Internet of Things, Neural Comput. Appl., pp. 1–15.
[3] Elhoseny M.; Shankar K. (2019): Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique, in IEEE Transactions on Reliability, vol. 69, no. 3, pp. 1077-1086.
[4] Gao Y., et al. (2019): A Hybrid Method for Mobile Agent Moving Trajectory Scheduling using ACO and PSO in WSNs, Sensors, 19 (3):575.
[5] Gupta D., et al. (2018): Efficient artificial fish swarm based clustering approach on mobility aware energy-efficient for MANET, Trans. Emerg. Telecommun. Technol., Art. no. e3524.
[6] Harn L, et al. (2016): The novel design of secure end-to-end routing protocol in wireless sensor networks, IEEE Sens. J., vol. 16, no. 6, pp. 1779–1785.
[7] Hurley S. D.; Wetherall J.; Adekunle A. (2017): SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks, in IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2927-2940.
[8] Kaur S.; Mahajan R. (2018): Hybrid meta-heuristic optimization based energy efficient protocol for wireless sensor networks, Egyptian Informatics Journal, Volume 19, Pages 145-15.
[9] Liu G.; Yan Z; Pedrycz W. (2018): Data collection for attack detection and security measurement in mobile ad hoc networks: A survey, J. Netw. Comput. Appl., vol. 105, pp. 105–122
[10] Mostafaei H. (2019): Energy-efficient algorithm for reliable routing of wireless sensor networks, IEEE Trans. Ind. Electron., vol. 66, no. 7, pp. 5567–5575.
[11] Oh Y. J.; Lee K. W. (2017): Energy-efficient and reliable routing protocol for dynamic-property-based clustering mobile ad hoc networks, Int. J. Distrib. Sens. Netw., vol. 13, Art. no. 1550147716683604.
[12] Prabaharan S. B.; Ponnusamy R.(2017): Enhanced Longevity of MANETs using ACO based Balanced Network Monitoring and

Routing Model (BNMR), Advances in Wireless and Mobile Communications, ISSN 0973-6972 Volume 10, pp. 1035-1049

[13] Rajashanthi, M.; Valarmathi, K. (2020): A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs, Wireless Pers Commun 112, 75–90.
[14] Ran B.; Rana D. (2017): Energy efficient load balancing with clustering approach in MANET, in Proc. Int. Conf. Energy, Commun., Data Anal. Soft. Comput., pp. 2019–2024.
[15] Ratanavilisagul C. (2017): Modified Ant Colony Optimization with Pheromone Mutation for Travelling Salesman Problem, 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON).
[16] Shankar K., et al. (2018): An efficient optimal key based chaos function for medical image security, IEEE Access, vol. 6, pp. 77145–77154.
[17] Singh O.; Singh J.; Singh R. (2017): DHHP: A Hybrid Technique for Protecting Mobile Adhoc Networks from Selective Packet Drop Attack, International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, pp. 1743-1763
[18] Vijayan K.; Raaza A. (2016): A novel cluster arrangement energy-efficient routing protocol for wireless sensor networks, Indian J. Sci. Technol., vol. 9, no. 2, pp. 1–9.
[19] Yang Y. (2014): Broadcast encryption based non-interactive key distribution in MANETs, J. Comput. Syst. Sci., vol. 80, no. 3, pp. 533–545.

Authors Profile

Sandeep Lalasaheb Dhende, received his B. E. (Electronics & Telecommunication) degree in 2010 from University of Pune, Pune, India and M. E. (Electronics and Telecommunication) degree in 2013 from Savitribai Phule Pune University, Pune, India. Since 2017, he has been with the department of Electronics and Telecommunication Engineering, SCTR's Pune Institute of Computer Technology, Pune, India as an Assistant Professor. His research area is QoS parameters for Mobile Ad-Hoc Networks.

Suresh Damodar Shirbahadurkar, received his B. E. (Electronics) degree in 1991 from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, India, M. E. (Electronics) degree in 1998 from Govt. COE, Aurangabad, M. S. (formerly CEDTI -Institute of National importance) in 2010 and Ph.D. from National Institute of Electronics & Information Technology, Aurangabad.
He has total 30 years of Teaching & Administration experience. He worked as Professor for 10 years out of which 6 years as Principal and 20 years as Asso. Professor & Asst. professor in E&TC Department of various engineering colleges. His primary research interests include Speech Processing, DSP, and Power Electronics. Over the years, he has supervised numerous bachelors and masters students. Under his guidance, 13 Ph.D. students are working [6 students completed & awarded]. He is associated with various universities & working on various committees. He has visited and tie-up with 7+ overseas universities.
He has published 8 patents, 10 SCI listed journal paper, 20 Scopus Indexed Journal Paper, 5 International Journal papers, 28 International Conference Paper and 19 national conference papers.