Received: October 19, 2021. Revised: December 9, 2021. 

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# Priority Based Trust Efficient Routing Using Ant Colony Optimization for IoT-based Mobile Wireless Mesh Networks

**Sudhakar Karna Narayana[1]*** **Naveen Thimmahanumaiah Hosur [2]**

[1]*CMR Institute of Technology, Bengaluru, India*
[2]*Government Engineering College, K R Pet, India*
* Corresponding author's Email: sudhakar.kn@cmrit.ac.in

**Abstract:** Wireless Mesh Networks (WMNs) are considered as an important structure for the next generation wireless networks that have numerous nodes organized in the mesh topology. In WMN, the data packets are forwarded through the multi-hop model. Nowadays, the combination of mesh clients with the Internet of Things (IoT) is gaining substantial importance for connecting numerous machines and it is used to acquire faster coverage. Moreover, the nodes in the WMN are susceptible to the malicious nodes which transmit the compromised and manipulated data to the destination. In this research, the Priority based Trust Efficient Routing using Ant Colony Optimization (PTER-ACO) is proposed to achieve data privacy and reliable routing over the WMN. Subsequently, Advanced Encryption Standard (AES) and Rivest Cipher 6 (RC6) are used to provide added security to the data. The PTER-ACO is analyzed by means of energy efficiency, network throughput, Packet Loss Rate (PLR), computational overhead, and latency. The existing methods such as Improved version of the Dijkstra Algorithm (IDA), Round Trip Time (RTT) based detection and Robust and Trusted Scheme (RTS) are used to evaluate the PTER-ACO, against these methods. The PLR of the PTER-ACO method is 21 % for 10 malicious nodes, which is less when compared to the IDA, RTT and RTS.

**Keywords:** Ant colony optimization, Energy efficiency, Internet of things, Mobile wireless mesh networks, Packet loss rate, Priority based trust efficient routing protocol.

## 1. Introduction

WMN is a self-configured and self-organized network where the nodes establish mesh connectivity between each other by generating an ad hoc network [1, 2]. WMN is used in various applications such as transportation systems, broadband home networking, emergency response communications, public safety, community networks, and building automation [3]. WMN comprises of a gateway, as well as two different types of nodes known as mesh clients, and mesh routers [4, 5, 6]. Mesh router is installed with multiple radio interfaces linked with many wireless channels, whereas the mesh clients have a single radio interface. Besides, the common channel medium is established between the mesh clients and routers to accomplish smooth communication [7]. The WMN is designed to deliver widespread network coverage without using any centralized infrastructure. Therefore, the WMNs can act as a backbone network for metropolitan area networks. In such networks, the gateways i.e., the wireless node with a rapid wired connection to the external Internet, is used to offer the Internet connection to the WMN [8, 9].

The developed WMN is generally a wireless multihop technology that is similar to the mobile ad hoc networks as well as it is assumed as a superset of the ad hoc network [10]. In a WMN, an end to end node is located beyond the radio transmission ranges. Therefore, intermediate nodes are required to be selected for transmitting the data among the nodes that are not in the transmission range. The routing algorithm is required to be developed to select the subset of intermediate nodes for generating the routing path from the source node to the destination [11, 12]. Generally, the multicast routing developed over the WMN is susceptible to various malicious

attacks. The effect of the attack over the multicast environment is high when compared to the unicast environment because a single malicious attack disturbs the data transmission towards many destinations [13]. Additionally, the routing over the mesh networks is challenging as the environment is unstable, hostile and restricted by the interference [14]. Meanwhile, the link disruptions, protocol errors and congestion causes the packet drop over the WWN during the communication [15].

The major contributions of this research are given as follows:

- At first, the routing between the source to the destination is achieved using the PTER-ACO, where trust is considered as an important cost value to achieve secure data transmission.
- Next, two-level encryption is developed for improving the security of the data packets.
- The developed PTER-ACO provides a better security over the WMN while minimizing the energy consumption during the data transmission.

