Received: June 10, 2021. Revised: July 29, 2021.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Ant Colony Optimization Based Modified AODV for Secure Routing in Mobile Ad Hoc Networks

Mallikarjuna Anantapur[1]* **Venkanagouda Chanabasavanagouda Patil[1]**

[1]*Department of Electronics & Communication Engineering, Ballari Institute of Technology & Management, India*
* Corresponding author's Email: mallikarjunaa@bitm.edu.in

Abstract: Mobile Ad hoc Network (MANET) is an infrastructure-less wireless network that is characterized by multi-hop communication, dynamic network topology, open medium, and so on. MANET is generally vulnerable to security threats because of its decentralized control architecture. Therefore, the malicious attack is required to be avoided in the routing path for improving the network efficiency. In this paper, the Ant Colony Optimization (ACO) based Modified Ad-hoc On-Demand Distance Vector (MAODV) is proposed to obtain secure data transmission over the MANET. The ACO considers the four fitness functions such as trust, residual energy, distance, and node degree to detect an optimal path under the constraints of blackhole attacks. The main objective of the MAODV-ACO method is to improve the Packet Delivery Ratio (PDR) while minimizing the delay. The performance of the MAODV-ACO method is analyzed in terms of PDR, throughput, average End to End Delay (EED) and overhead. This proposed MAODV-ACO method is compared with Context-Aware Routing Protocol (CARP) and, Ad-hoc On-Demand Distance Vector (AODV) using Bayesian Approach and Dempster Shafer Theory (BA-DST) to evaluate the network performances. The PDR of the MAODV-ACO method is 99.66 % for 100 nodes, which is high when compared to the CARP and AODV-BA-DST.

Keywords: Blackhole attack, Mobile ad hoc network, Modified ad-hoc on-demand distance vector routing protocol, Trust, Packet delivery ratio.

1. Introduction

MANET is a set of self-organized wireless mobile nodes that can interact with each other without using fixed network infrastructure or centralized administration. Subsequently, the mobile nodes in the MANET communicate with each other over a wireless channel [1, 2]. The nodes of the MANET are used to accomplish both the hosts and routers for transmitting the data packets to the desired destination using the routing protocol [3, 4]. Moreover, the nodes in the MANET have three modes of operation which are transmission, calculation and sensing operation [5]. The node communication is restricted in the network based on the transmitter range. If two nodes are present within the transmission range, then the nodes can interact with each other. However, an intermediate node should be used, when the distance between a pair of nodes is too long in the network. This is obtained in two different ways such as single-hop and multi-hop routing methods [6]. Since, an important feature of the MANET are ease of organization, inexpensive, flexibility and multi-hop communication [7]. The aforementioned features make the MANET more applicable to real-time applications like battlefield communications, disaster management, environmental monitoring, and combat operations [8, 9].

Since the routing in the MANET is complex and difficult due to the frequent changes in the network topology and its higher unpredictable nature [10]. The nodes in the MANET are vulnerable to security threats because of the open structure and the restricted energy of the nodes. Some nodes are uncooperative or act maliciously which affects the efficiency, fairness, and reliability of the MANET [11, 12]. Therefore, the trust-based approaches are developed to collect the trust factors which evaluate

the target node using the trust model. Since the trust factor is information that defines the activities of the mobile nodes [13]. The trust established in the ad hoc networks is required to detect and avoid malicious nodes during the routing process [14]. The validation of trustworthiness is essential to assure resource sharing among only the trustworthy nodes. However, the trust level among the nodes is decreased, when there is an absence of the location which is updated in the ad-hoc on-demand vector protocol [15].

The major contributions of this research paper are given as follows:

- An AODV routing protocol is modified using the pheromone value of ACO which obtain to secure the data transmission from a source node to the destination node.
- The pheromone value of ACO is calculated using four different fitness values trust, residual energy, distance and node degree. Here, the trust value is computed based on the data forwarding among two nodes which used to detect the black hole attacks.
- Therefore, the black hole attacks present in the MANET are avoided using the trust value which assists to avoid the packet drop during the communication.

