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)

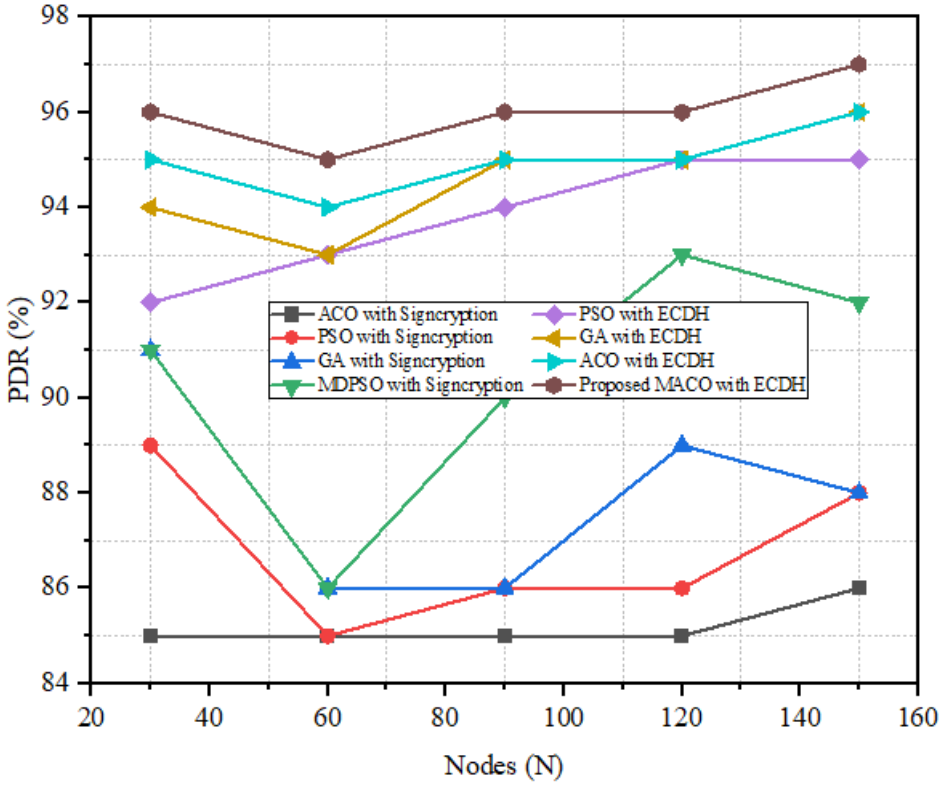

Fig. 1. Analysis based on PDR (Higher PDR is better)

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)

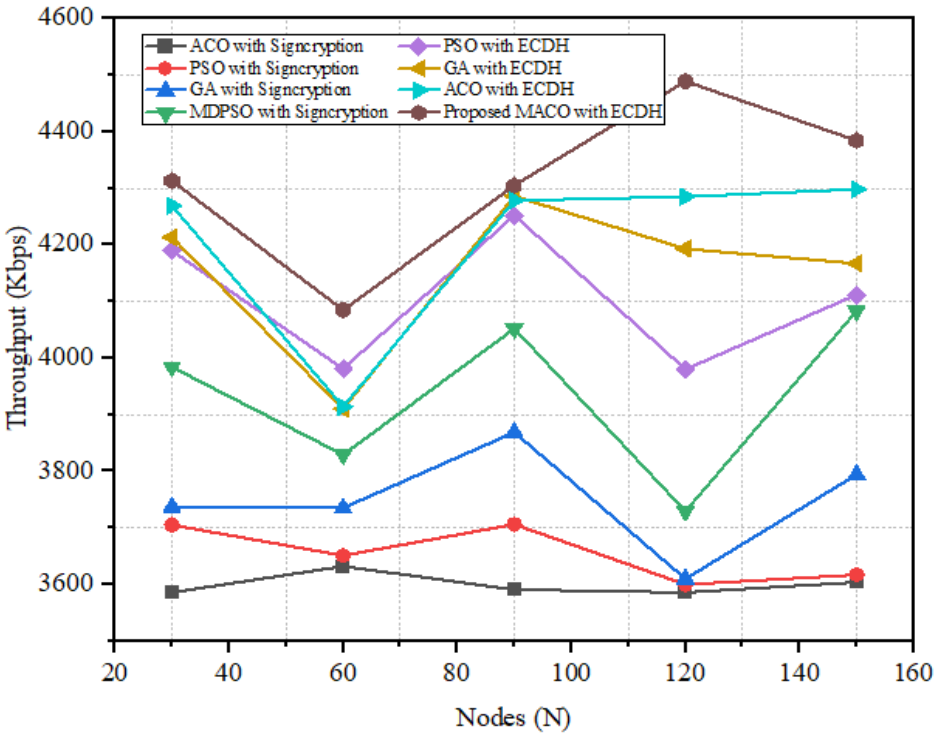

Fig. 2. Throughput analysis (Higher throughput is better)