Here, the developed PTER-ACO method is analyzed for varying malicious nodes to evaluate the data delivery over the network.

The overall organization of the paper is given as follows: Section 2 specifies the related work about the recent researches done in secure routing over the WMN. The clear description about the proposed PTER-ACO method is provided in the section 3. Section 4 provides the results and discussion of the PTER-ACO method. Finally the conclusion is made in section 5.

## 2. Related work

Roy and Khan [16] presented an effective handoff authentication protocol along with the privacy protection of nonce and transmitted the ticket against external attacks at the handoff process. Additionally, the robustness from the internal attacks was obtained using the round trip time (RTT) based detection protocol. The transfer ticket and nonce were encrypted to obtain the privacy protection of the transfer ticket and nonce. Therefore, the RTT was used to prevent the AODV routing, from a wormhole attack. Here, the detection of malicious nodes was obtained by computing the processing time and RTT. However, the AODV routing only depended on the RTT.

Navmani and Yogesh, [17] developed the trust based secured reliable routing (TSRR) protocol to generate the reliable routing path for infrastructure-based WMN. Moreover, the node's forwarding reliability and trusted nodes were considered to form the reliable routing path. In mesh routers, the cross layer and subject logic based dynamic reputation (CLSL-DR) method was developed to preserve the WSN from misdirecting and packet dropping attacks. The developed CLSL-DR decreased the control packets that were forwarded during the route discovery. This CLSL-DR failed to consider the distance in route discovery, therefore it generated the path with a high distance which caused higher energy consumption.

Shi [18] presented an IDA for generating the secure route for WSNs. In this secure routing protocol, the node's related information such as trust value, distance to the sink node and residual energy were considered for each intermediate node of a transmission path, because the trust value is the node's attack probability that is computed based on the previous packet-forwarding process. The route near the sink was selected to minimize the delay and energy of the node. However, the IDA cannot be used for analysis in the large scale environment.

Roy and Khan [19] developed the detection technique for the wormhole attack by using the processing time and RTT. Besides, the probability of delay was calculated for transmitting and receiving packets among the relay nodes, in each routing path. The developed RTT-based attack detection was used to protect the AODV protocol against wormhole attacks. If the source sequence number was not updated in the AODV, then the intermediate node created inconsistent routing path.

Haseeb [20] presented a robust and trusted scheme (RTS) for IoT based mobile WMN to offer data security. At first, the data routing among the gateway devices, mesh clients, and routers were achieved by using the RTS based on the packet loss rate. Next, the public-private key cryptography was used to improve the mesh client protection with less overhead. However, the RTS considered only the PLR for accomplishing the routing between the nodes of WMN.

## 3. PTER-ACO method

The main aim of the proposed PTER-ACO method is to perform an effective secure data transmission over the IoT based MWMN. The security of the IoT based MWMN is developed based on the following two strategies that are: secure routing path generation using PTER-ACO and data security based on two level encryption. Generally, the mesh clients, routers, and gateway devices (i.e., Base station) are linked through the multi-hop model for

constructing the topological infrastructure as shown in Fig. 1. With the help of the basic information obtained from the topological infrastructure, and cost metrics derived using trust, QUN, link quality and distance, a secure data transmission path is detected by using the PTER-ACO. Specifically, trust is considered as the primary factor that helps to mitigate the malicious nodes during the communication. Subsequently, the AES and RC6 are used in the two level encryption to provide added security for the data. Therefore, the security over the IoT based MWMN is improved while minimizing the energy consumed by the mesh clients / routers. Fig. 2 illustrates the flow chart of the PTER-ACO method.