The overall organization of the paper is given as follows: Section 2 represents the literature survey about the trust-based routing algorithms developed for the MANET. A detailed explanation of the proposed MAODV-ACO method is described in Section 3. Section 4 presents the results and discussion of the MAODV-ACO method. Finally, the conclusion is made in Section 5.

2. Literature survey

Tripathy [16] presented the CARP that dynamically configures the routing operations according to the network. Here, the routing protocol was configured based on the following parameters such as the contextual features, behavioural dynamics and varying requirements. This adaptive routing protocol used control messages similar to the AODV protocol. Additionally, the recommendations from the adjacent nodes and behavioural inquiry of the nodes were used to design the trust model. Therefore, the developed context-aware routing was used to select the node with energy, trust and mobility. The calculation of the node was affected because of the recent activities of a node.

Pathan [17] developed the Trust-based Secure QoS Routing Scheme (TSQRS) that integrates the QoS trust and social trust. This TSQRS method was generated an appropriate path by selecting the node using the residual energy, channel quality and link quality. Moreover, the trust of adjacent nodes was used to identify and avoid intrusions during the communication. Next, the TSQRS method was used to minimize the route failure that increased the performances of the entire system. However, the path failure was occurred in the network due to the increment in breakage in links.

Xu [18] presented a Trust-based Probabilistic Broadcast scheme (TPB) to secure the data transmission. The previous communication among the nodes was used to compute the trust value of the nodes. Here, the rebroadcast order of the routing packets was computed using the rebroadcast delay based on the trust level. Next, the untrusted nodes were avoided in the route discovery using the probability of rebroadcast. This TPB method was used to minimize the amount of unwanted rebroadcasting packets. However, the TPB only considered the trust value of the nodes during the data transmission.

Vatambeti [19] developed the Grey Wolf Trust Accumulation (GWTA) approach to obtain trustful data transmission. The trust accumulation approach was accomplished in the grey wolf optimization to improve the identification and prevention approaches. This GWTA was used the monitoring node to observe the activities of the nodes. Moreover, the performance of the GWTA was affected due to the increment in the number of nodes.

Sarbhukan and Ragha [20] presented the BA and DST to calculate the trust value of the nodes. Here, the AODV routing protocol was used to transmit the data packets from the source to a destination node. The nodes with less trust value were avoided in the data transmission. Hence, the security of the MANET was increased using the unified trust management approach with the AODV protocol. But, this developed AODV protocol was considered the only trust during the communication which affected the MANET performances.

3. MAODV-ACO method

In this MAODV-ACO method, a MAODV routing protocol using ACO is used to avoid the blackhole attacks a secure data transmission over the MANET. The fitness function of the ACO considers four different fitness values like trust, residual energy, distance and node degree. Specifically, the trust value of nodes is considered in the ACO's fitness function helps to avoid the blackhole attacks while generating the path using the MAODV

