MACO-DHKE Based Secure Data Transmission in MANETs

Original Scientific Paper

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

Abstract *– Mobile ad hoc networks (MANETs) are the self-sufficient nodes with their unique characteristics, such as open wireless mediums and self-motivated topology, which suffers from security weaknesses. Due to the complexity of the MANET security architecture, it is difficult to detect and prevent security issues in the wired networks. Hence, this paper proposes a secure and QoS-aware data transmission in the MANET that improves the efficiency of the transmission. The optimal route, which is the shortest possible path, is chosen using the modified ant colony optimization algorithm (MACO algorithm) and the secure transmission in MANET is ensured using the Diffie-Hellman key-exchange algorithm (DHKE strategy). The key exchange method is used to improve the security of the transmission of the MANET. This paper shows a high transmission rate on a secure path with a higher PDR and throughput.*

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

1. INTRODUCTION

The MANET network is a distributed multi-hop network composed of mobile nodes that can be used for various applications [1] [2]. These nodes can interact with each other in a multi-hop fashion. Each of the nodes in a network is a part of the same network, which means that they play an equal role in the transmission of data. The mobile devices in a network are known as routers, which are used to control and route the data packets. The routing protocol serves as a way for a network to establish contact with its source and destination. It also determines the best path for a packet to reach its intended destination. The MANET communication is investigated using several network parameters, such as packet delivery ratio (PDR), delay, distance, and so on, which are enclosed within the Quality of service (QoS) of the network [3]. The optimal route for availing quality-of-service is chosen using the following factors: MACO, HRM, and energy efficiency [2].

Outstanding routing techniques were developed with the goal of eliminating wasteful data transfer losses [20] [22]. Routing methods reduce routing communication to a bare minimum to ensure efficiency, but the resulting minimal data creates a barrier for a Routing Attack Detection System (RADS) [21]. The main issue with course disclosure is that it can result in loss of data. Fortunately, there are various algorithms that can help minimize this issue. Some of these include the Genetic algorithm, simulated annealing, and particle swarm optimization [2]. Secure routing techniques have been developed to protect MANETs from attacks, but these protocols do not protect additional data [23]. Because wireless sensor networks may be used in hostile environments such as battlefields [24] security in data communication is an important problem to consider when developing them. The Bee Ad Hoc fuzzy logic (FBeeAdHoc) framework has been used to provide a security layer for routing protocols in MANETs. In MANETS, the Homomorphic Encryption (HE) approach is used to accomplish multi-level security, which means that the data will be subjected to a cryptographic hash function and an encryption algorithm will be sent to the end, where the data will be decrypted and the data's dependability will be checked. The wormhole attack is one of the most serious security threats that can significantly disrupt network connectivity. When a node breaks the security standards and so becomes vulnerable to attack, this is referred to as malicious behavior [25].

The paper proposes a routing protocol that can increase distribution ratios and reduce end-to-end delay. It also uses the Diffie-Hellman algorithm to improve security of path. The paper is divided into four sections: Section 2, Section 3, Section 4, and Section 5. The topics covered by these sections include: (1) an overview of the concepts of routing and data protection (2) a comparison of various secure routing and protection protocols (3) a description of the characteristics of the proposed method.

2. LITERATURE REVIEW

In this section, the review of the existing literature is presented with the upcoming challenges of the research. An approach was proposed in 2019 to find the best CH for a stable MANET security level. The proposed model combines the number of attackers and the approximate distance and TV consumption of each certificate holder to ensure that the data is available and stable [1]. In 2019, Mariappan Rajashanthi and K. Vathi proposed a secure multipath routing scheme that is energy-efficient and has an encryption technique [4]. In 2018, the authors of this paper proposed various security-related regulations for data collection. They then reviewed the various methods and techniques related to MANET detection [5]. In 2017, the two authors updated the LEACH and AOMDV routing strategies. They provided a uniform approach for multipath routing and cluster generation [6]. In 2017, mobile ad hoc networks (MANETs) were introduced to the concept of security through the use of pre-existing routing protocols. The goal is to gain fast and secure communication while protecting the integrity and authenticity of the network [7].