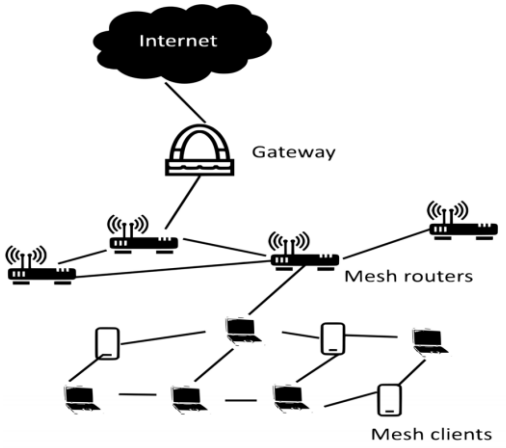


Figure. 1 Architecture of wireless mesh network

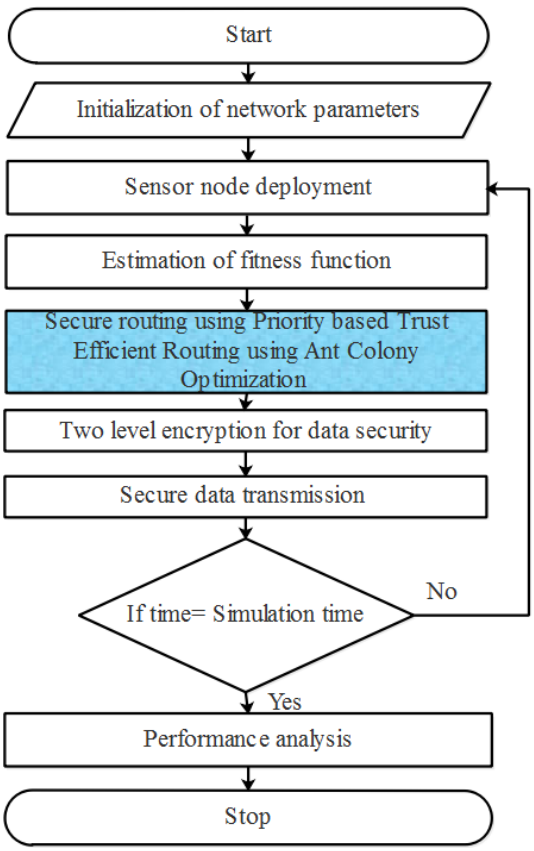


Figure. 2 Flow chart of the PTER-ACO method

### 3.1 Priority based trust efficient routing using ACO

Initially, the mesh clients and mesh routers broadcast their location information to generate the routing table. Next, the routing table is updated whenever a new mesh client is connected / disconnected the network. Each mesh node forwards its information such as unique ID and current location over the network for generating the transmission path. Here, the transmission path between the source mesh client and destination mesh router is identified by using PTER-ACO method. Generally, ACO is one of the metaheuristic algorithms that is utilized to resolve optimization problems. One such issue is discovering the shortest path among two points. Therefore artificial ants are developed in the ACO for imitating behaviors of real ants to discover the optimal path. The process of route generation using PTER-ACO is given in the following steps:

1. At first, the route setup packets namely forward ant packets (FAP) are generated by the source mesh client.
2. Subsequently, the generated FAPs are randomly broadcasted to the successive next hop nodes until the FAP reaches the destination. The nodes referred to in the ACO are mesh clients or mesh routers that exist in IoT based MWMN.
3. Each packet generates a local database about its routing path, where the database has the information about the path's cost value such as trust metric, queue utilization between nodes (QUN), link quality and distance.
4. The backward ant packet is created using the local database, once the FAP reaches the destination. Subsequently, this backward ant is navigated in the same path that was used during the forward journey (i.e., destination mesh router to the source mesh client).
5. The pheromone of each path is updated in the backward journey by using the cost metrics.
6. Further, the pheromone dropped by all ants is used to update the probability matrix. Eq. (1) expresses the probability value of an ant $k$ traveling from one node $i$ to another node $j$.