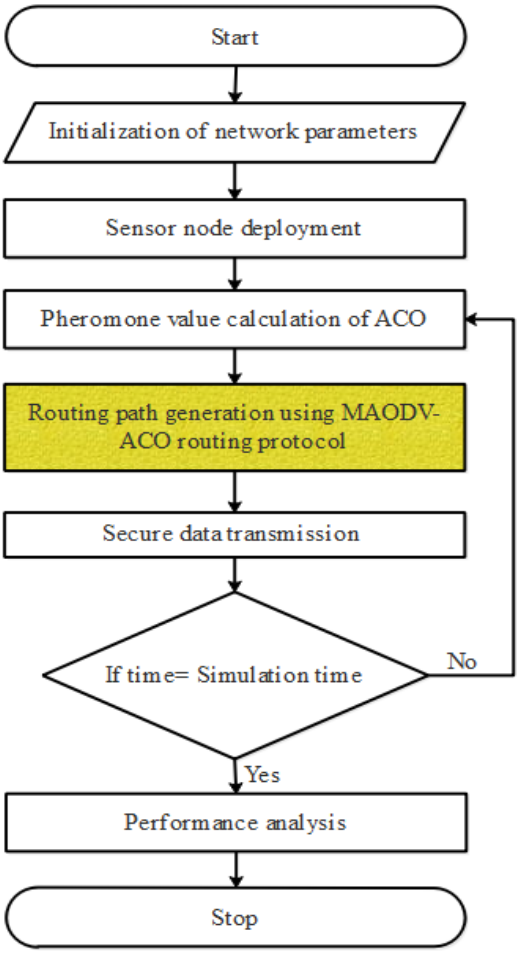

Figure. 1 Flowchart of the proposed method

protocol. However, the conventional AODV deliberates all the nodes in the MANET as cooperative which leads to susceptibility by the attacks. Therefore, the modified AODV routing protocol using ACO assists to avoid blackhole attacks which improves data transmission. The flowchart of the proposed method is shown in Fig. 1.

3.1 Calculation of pheromone value for ACO

In this proposed method, the conventional AODV routing protocol is combined with the ACO algorithm to avoid malicious attacks during data transmission. Here, the security is obtained by considering the trust values of the nodes in the fitness function of the ACO. Moreover, the fitness values of the ACO consider three more fitness values along with the trust such as residual energy, distance, and node degree which helps to improve the data transmission.

Generally, ACO is a metaheuristic algorithm that is inspired by the searching behavior of ants. In real life, the ants search together for identifying the route to the food source. The ants in the real-life emit the pheromone through the path, so that other ant discovers the trail in the same direction. Therefore, it has a better possibility for following the trail. Subsequently, the ants go in the same path and also emit some pheromone over the same path. Accordingly, the pheromone level of the path is exponentially increased as well as more ants probably use the same path for the searching process. Therefore, the ants follow the path which has the higher pheromone level. The same principle is combined in the AODV routing protocol to improve the searching process under blackhole attacks.

In the routing path identification, an adjacent node is not always considered desirable in the next-hop selection for the source node. Because the adjacent node may be an attacker node that drops the packet over the network. Hence, this scheme uses the pheromone value to select the next-hop and this pheromone value is expressed in Eq. (1).

$$PV = Trs + RE + D + ND \quad (1)$$

Where PV represents the pheromone value; Trs represents the trust value of the nodes; RE

represents the residual energy; D indicates the distance among the nodes and ND defines the node degree for the respective node.

3.1.1. Trust

Trust is considered an important objective in the MAODV-ACO method to improve security against blackhole attacks. The mobile nodes in the network establish communication based on mutual trust which is accomplished in a certain time interval. The trust value obtained from the direct communications is used as an important fitness value. Here, the trust between the nodes i and j is computed based on the forwarding ratio that is the ratio between the number of transmitted packets to the collected packets. The calculation of trust based on the forwarding ratio is expressed in Eq. (2).

$$Trs_{i,j}(t) = \frac{P_{i,j}^{T}(t)}{P_{i,j}^{C}(t)} \tag{2}$$

Where t defines the time; $P_{i,j}^{T}$ and $P_{i,j}^{C}$ represents the amount of transmitted and received packets between the nodes. The trust consideration in the ACO helps to avoid the blackhole attacks while generating the path.

3.1.2. Residual energy

The remaining energy in the node is defined as the residual energy which is used to perform different tasks like sensing, computation and communication. Therefore, the node with higher residual energy is preferred in routing path generation and Eq. (3) expresses the residual energy of the node.

$$RE = \frac{1}{E_i} \tag{3}$$

where, the residual energy of the i^{th} node is represented as E_i.

3.1.3. Distance

It defines the Euclidean distance between one node to another node. For an effective transmission, the routing path with a lesser distance to the DN is essential to minimize the energy consumption. The calculation distance between the node i and j is expressed in Eq. (4).

$$D = \sqrt{\left(x_i - x_j\right)^2 - \left(y_i - y_j\right)^2} \tag{4}$$

Where, x_i & y_i, and x_j & y_j are the coordinates of the node i and j.

3.1.4. Node degree

Node degree is defined as the number of nodes that are connected to the respective transmitter node in the network. In this MAODV-ACO, the node with a lesser amount of node degree is considered while generating the routing path.