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)

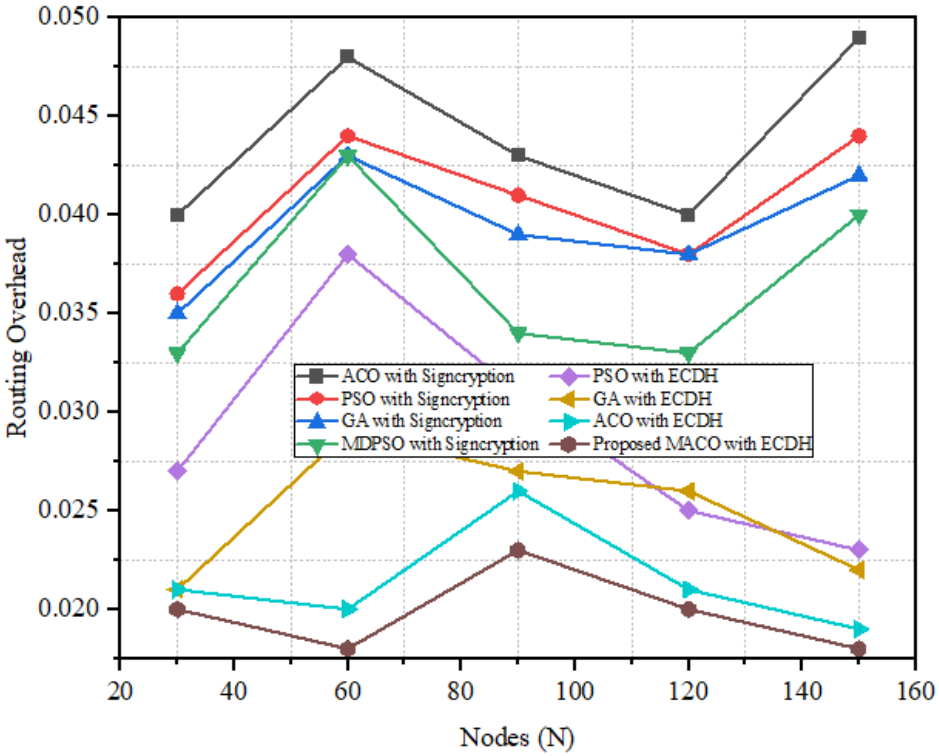

Fig. 3. Overhead analysis (Minimal overhead is better)

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.

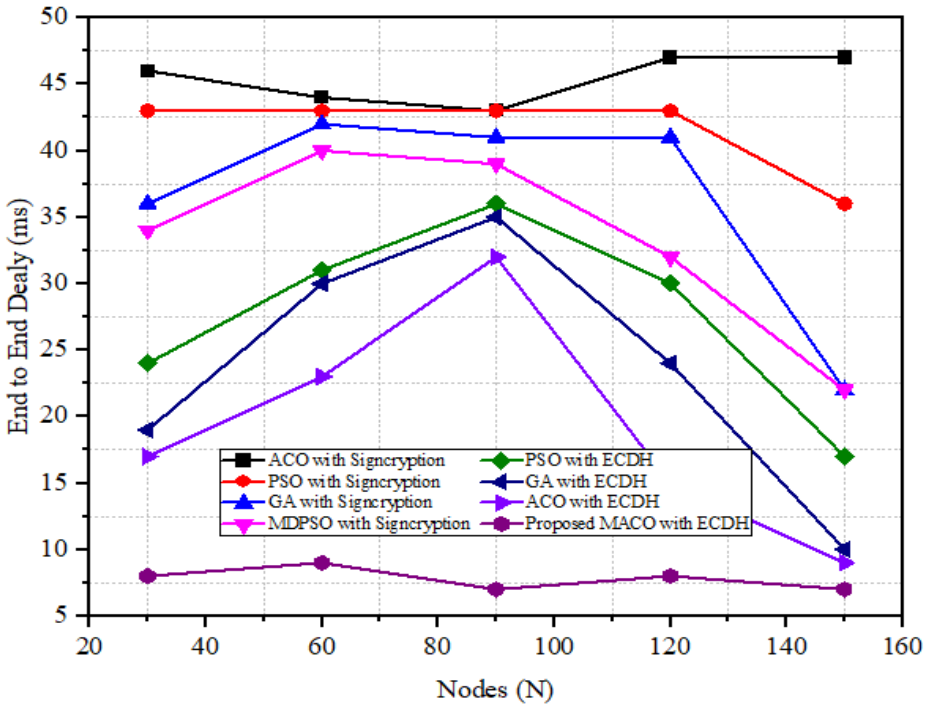

Fig. 4. Delay analysis (Minimal delay is better)

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.