$$P_{ij}^{k}(t) = \begin{cases} \dfrac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}}{\sum_{l \in allowed_k}[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}} & \text{if } j \in allowed_k \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Where the pheromone value of path from the node $i$ to node $j$ is represented as $\tau_{ij}$; the iteration number is denoted as $t$; $\eta_{ij}$ is the heuristic value of the ant that is calculated as $\eta_{ij} = 1/d_{ij}$; $d_{ij}$ defines the distance between the node $i$ and $j$; the constant parameters utilized for adjusting the influence of pheromones are $\alpha$ and $\beta$, and the nodes which are not visited by the $k$ th ant is represented as $allowed_k$ . The aforementioned metrics contribute to the decision-making of ants.

The value of the pheromone trail for each ant is updated in each iteration to identify the optimal path. Eq. (2) is used to accomplish the local update of PTER-ACO.

$$\tau_{ij}(t+1) = (1-\rho)\tau_{ij}(t) + \Delta\tau_{ij} \tag{2}$$

Where, the evaporation rate of pheromone is denoted as $\rho$ that controls the evaporation speed, the minimization of $\tau_{ij}$ is regulated by the $\rho \in [0, 1]$ and the current iteration's pheromone value is represented as $\Delta\tau_{ij}$ which is expressed in Eq. (3).

$$\Delta\tau_{ij} = \sum_{k=1}^{M} \Delta\tau_{ij}^{k} \tag{3}$$

The pheromone left by ant $k$ leaving the node $i$ and reaching the node $j$ is computed by using the Eq. (4).

$$\Delta\tau_{ij}^{k} = \frac{Q}{c_k} \tag{4}$$

Where $Q$ is the constant and $c_k$ is the cost metric identified by $k$th ant.

#### 3.1.1. Cost metric derivation

The cost metrics used in the PTER-ACO method are trusted metric, QUN, link quality, and distance. Therefore, the designed cost metrics are used to avoid the malicious nodes by providing a high priority to the trust value for the trust metric during the routing process. The subsets of the cost metrics such as QUN, link quality, and distance are used to improve the performance in terms of energy consumption and overhead.

**a. Trust metric**

Trust is considered as a primary cost value for the routing over the IoT based MWMN which is used to enhance the security against the malicious nodes. The mobile nodes in the IoT based MWMN communicate with each other by using the mutual trust accomplished among the nodes in the time interval. Direct trust is generally a packet forwarding behavior which is the proportion among the number of transmitted packets ($TP_{ij}$) and the number of received packets ($RP_{ij}$). The direct trust degree is calculated based on the following Eq. (5).

$$Trust = \frac{TP_{ij}}{RP_{ij}} \tag{5}$$

The trust value is used to mitigate the malicious nodes while generating the routing path.

**b. QUN and link quality**

QUN is defined as the ratio among the number of packets occupied in the queue of $j$th node $(QUN_j)$ and the total amount of available packets in the respective node's queue ($QUN_{total}$). Eq. (6) is used to compute the QUN.

$$QUN = \frac{QUN_j}{QUN_{total}} \tag{6}$$

Link quality is defined as the ratio among the amount of transmission and retransmissions which are essential for the successful transmission of data packets between node $i$ and $j$.

$$Link\ quality = \frac{1}{f \times r} \tag{7}$$

Where, $f$ and $r$ represent the forward and reverse data delivery between the nodes.

**c. Distance**

Euclidean distance between the nodes is calculated to identify the shortest path over the IoT-based MWMN and the euclidean distance is calculated by using Eq. (8).

$$Distance = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \tag{8}$$

Where, $x_i, x_j$ and $y_i, y_j$ are the coordinates of the nodes $i$ and $j$.