3.2 Modified AODV routing using ACO

The calculated pheromone value from the ACO is integrated with the AODV routing to achieve a secure and reliable data transmission over the network. Generally, the conventional AODV is a reactive routing protocol that has two different phases as route discovery and route maintenance. There are four different types of control messages are used by this MAODV routing using ACO algorithm like Route Request (RREQ), Route Reply (RREP), Route Error (RERR), and hello (HELLO). The aforementioned control messages are used to discover the routing paths. Here, the pheromone value of the ACO is combined with the control messages of RREQ and RREP to avoid malicious attacks during the communication. This helps to minimize the packet drop in the network while minimizing the overhead of the MANET. The process of routing identification is accomplished, only when the source is required to forward the data packets to the destination node (DN).

3.1.5. Route identification process

The process of route identification of MAODV routing has three main steps.

Step 1: Initially, the source node (SN) broadcasts the RREQ messages to the adjacent nodes in the network. In this MAODV, the format of the RREQ message is changed by adding one more field namely the pheromone value. The modified RREQ message format and RREQ message distribution are shown in the following Fig. 2 and 3 respectively.

Here, the SN broadcasts the RREQ by fixing the pheromone value as 0. Each intermediate node adds the pheromone value with the previous node's pheromone value while propagating the RREQ messages in the network. Therefore, the pheromone value of the RREQ message defines the connectivity level, when it reaches the destination.

Step 2: The reverse route is generated with the SN, when an intermediate sensor doesn't have any route to the DN. After updating the collected RREQ

Src_address	Src_sequenceno	Request_id	Dest_address	Dest_sequenceno	Hop_Count	Pheromone level (PV)

Figure. 2 Modified RREQ format

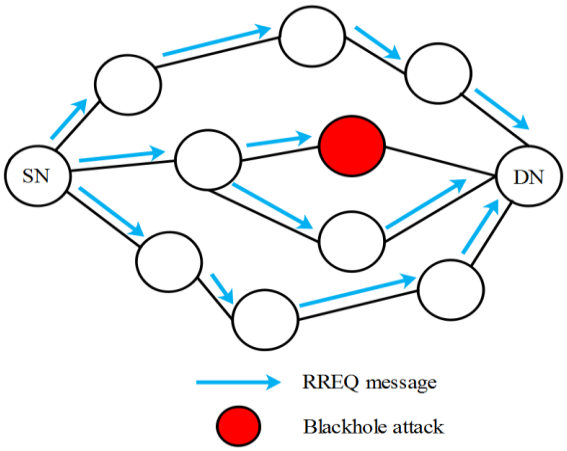

Figure. 3 RREQ message transmission of MAODV-ACO

message, the RREQ message is again broadcasted to the adjacent nodes in the network. A similar process is repeated until the RREQ message is received by the DN.

The pheromone value of the RREP message is updated in DN with the maximum pheromone value from the multiple RREQ messages. Subsequently, the path which has a higher pheromone value sends the RREP message. The RREP message is unicasted to the SN through the reverse routing when the DN receives the RREQ message. The RREP format is modified by adding one more extra field namely pheromone value as shown in Fig. 4. Next, the RREP transmission over the reverse route is illustrated in Fig. 5.

Step 3: In this step, the SN selects the routing path which has a higher pheromone value. Then the SN starts to forward the packets to the desired DN.

3.1.6. Route maintenance

The MAODV-ACO frequently transmits the HELLO messages to maintain the routes. If the HELLO message is not received from an adjacent node, then the MAODV-ACO considers that the respective link is broken during the communication.

Source_address	Destination_address	Destination_sequenceno	Lifetime	HopCount	Pheromone level (PV)

Figure. 4 Modified RREP format

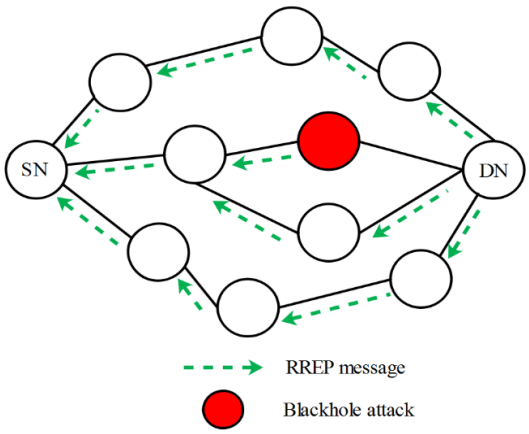

Figure. 5 RREP message transmission of MAODV-ACO

The secure data transmission over the MANET is obtained by considering the trust value of the nodes in the MAODV-ACO. An average EED is minimized by identifying the shortest path using the ACO. Moreover, the node failure is avoided in the MAODV-ACO by considering the residual energy during the routing path generation.