The goal of a network is to receive and send messages from two users. To achieve this, the algorithm used to set the routing path was optimized. It allowed for better packet delivery and lower EC [8]. In 2018 [9], Mostafaei recommended a disseminated learning machine based calculation to work on the organization's exhibition with a few obliged QoS boundaries. It took a couple of QoS directing limitations into the record in way choice, like start to finish steady quality and deferral. As far as start to finish postponement and energy-viability, the outcomes showed that the estimation performed better compared to the present status of the craftsmanship brutal computations.

To decide the best area of the gathering particles, the fundamental multitude streamlining was refreshed. On account of a steady organization structure, one molecule is relied upon to decide the G-best position, and the leftover particles can search for additional spaces to confirm that the best position is G-best, not the flow one. In this article, Modified Ant Colony Optimization (MACO) is used to tackle the inadequacies of current renditions of MANET. Most of past research has focused on either energy productivity or unwavering quality; in any case, in this article, both energy-effective bunching and dependability are joined in a solitary MANET model.

3. PROPOSED SECURE TRANSMISSION IN MANET USING THE MACO ALGORITHM AND DHKE STRATEGY:

The method of sending information from a source to an objective without the need of a wired media is known as remote correspondence. A portion of the WSN's and MANET's elements are practically indistinguishable. In the modern days, MANET plays a significant role in rendering the network services equipped within the hand-held devices. Hence, there is a need to utilize the routing protocol for ensuring the easy access to the network services, where the optimal route is decided for reaching the services available through the hand-held devices. In this research, MACO algorithm is proposed for selecting the optimal communication path in MANET. Moreover, rendering security for the data provider and user is very significant, which is ensured using the DHKE strategy. The MACO algorithm and DHKE strategy are utilized in the MANET, which further promotes the QoS of the network.

3.1 MANET COMMUNICATION

The network is equipped with numerous sensor nodes, which are engaged in the data transmission in the network as shown in figure 2. Following table 1 shows the network parameters employed for simulating the MANET in NS2. The source node generates the request message for initiating the communication with the destination node, and the communication is preceded only if the security keys of both the source and destination nodes matches with each other. In this context, optimal route selection and selection of the secure path is the major focus.

3.2 PROPOSED MODIFIED ANT COLONY OPTIMIZATION (MACO) FOR OPTIMAL PATH SELECTION IN MANET:

In the MANET, ensuring the throughput rates is important to meet the client demands with an effective QoS. Due to different plan hardships and imperative satisfaction, conventional conventions fail to address the user challenges. Hence, upgrading throughput turns into a basic issue to fulfill client needs and application support. Therefore, throughput is the significant factor for rendering the required QoS for any kind of MANET applications and in this research, MACO streamlining technique considers throughput as one of the factor in selecting the optimal routing path for MANET communication.

3.2.1 Solution representation:

In a optimization algorithm, the solution representation signifies the solution declared by the algorithm. In this research, solution is the routing path with the source node as the initiating node or the data sender S and destination node D as the terminating node or the receiver, with the intermediating nodes $(I_1, I_2, \dots I_n) such that (n<m)$ being the communicating nodes between the source and destination nodes as shown in figure 1.

S	I_1	I_2	………………	D

Fig. 1. Solution representation

where, *m* is the total nodes in the MANET with *n* being the intermediate nodes in the communicating nodes.

3.2.2 Fitness measure:

The optimal solution, which is the optimal routing path, is decided by MACO using the fitness measures, such as throughput, PDR, routing overhead, and delay. The solution is selected as optimal when the throughput and PDR is high with the minimal overhead and transmission delay.

3.2.3 MACO description:

The MACO algorithm is the modified version of the ACO algorithm, which aims at the selection of the optimal route between the source and the destination nodes. The optimal route is the solution of MACO as per the figure 1. Technically, the solution or the route refers to the ants in the MACO and initially, the proposed MACO establishes the random solutions at the initial iteration, which is accompanied with the generation of all the possible routes between the source and the destination nodes, from which the optimal route satisfying the fitness measure is selected for communication.

The MACO builds the connection's packet transmission rate, bringing about a reasonable course choice arrangement. Forward ant is begun by the source hub at arbitrary to visit the entirety of the open hubs in the course [15]. During their crossing, the ants leave a little amount of pheromone on the visited joins. At the point when the ants show-up at their objective, the ants update the pheromone of all hubs visited all through the crossing. A hub's throughput is treated as a pheromone for this situation. The throughput work is utilized to refresh a hub's pheromone [16] [17].