In PTER-ACO, a weight value ($\delta$) is considered to convert each cost value into a single cost value as shown in the Eq. (9).

$$c_k = \delta_1 \times Trust + \delta_2 \times QUN + \delta_3 \times Link\ quality + \delta_4 \times Distance \tag{9}$$

Where the weighted values $\delta_1, \delta_2, \delta_3$ and $\delta_4$ are equal to 0.35, 0.25, 0.25 and 0.15 respectively. The derived cost function of Eq. (9) is used in Eq. (4)

where it is used to update the pheromone value of ants. Based on the updated pheromone value, the probability value is calculated as per Eq. (1). With the help of the trust metric, the malicious nodes which cause the packet drop are avoided while generating the routing path. Next, the QUN and link quality are considered in the cost metric for generating the route with less traffic. This helps to minimize the collision during the communication and increases the packet delivery. Further, the shortest path is identified for minimizing the energy consumption of the nodes.

#### 3.1.2. Data transmission

In IoT based MWMN, each mesh client registers its ID in the routing table, once it receives the data. After receiving the data, the mesh client starts forwarding the data to the desired destination. If the source mesh client receives many detection messages from its neighbor mesh clients, then the PTER-ACO considers the path which has a higher pheromone rate. The mesh clients which have a one-hop connection with the mesh router perform the direct data transmission whereas the mesh clients which are far from the mesh router perform the multichip communication using the PTER-ACO. Therefore, the data packets are forwarded through the path which has a higher pheromone rate.

### 3.2 Data security using two level encryption

The added security is provided for the data transmitted from the mesh clients to the mesh routers by using two level encryption. The term two level encryption defines that there are two different encryption algorithms used for two different blocks of a given input. Specifically, the input packet given at the source mesh client is divided into two sub-blocks. The encryption algorithms used in the IoT based MWMN are AES and RC-6, where these algorithms are randomly taken between each sub-blocks. The divided sub-blocks are $pkt_1[0:((L/2)-1)]$ and $pkt_2[(L/2):(L-1)]$, where $L$ is the length of data packets. At first, the first $L/2$ data packets are encrypted by using the AES with the key of $K_{AES}$. The data separation of $L/2$ data packets and AES encryption over those packets are expressed in the Eqs. (10) and (11) respectively.

$$pkt_1 = \sum_{l=0}^{l=\frac{L}{2}-1} Data\ packets_l \quad 0 \le l \le (L/2)-1 \quad (8)$$

$$C_1 = Enc_{AES}(K_{AES}, pkt_1) \quad (9)$$

Where, the data encrypted using AES is $C_1$. Similarly, the $pkt_2[(L/2):(L-1)]$ block of data packets is encrypted using the RC6 algorithm. Moreover, the RC6 used in the PTER-ACO method increases the security level of data without maximizing the execution time. The second sub-block of data separation and RC6 encryption over those packets are expressed in the Eqs. (10) and (11) respectively.

$$pkt_2 = \sum_{l=\frac{L}{2}}^{l=L-1} Data\ packets_l \quad (L/2) \le l \le (L/2)-1 \quad (10)$$

$$C_2 = Enc_{RC6}(K_{RC6}, pkt_2) \quad (11)$$

Where, the $C_2$ represents the encrypted data using $RC6$. The encrypted data are combined and transmitted from the mesh client to the mesh router. Further, the data are decrypted using the inverse operation of the encryption process.

## 4. Results and discussion

The results and discussion of the PTER-ACO method are provided in this section. The implementation and simulation of the PTER-ACO method are conducted using network simulator-3 where the system uses the 4-GB RAM and Intel Core processor. The PTER-ACO method is used to obtain the secure routing between the source mesh client to the destination mesh router. The mesh clients in the PTER-ACO method are randomly deployed in the area of $500 \times 500m^2$ where the malicious nodes are varied from 2 to 10 to analyze the performances. The simulation specifications are mentioned in Table 1.