4. Results and discussion

The performance analysis of the proposed MAODV-ACO method is shown in this section.

Here, the NS-2 simulator with a version of 2.34 is used in the Ubuntu 16.04 OS platform to evaluate the performances of the MAODV-ACO method. Secure communication over the MANET is achieved using the ACO-based MAODV routing for data transmission. The simulation is carried out over the area of $300 \times 300\ m^2$ with the IEEE 802.11 MAC. Subsequently, the mobile nodes are varied as 80, 90 and 100 for demonstration purposes. The specifications used in the MAODV-ACO method are given in Table 1.

Table 1. Specification parameters

Parameter	Value
Area	$300 \times 300\ m^2$
Number of nodes	80, 90 & 100
Routing protocol	MAODV-ACO
Initial energy	2J
MAC protocol	IEEE 802.11
Packet size	512 Bytes
Traffic type	CBR/ UDP
Antenna model	Omnidirectional
Propagation model	Two ray ground
Network interface type	Phy/WirelessPhy
Attack	Blackhole attack
Simulation time	300s

4.1 Performance analysis

The performance of the MAODV-ACO method is analyzed as PDR, throughput, average end-to-end delay and overhead. Here, the MAODV-ACO method is compared with the CARP [16] and AODV-BA-DST [20] to justify the efficiency of the MAODV-ACO method. The performance analysis is described as follows:

4.1.1. Packet delivery ratio

PDR is defined as the ratio between the amount of received packets to the amount of generated packets which is expressed in Eq. (5).

$$PDR = \frac{\sum_0^n Packets\ received}{\sum_0^n Packets\ sent} \times 100\ \% \qquad (5)$$

Where, n defines the node count.

Fig. 6 and Table 2 show the PDR comparison for the MAODV-ACO method with the CARP [16] and AODV-BA-DST [20]. From Fig. 6 and Table 2, it is concluded that the PDR of the MAODV-ACO method is better than the CARP [16] and AODV-BA-DST [20]. For example, the MAODV-ACO is 99.48 % for 80 nodes which is high when compared to the CARP [16] and AODV-BA-DST [20]. The MAODV-ACO method achieves higher PDR to avoid link failure and blackhole attacks during the communication.

Table 2. Performance analysis of PDR

Number of nodes	CARP [16]	AODV-BA-DST [20]	MAODV-ACO
80	96 %	95 %	99.4877 %
90	97.5 %	88 %	99.8711 %
100	97 %	90 %	99.6644 %