Equation 1 is used to calculate $\mathrm{f(t)}$.

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

Where k denotes the packet transmission limit, $\mathrm{p(i)}$ is the number of packets successfully transferred, and $\mathrm{t(i)}$ 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 shown as follows:

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

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.

$$\rho_{ij}^{d}(t) = \frac{[\tau_{ij}(t)]^{\alpha}.[\mu_{ij}(t)]^{\beta}.[e_j(t)]^{\gamma}}{\sum_{j\in N}[\tau_{ij}(t)]^{\alpha}.[\mu_{ij}(t)]^{\beta}.[e_j(t)]^{\gamma}} \qquad (3)$$

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

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

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

Where, Δ_{ij}^{n} is the change in pheromone amount in the link ij, updated by the mth 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 proceeded until the state of stagnation is satisfied. The street that arises after a time of balance is viewed as the best way for correspondence. This methodology is done for every information transmission. This progression flags the beginning of the organization's transmission interaction. The figure 2 portrays the most limited way that is discovered utilizing AODV considering every one of the elements of MACO improvement calculation.

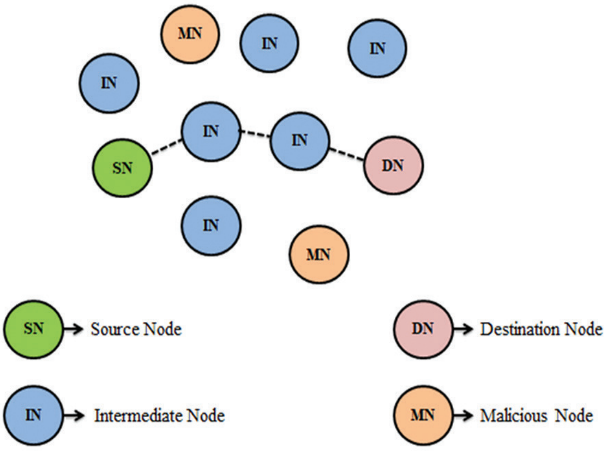

Fig. 2. MANET network

3.3 DHKE STRATEGY FOR THE SECURE COMMUNICATION IN MANETS

Using a finite number of nodes, a MANET is simulated in NS2, where the nodes communicate the data between the nodes only when the routing path offers better QoS with guaranteed security. Thus, security is ensured through DHKE strategy, which ensures the path is secure. Initially, find the source and destination nodes in the MANET for transferring the data packets between the nodes. The AODV routing protocol is used with MACO to identify the shortest path between these nodes. The shortest route from source to destination is chosen using MACO, where the security is guaranteed using DHKE [19].

First and foremost, a conduit from source to destination is constructed followed with the data transfer. Nodes at the source and destination locations for data transfer create two random numbers, p (prime number) and b (base number) in a DHKE-based strategy. The source node generates the private key Pk1 and the destination node generates the private key Pk2. Using the following formulas, two values A and B are calculated on the source and destination ends, respectively.

$$\mathrm{A} = \mathrm{bPk1modp} \tag{5}$$

$$\mathrm{B} = \mathrm{bPk2modp} \tag{6}$$

The values of A and B are exchanged across the nodes in order to calculate the secret key values at both ends. The formulae for computing the value of the secret key at the source and destination nodes are as follows:

$$\mathrm{Cs} = \mathrm{BPk1modp} \tag{7}$$

$$\mathrm{Ds} = \mathrm{APk2modp} \tag{8}$$

These secret key values are compared with each other for enabling the secure data transfer. Upon the mismatch in the secret keys between the source and destination nodes, the packets drop intimating the presence of the malicious nodes in the network thereby, blocking further communication. The DHKE strategy for secure path selection is depicted in figure 3 as a flowchart.