The performance of the PTER-ACO method is analyzed in terms of energy efficiency, network throughput, packet loss rate, computational overhead and latency. The existing methods such as IDA [18], RTT [19] and RTS [20] are designed by using the

Table 1. Simulation parameters

| Parameter | Value |
|---|---|
| Area | $500 \times 500m^2$ |
| Number of mesh clients | 200 |
| Deployment | Random |
| Malicious nodes | 2 to 10 |
| MAC layer | IEEE 802.11b |
| Wireless propagation protocol | TwoRayGround |
| Traffic type | CBR |
| Packet size | 250 bits |
| Network interface type | WirlessPhy |
| Antenna pattern | OmniAntenna |
| Queue type | PriQueue |
| Simulation time | 1000 s |

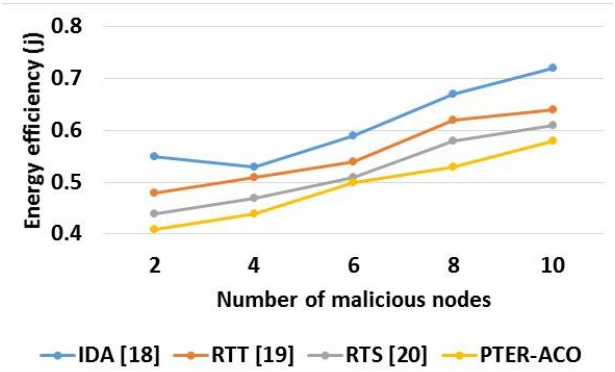


Figure. 3 Comparison of energy efficiency

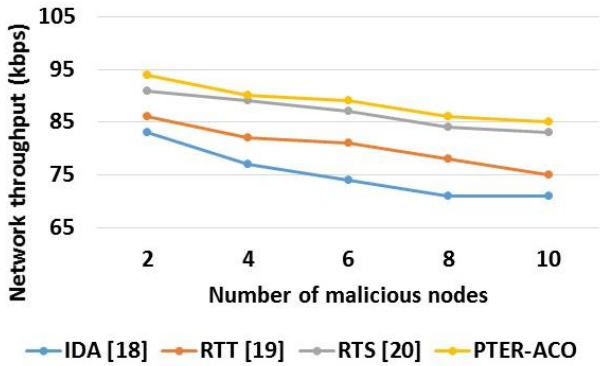


Figure. 4 Comparison of throughput

same specification mentioned in Table 1 to analyze the PTER-ACO method.

**a. Energy efficiency**

Energy efficiency represents the amount of energy consumed while transmitting and receiving the data packets.

Fig. 3 shows the energy consumption comparison for PTER-ACO method with IDA [18], RTT [19] and RTS [20] methods. From Fig. 3, it is known that the energy consumption of the PTER-ACO is less when compared to the IDA [18], RTT [19] and RTS [20]. The energy consumption of the PTER-ACO method is less due to its shortest path generation.

**b. Network throughput**

The comparison of throughput for PTER-ACO method with IDA [18], RTT [19] and RTS [20] is shown in Fig. 4. From Fig. 4, it is known that the throughput of the PTER-ACO is high when compared to the IDA [18], RTT [19] and RTS [20]. The mitigation of malicious nodes helps to increase the throughput.