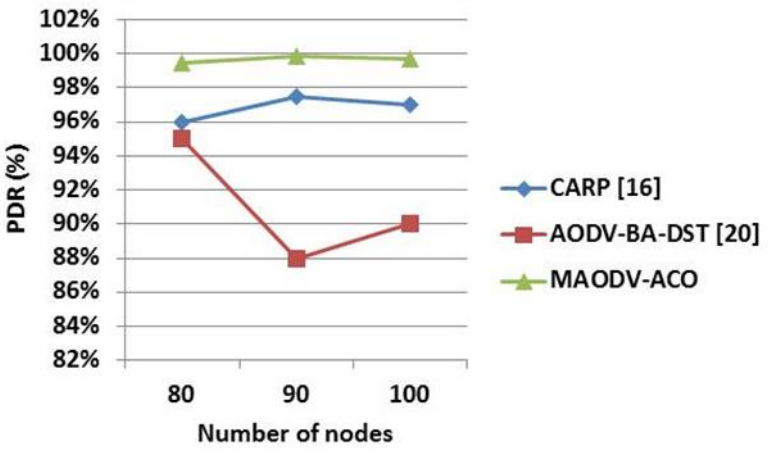

Figure. 6 Comparison of PDR

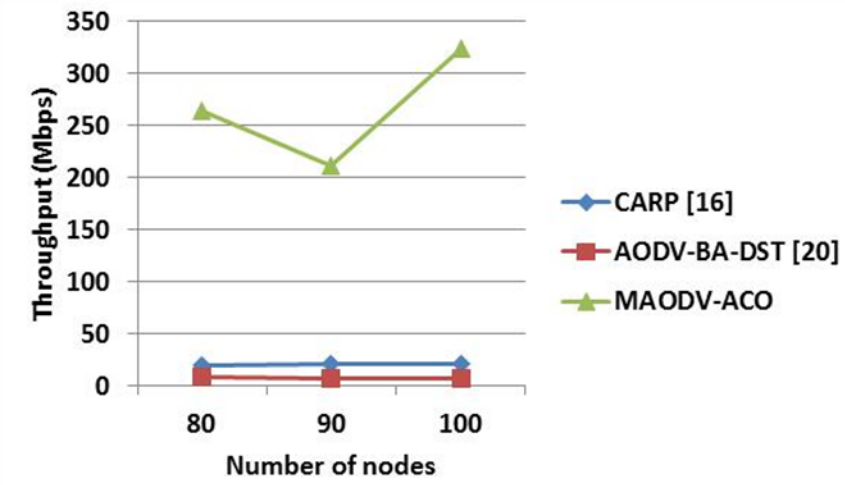

Figure. 7 Comparison of throughput

4.1.2. Throughput

The success rate of data transmission over the communication channel is defined as throughput which is analyzed in bits per second (bps). Moreover, the throughput is considered an important parameter to analyze the MAODV-ACO's efficiency. Eq. (6) expresses the throughput.

$$Throughput = \frac{\sum_0^n Packet\ received\ (n) \times Packetsize}{1000} \quad (6)$$

The throughput comparison among the CARP [16], AODV-BA-DST [20] and MAODV-ACO is presented in Table 3 and Fig. 7. From the analysis, it is concluded that the throughput of the MAODV-ACO is higher than the CARP [16] and AODV-BA-DST [20]. The throughput of the MAODV-ACO is increased based on the following reasons such as optimal node selection using the ACO's fitness function and 2) blackhole attack mitigation using the trust value of the nodes.

Table 3. Performance analysis of throughput

Number of nodes	CARP [16]	AODV-BA-DST [20]	MAODV-ACO
80	20.2 Mbps	8.23 Mbps	264.485 Mbps
90	20.9 Mbps	7.59 Mbps	211.098 Mbps
100	20.7 Mbps	6.83 Mbps	323.592 Mbps

4.1.3. Average end to end delay

Average EED is an average time required for the successful transmission of data packets from the source to the destination and this average EED is expressed in Eq. (7).

$$Average\ EED = \frac{1}{n}\left(\sum_0^n Packet\ received\ time\ (n) - Packet\ sent\ time\ (n)\right) \quad (7)$$

An average EED comparison among the CARP [16], AODV-BA-DST [20] and MAODV-ACO is presented in Table 4 and Fig. 8. From the analysis, it is concluded that the average EED of the MAODV-