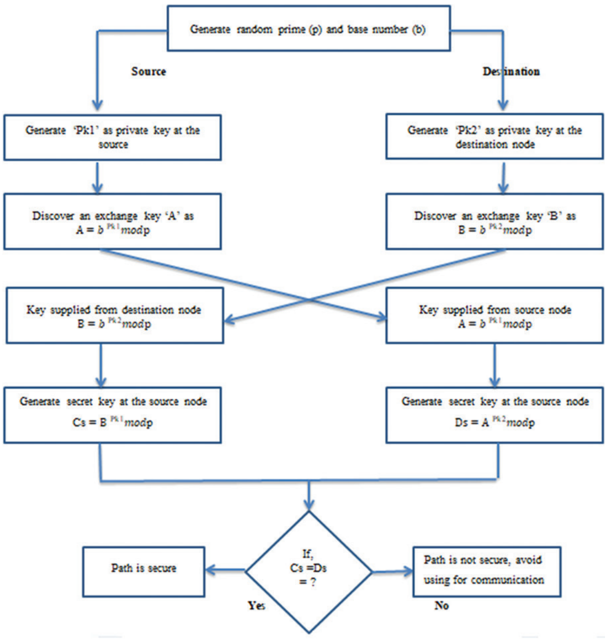
Generate random prime (p) and base number (b)
Source
Des ination
Generate 'Pk1' as private key at the source
Generate 'Pk2' as private key at the destination node
Discover an exchange key 'A' as A = $b^{Pk1}modp$
Discover an exchange key 'B' as B = $b^{Pk2}modp$
Key supplied from destination node B = $b^{Pk2}modp$
Key supplied from source node A = $b^{Pk1}modp$
Generate secret key at the source node Cs = $B^{Pk1}modp$
Generate secret key at the source node Ds = $A^{Pk2}modp$
Path is secure
If, Cs =Ds = ?
Path is not secure, avoid using for communication
Yes
No

Figure 3. Diffie-Hellman approach for checking whether path is secure or not

4. RESULT ANALYSIS

In this section, the achievements of the MACO with DHKE strategy are portrayed in order to enumerate the effectiveness compared with the existing state-of-art methods.

4.1 SIMULATION ENVIRONMENT:

The simulation is established in NS2 environment with the network settings shown in table 1. In the MANET network, a maximal of 150 nodes are distributed in the simulation area of coverage 1500 m × 1500 m.

Table 1. Parameters for simulation

Parameters	Network Settings
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

4.2 PERFORMANCE METRICS:

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

4.3 COMPARATIVE ANALYSIS:

The methods employed for the comparative analysis include: ACO, genetic algorithm (GA), particle swarm optimization (PSO), and MDPSO [1]. The difference in the packet delivery ratio (PDR) with respect to the quantity of hubs is displayed in Figure 4. The proposed MACO with DHKE acquires better PDR, throughput, delay and overhead when compared with the existing methods, like ACO with signcryption, PSO with signcryption, GA with signcryption, MDPSO with signcryption, PSO with DHKE, GA with DHKE, and ACO with DHKE. Table 2 shows the acquired throughput for the methods. The PDR, throughput, overhead and delay analysis is enumerated in figures (4) – (7) and tables (2) – (5).

The PDR analysis is performed with respect to the number of the nodes (in table 2), where it is highlighted that the PDR percentage shows slight improvement with the increasing number of nodes. Though the PDR decreases with the increasing number of nodes due to link failure, the application of the secure path selection method boosts the PDR through enhancing the link lifetime of the network. The proposed MACO with DHKE acquired the PDR of 97% when 150 nodes are communicating in the network, which is the best ever acquired PDR percenatge, which is mainly due to the development of the secure path selection mechanism.

The throughput analysis of the methods based on the total nodes is demonstrated in the figure 5. The throughput of the methods are affected when the transmission overhead prevails in the network due to the total number of users. When the total nodes is 150, the throughput acquired by the proposed MACO with DHKE is 4367 kbps, which is better when compared with the existing methods, justifying the effectiveness of the proposed method.

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

Number of nodes	ACO with signcryption	PSO with signcryption	GA with signcryption	MDPSO with signcryption	PSO with DHKE	GA with DHKE	ACO with DHKE	**proposed MACO with DHKE**
30	85	89	91	91	92	93	94	**94**
60	85	85	86	86	91	92	92	**94**
90	85	86	86	90	94	94	95	**96**
120	85	86	89	93	95	95	95	**95**
150	86	88	88	92	94	95	96	**97**