**c. Packet loss rate**

PLR is the proportion between the amount of

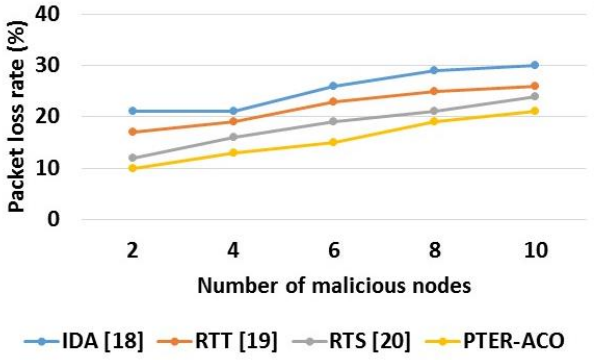


Figure. 5 Comparison of packet loss rate

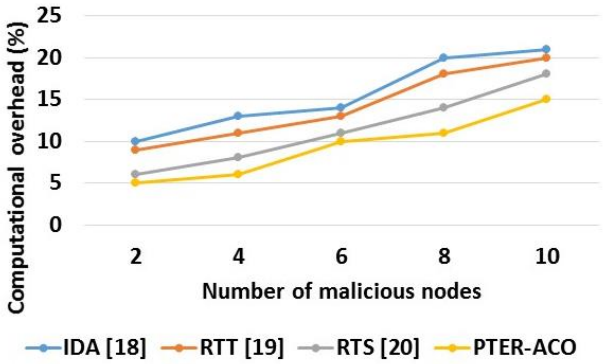


Figure. 6 Comparison of computational overhead

dropped data packets and the number of packets generated by the source mesh client. This PLR is shown in the following Eq. (16).

$$PLR = \frac{Amount\ of\ dropped\ packets}{Amount\ of\ generated\ packets} \times 100 \quad (16)$$

Fig. 5 shows the PLR comparison for PTER-ACO method with IDA [18], RTT [19] and RTS [20] methods. From Fig. 5, it is known that the PLR of the PTER-ACO is less when compared to the IDA [18], RTT [19] and RTS [20]. An appropriate selection of routes without any malicious nodes is used to minimize the PLR.

**d. Computational overhead**

The computational overhead is the ratio of the number of control packets generated during route discovery to the number of packets received at the gateway.

The comparison of computational overhead for the PTER-ACO method with IDA [18], RTT [19] and RTS [20] is shown in Fig. 6. From Fig. 6, it is known that the computation overhead of the PTER-ACO is less when compared to the IDA [18], RTT [19] and RTS [20]. The developed PTER-ACO method requires only less control packets during the route

Table 2. Comparative analysis of PTER-ACO method

| Performances | Methods | Number of malicious nodes | | | | |
|---|---|---|---|---|---|---|
| | | 2 | 4 | 6 | 8 | 10 |
| Energy efficiency (j) | IDA [18] | 0.55 | 0.53 | 0.59 | 0.67 | 0.72 |
| | RTT [19] | 0.48 | 0.51 | 0.54 | 0.62 | 0.64 |
| | RTS [20] | 0.44 | 0.47 | 0.51 | 0.58 | 0.61 |
| | PTER-ACO | 0.41 | 0.44 | 0.50 | 0.53 | 0.58 |
| Network throughput (kbps) | IDA [18] | 83 | 77 | 74 | 71 | 71 |
| | RTT [19] | 86 | 82 | 81 | 78 | 75 |
| | RTS [20] | 91 | 89 | 87 | 84 | 83 |
| | PTER-ACO | 94 | 90 | 89 | 86 | 85 |
| Packet loss rate (%) | IDA [18] | 21 | 21 | 26 | 29 | 30 |
| | RTT [19] | 17 | 19 | 23 | 25 | 26 |
| | RTS [20] | 12 | 16 | 19 | 21 | 24 |
| | PTER-ACO | 10 | 13 | 15 | 19 | 21 |
| Computational overhead (%) | IDA [18] | 10 | 13 | 14 | 20 | 21 |
| | RTT [19] | 9 | 11 | 13 | 18 | 20 |
| | RTS [20] | 6 | 8 | 11 | 14 | 18 |
| | PTER-ACO | 5 | 6 | 10 | 11 | 15 |
| Latency (ms) | IDA [18] | 0.0263 | 0.0281 | 0.0288 | 0.0294 | 0.0301 |
| | RTT [19] | 0.0231 | 0.0260 | 0.0269 | 0.0281 | 0.0286 |
| | RTS [20] | 0.0222 | 0.0243 | 0.0260 | 0.0268 | 0.0277 |
| | PTER-ACO | 0.0210 | 0.0235 | 0.0251 | 0.0258 | 0.0262 |