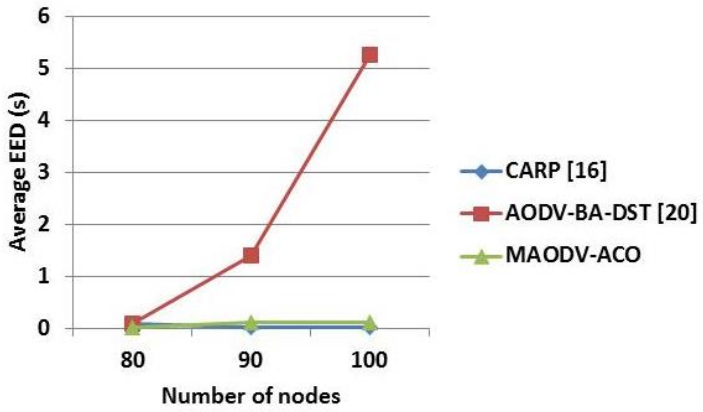

Figure. 8 Comparison of average EED

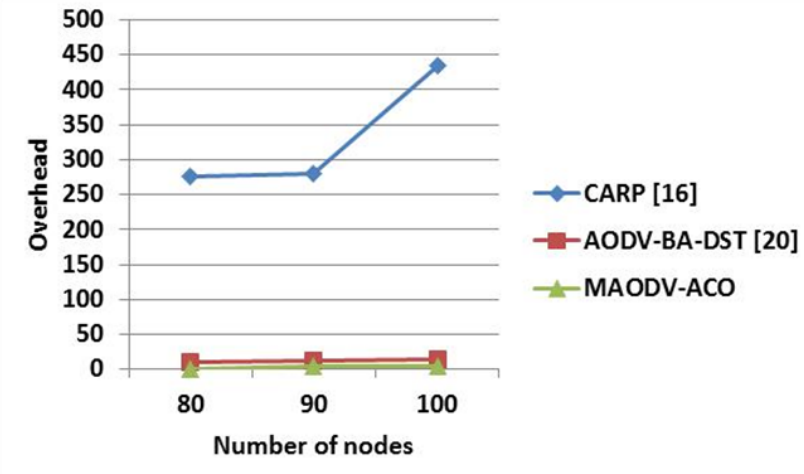

Figure. 9 Comparison of overhead

Table 4. Performance analysis of average EED

Number of nodes	CARP [16]	AODV-BA-DST [20]	MAODV-ACO
80	0.09 s	0.1 s	0.0321 s
90	0.02 s	1.4 s	0.1269 s
100	0.02 s	5.26 s	0.1180 s

ACO is improved than the CARP [16] and AODV-BA-DST [20].

The delay of the MAODV-ACO for 80 nodes is 0.0321 which is less than the CARP [16] and AODV-BA-DST [20]. However, the AODV-BA-DST [20] causes higher delay, because it doesn't consider the distance while generating the routing path.

4.1.4. Overhead

Overhead is the ratio among the amount of generated control packets to the amount of packets received by the destination.

Fig. 9 and Table 5 show the overhead comparison of the MAODV-ACO method with the CARP [16] and AODV-BA-DST [20]. Fig. 9 and Table 5, shows that the overhead of the MAODV-ACO method is less than the CARP [16] and AODV-BA-DST [20]. For example, the AODV-BA-DST [20] causes higher overhead because it transmits a high amount of control messages while generating the routing path. But, the MAODV-ACO method doesn't transmit more control packets due to the pheromone level considered in the fitness function.

Table 5. Performance analysis of overhead

Number of nodes	CARP [16]	AODV-BA-DST [20]	MAODV-ACO
80	275	10.8	0.424305
90	280	12.6	4.49677
100	435	13.8	4.93855

The data delivery of the MAODV-ACO method is improved based on the optimal node identification during the routing path generation and mitigation of blackhole nodes by using the trust values of the nodes. For example, the PDR of the MAODV-ACO method is 99.66 % for 100 nodes, which is high when compared to the CARP [16] and AODV-BA-DST [20]. Next, the MAODV-ACO method identifies the routing path with less transmission distance which results in lesser delay. Moreover, less overhead is achieved by the MAODV-ACO method, because of the pheromone level considered in the ACO algorithm. Therefore, the MAODV-ACO method provides better PDR while minimizing the overhead of the network.

5. Conclusion

In this paper, a MAODV-ACO routing protocol is utilized to mitigate the blackhole attacks to achieve a secure data transmission in the MANET. The pheromone value of the ACO is identified using four fitness values such as trust, residual energy, distance, and node degree. Here, the trust value computed from the data forwarding ratio is used to minimize the packet loss by mitigating the blackhole attack. Therefore, the selection of data forwarding nodes using MAODV-ACO helps to improve the PDR of the network. Moreover, the control packets transmitted for route establishment are minimized by avoiding link failure and blackhole attacks. Accordingly, the overhead of the MAODV-ACO is minimized as well as delay is minimized by identifying the shortest path in the MANET. The MAODV-ACO outperforms well when compared to the CARP and AODV-BA-DST. The PDR of the MAODV-ACO method is 99.66 % for 100 nodes, which is high when compared to the CARP and AODV-BA-DST. In future, the performance of the

MANET can be improved by using a novel optimization algorithm.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] L. G. Delgado, E. P. Segarra, A. M. Mezher, and J. Forné, "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, No. 1, pp. 1-16.