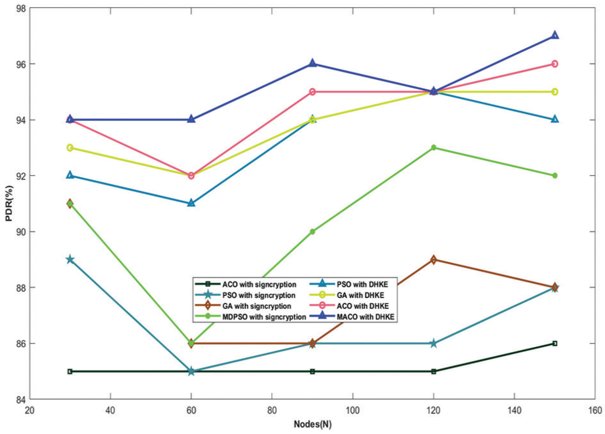

Fig. 4. Analysis based on PDR (Higher PDR is better)

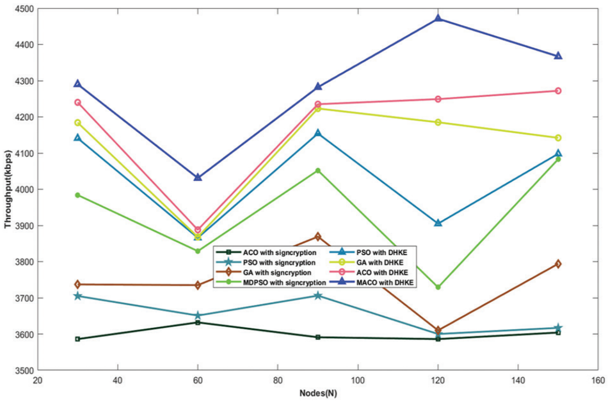

Fig. 5. Throughput analysis (Higher throughput is better)

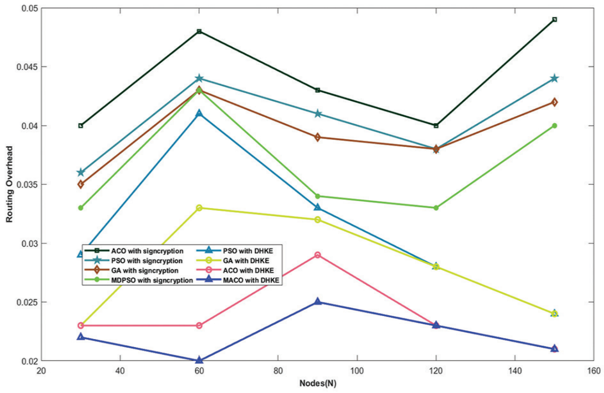

Fig. 6. Overhead analysis (Minimal overhead is better)

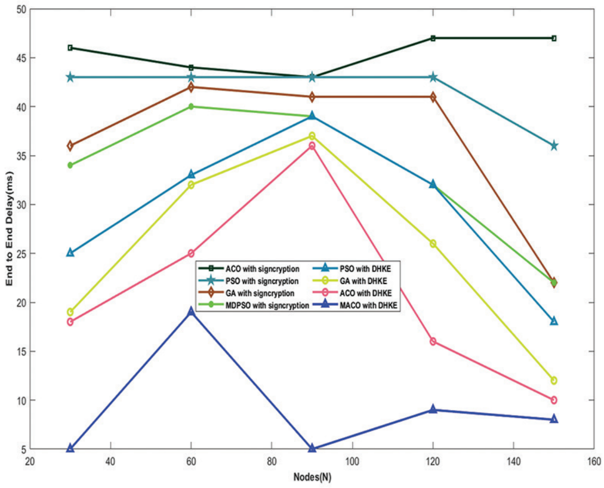

Fig. 7. Delay analysis (Minimal delay is better)

Similarly, the overhead analysis is performed, which focuses on the analysis of the computational complexity of the network when the node communication increases. When the total nodes is 30, the overhead is minimal, while the overhead incrases with the increase in the total simulated nodes in the network. However, when compared with the existing methods, the computational overhead of the proposed model is minimal, which insists that the proposed method schedules the communication through the optimal path.

Likewise, the delay analysis in the figure 7 insists that the effective performance of the network is based on the minimal delay of data communication between the nodes. For instance, as mentioned in the table 5, when the network is simulated with 150 nodes, the network communication delay is found to be around 8ms while using the proposed MACO with DHKE, which shows the siginificance of the proposed method in exhibiting the effective performance.