[2] M. M. Mukhedkar and U. Kolekar, "E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network", *International Journal of Communication Systems*, Vol. 33, No. 7, pp. e4252, 2020.

[3] M. E. Semary and H. Diab, "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map", *IEEE Access*, Vol. 7, pp. 95197-95211, 2019.

[4] U. Venkanna, J. K. Agarwal, and R. L. Velusamy, "A cooperative routing for MANET based on distributed trust and energy management", *Wireless Personal Communications*, Vol. 81, No. 3, pp. 961-979, 2015.

[5] R. T. Merlin and R. Ravi, "Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET", *Wireless Personal Communications*, Vol. 104, No. 4, pp. 1599-1636, 2019.

[6] M. Malathi and S. Jayashri, "Modified Bi-directional Routing with Best Afford Path (MBRBAP) for Routing Optimization in MANET", *Wireless Personal Communications*, Vol. 90, No. 2, pp. 861-873, 2019.

[7] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET", *Wireless Networks*, Vol. 25, No. 4, pp. 1685-1695, 2019.

[8] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network", *Security and Communication Networks*, 2021.

[9] R. J. Cai, X. J. Li, and P. H. J. Chong, "An evolutionary self-cooperative trust scheme against routing disruptions in MANETs", *IEEE Transactions on Mobile Computing*, Vol. 18, No. 1, pp. 42-55, 2018.

[10] V. Keerthika and N. Malarvizhi, "Mitigate black hole attack using hybrid bee optimized weighted trust with 2-opt AODV in MANET", *Wireless Personal Communications*, Vol. 106, No. 2, pp. 621-632, 2018.

[11] M. N. Ahmed, A. H. Abdullah, H. Chizari, and O. Kaiwartya, "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs", *Journal of King Saud University-Computer and Information Sciences*, Vol. 29, No. 3, pp. 269-280, 2017.

[12] K. R. Abirami, and M. G. Sumithra, "Preventing the impact of selfish behavior under MANET using Neighbor Credit Value based AODV routing algorithm", *Sādhanā*, Vol. 43, No. 4, pp. 1-7, 2018.

[13] S. Tan, X. Li, and Q. Dong, "Trust based routing mechanism for securing OSLR-based MANET", *Ad Hoc Networks*, Vol. 30, pp. 84-98, 2015.

[14] R. Menaka, V. Ranganathan, and B. Sowmya, "Improving performance through reputation based routing protocol for manet", *Wireless Personal Communications*, Vol. 94, No. 4, pp. 2275-2290, 2017.

[15] G. Dhananjayan and J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET", *Springer Plus*, Vol. 5, No. 1, pp. 1-16, 2016.

[16] B. K. Tripathy, S. K. Jena, P. Bera, and S. Das, "An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks", *Wireless Personal Communications*, Vol. 114, pp. 1339-1370, 2020.

[17] M. S. Pathan, N. Zhu, J. He, Z. A. Zardari, M. Q. Memon, and M. I. Hussain, "An efficient trust-based scheme for secure and quality of service routing in MANETs", *Future Internet*, Vol. 10, No. 2, p. 16, 2018.

[18] H. Xu, H. Si, H. Zhang, L. Zhang, Y. Leng, J. Wang, and D. Li, "Trust-based probabilistic broadcast scheme for mobile ad hoc networks", *IEEE Access*, Vol. 8, pp. 21380-21392, 2020.

[19] R. Vatambeti, "A Novel Wolf Based Trust Accumulation Approach for Preventing the Malicious Activities in Mobile Ad Hoc

Network", *Wireless Personal Communications*, Vol. 113, No. 4, pp. 2141-2166, 2020.

[20] V. V. Sarbhukan and L. Ragha, "Establishing secure routing path using trust to enhance security in MANET", *Wireless Personal Communications*, Vol. 110, No. 1, pp. 245-255, 2019.