In short, the method that exhibts the minimal delay, minimal communication overhead, higher throuhgput and higher PDR are the best method. The proposed MACO with DHKE outperforms the existing methods with the minimal delay of 5ms with 30 and 90 nodes, and the minimal overhead of 0.02. On the other hand, the maximal PDR and throughput acquired by the proposed MACO with DHKE is 97% (with 150 nodes) and 4471 kbps (with 120 nodes), respectively.

Table 3. Throughput analysis (in kbps) (Higher throughput is better)

Number of nodes	ACO with signcryption	PSO with signcryption	GA with signcryption	MDPSO with signcryption	PSO with DHKE	GA with DHKE	ACO with DHKE	**proposed MACO with DHKE**
30	3586	3705	3737	3984	4141	4184	4240	**4290**
60	3632	3651	3735	3829	3866	3868	3888	**4031**
90	3591	3706	3869	4052	4154	4223	4235	**4282**
120	3586	3600	3610	3729	3905	4185	4249	**4471**
150	3604	3617	3794	4083	4098	4142	4272	**4367**

Table 4. Overhead analysis (Minimal overhead is better)

Number of nodes	ACO with signcryption	PSO with signcryption	GA with signcryption	MDPSO with signcryption	PSO with DHKE,	GA with DHKE	ACO with DHKE	**proposed MACO with DHKE**
30	0.04	0.036	0.035	0.033	0.029	0.023	0.023	**0.022**
60	0.048	0.044	0.043	0.043	0.041	0.033	0.023	**0.02**
90	0.043	0.041	0.039	0.034	0.033	0.032	0.029	**0.025**
120	0.04	0.038	0.038	0.033	0.028	0.028	0.023	**0.023**
150	0.049	0.044	0.042	0.04	0.024	0.024	0.021	**0.021**

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

Number of nodes	ACO with signcryption	PSO with signcryption	GA with signcryption	MDPSO with signcryption	PSO with DHKE,	GA with DHKE	ACO with DHKE	**proposed MACO with DHKE**
30	46	43	36	34	25	19	18	**5**
60	44	43	42	40	33	32	25	**19**
90	43	43	41	39	39	37	36	**5**
120	47	43	41	32	32	26	16	**9**
150	47	36	22	22	18	12	10	**8**

5. CONCLUSION:

With the aid of an MACO with DHKE approach, the researchers suggested a unique model for a secure transmission in the MANET. The MACO-based MANET routing was utilized to find the best and shortest path in the network. For data security in the MANET, the DHKE strategy is used, which determines whether the path between the source and destination nodes is safe. Furthermore, the suggested model combined the number of attackers with the performance evaluation procedure to examine the number of attackers. The performance of the proposed MACO with DHKE is enumerated based on the performance measures, such as delay, throughput, PDR, and overhead. The proposed method exhibts the minimal delay, minimal communication overhead, higher throuhgput and higher PDR of 5ms with 30 and 90 nodes, and the minimal overhead of 0.02, maximal PDR and throughput of 97% (with 150 nodes) and 4471 kbps (with 120 nodes), respectively. Furthermore, the suggested MACO with DHKE method achieved an improved result. To provide security in the MANET, backup routing in ad hoc networks (AODV) with a DHKE approach might be studied for detection of malicious node in future study. In addition, by combining bio-inspired and security algorithms, the performance of MANETs with security may be increased.

6. REFERENCES:

[1] M. Elhoseny, K. Shankar, "Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique", IEEE Transactions on Reliability, Vol. 69, No. 3, 2020, pp. 1077-1086.

[2] L. Harn, C. F. Hsu, O. Ruan, M. Y. Zhang, “The novel design of secure end-to-end routing protocol in wireless sensor networks”, IEEE Sensors Journal, Vol. 16, No. 6, 2016, pp. 1779–1785.

[3] K. Vijayan, A. Raaza, "A novel cluster arrangement energy-efficient routing protocol for wireless sensor networks", Indian J. Sci. Technol., Vol. 9, No. 2, 2016, pp. 1–9.

[4] M. Rajashanthi, K. A. Valarmathi, "Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs", Wireless Personal Communications, Vol. 112, 2020, pp. 75–90.

[5] G. Liu, Z. Yan, W. Pedrycz, "Data collection for attack detection and security measurement in mobile ad hoc networks: A survey", Journal of Network and Computer Applications, Vol. 105, 2018, pp. 105–122.

[6] B. Rana, D. Rana, "Energy efficient load balancing with clustering approach in MANET", Proceedings of the International Conference on Energy, Communication, Data Analytics and Soft Computing, Chennai, India, 1-2 August 2017, pp. 2019–2024.

[7] D. Hurley-Smith, J. Wetherall, A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", IEEE Transactions on Mobile Computing, Vol. 16, No. 10, 2017, pp. 2927-2940.

[8] Y. J. Oh, K. W. Lee, "Energy-efficient and reliable routing protocol for dynamic-property-based clustering mobile ad hoc networks", Int. J. Distrib. Sens. Netw., Vol. 13, No. 1, 2017.

[9] H. Mostafaei, "Energy-efficient algorithm for reliable routing of wireless sensor networks", IEEE Transactions on Industrial Electronics, Vol. 66, No. 7, 2019, pp. 5567–5575.

[10] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things", Neural Computing Applications, 2018, pp. 1–15.

[11] K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu, W. Wu, "An efficient optimal key based chaos function for medical image security", IEEE Access, Vol. 6, 2018, pp. 77145–77154.

[12] D. Gupta, A. Khanna, K. Shankar, V. Furtado, J. J. Rodrigues, "Efficient artificial fish swarm based clustering approach on mobility aware energy-efficient for MANET", Transactions on Emerging Telecommunications Technologies, 2018, Art. No. e3524.

[13] Y. Yang, "Broadcast encryption based non-interactive key distribution in MANETs", Journal of Computer and System Sciences, Vol. 80, No. 3, 2014, pp. 533–545.

[14] S. B. Prabaharan, R. Ponnusamy, " Enhanced Longevity of MANETs using ACO based Balanced Network Monitoring and Routing Model (BNMR)", Advances in Wireless and Mobile Communications, Vol. 10, No. 5, 2017, pp. 1035-1049.

[15] C. Ratanavilisagul, "Modified Ant Colony Optimization with Pheromone Mutation for Travelling Salesman Problem", Proceedings of the 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Phuket, Thailand, 27-30 June 2017.

[16] S. Kaur, R. Mahajan, "Hybrid meta-heuristic optimization based energy efficient protocol for wireless sensor networks", Egyptian Informatics Journal, Vol. 19, No. 3, 2018, pp. 145-150.

[17] Y. Gao, J. Wang, W. Wu, A. K. Sangaiah, S.-J. Lim, "A Hybrid Method for Mobile Agent Moving Trajectory Scheduling using ACO and PSO in WSNs", Sensors, Vol. 19, No. 3, 2019, p. 575.

[18] M. Alotaibi, "Security to wireless sensor networks against malicious attacks using Hamming residue method", EURASIP Journal on Wireless Communications and Networking, Vol. 8, 2019.

[19] O. Singh, J. Singh, R. Singh, "DHHP: A Hybrid Technique for Protecting Mobile Adhoc Networks from Selective Packet Drop Attack", International Journal of Computational Intelligence Research, Vol. 13, No. 7, 2017, pp. 1743-1763.

[20] M. Rajashanthi, K. Valarmathi, "A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs", Wireless Personal Communications, Vol. 112, 2020, pp. 75–90.

[21] G. Liu, Z. Yan, W. Pedrycz, "Data collection for attack detection and security measurement in mobile ad hoc networks: A survey", Journal of Network and Computer Applications, Vol. 105, 2018, pp. 105–122.

[22] R. Anita, “Joint cost and secured node disjoint energy efficient multipath routing in mobile ad hoc network”, Wireless Networks, Vol. 23, No. 7, 2017, pp. 2307–2316.

[23] D. Hurley-Smith, J. Wetherall, A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks," IEEE Transactions on Mobile Computing, Vol. 16, No.10, 2017, pp. 2927-2940.

[24] K. Vijayan, A. Raaza, “A novel cluster arrangement energy-efficient routing protocol for wireless sensor networks”, Indian Journal of Science and Technology, Vol. 9, No. 2, 2016, pp. 1–9.

[25] M. Rafsanjani, H. Fatemidokht, “FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs”, AEU-International Journal of Electronics and Communications, Vol. 69, No. 11, 2015, pp. 1613–1621.