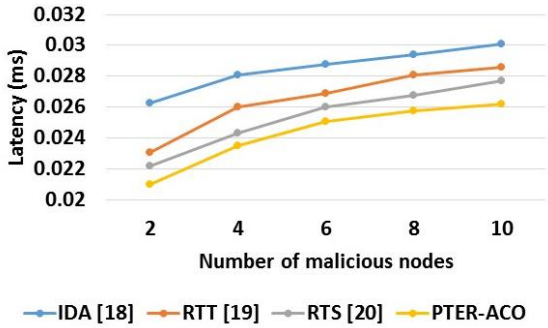


Figure. 7 Comparison of latency

discovery, hence the computational overhead is less when compared to the IDA [18], RTT [19] and RTS [20].

**e. Latency**

Fig. 7 shows the latency comparison for the PTER-ACO method with IDA [18], RTT [19] and RTS [20] methods. From Fig. 7, it is known that the latency of the PTER-ACO is less when compared to the IDA [18], RTT [19] and RTS [20]. The shortest path selection using the PTER-ACO is used to minimize the latency during the transmission. Table 2 shows the comparative analysis of the PTER-ACO method. From the Table 2, it can be concluded that the proposed PTER-ACO method provides better performance than the IDA [18], RTT [19] and RTS [20]. Due to appropriate fitness function of PTER-ACO method, it minimizes the packet drop caused by the malicious nodes and the congestion. On the other hand, the data transmitted over the WMN is further secured by using a two-level encryption (i.e., AES and RC6). Moreover, the energy consumption and latency of the PTER-ACO method are minimized based on the shortest path generation.

## 5. Conclusion

In this paper, ant colony optimization (PTER-ACO) is developed for IoT-based mobile WMN to perform a secure data transmission. The cost metrics such as trust, QUN, link quality, and distance are derived by using the basic information obtained from the topological infrastructure. Subsequently, the derived cost metrics are used in the PTER-ACO to obtain the secure data transmission path. Specifically, trust is considered as the primary factor that helps to mitigate the malicious nodes during the communication. Subsequently, the AES and RC6 were used in the two level encryption to provide added security for the data. Therefore, the security in the IoT based MWMN is improved while minimizing the energy consumed by the mesh clients / routers. From the performance analysis, it is concluded that the PTER-ACO provides better performance than the IDA, RTT and RTS. The PLR of the PTER-ACO method is 21 % for 10 malicious nodes, which is lesser when compared to the IDA, RTT and RTS. In future, a novel optimization technique can be used for improving the performances of WMN.

## 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] S. Sakamoto, T. Oda, M. Ikeda, L. Barolli, and F. Xhafa, "Implementation and Evaluation of a Simulation System based on Particle Swarm Optimisation for Node Placement Problem in Wireless Mesh Networks", *International Journal of Communication Networks and Distributed Systems*, Vol. 17, No. 1, pp. 1-13, 2016.

[2] M. Gheisari, J. Alzubi, X. Zhang, U. Kose, and J. A. M. Saucedo, "A New Algorithm for Optimization of Quality of Service in Peer to Peer Wireless Mesh Networks", *Wireless Networks*, Vol. 26, No. 7, pp. 4965-4973, 2020.

[3] R. Murugeswari, S. Radhakrishnan, and D. Devaraj, "A Multi-Objective Evolutionary Algorithm based QoS routing in Wireless Mesh Networks", *Applied Soft Computing*, Vol. 40, pp. 517-525, 2016.

[4] Y. Chai, W. Shi, and T. Shi, "Load-aware cooperative hybrid routing protocol in hybrid wireless mesh networks", *AEU - International Journal of Electronics and Communications*, Vol.74, pp.135-144, 2017.

[5] G. Akilarasu and S. M. Shalinie, "Privacy Preserving Protocol for Secure Routing in Wireless Mesh Networks", *International Journal of Mobile Network Design and Innovation*, Vol. 8, No. 1, pp. 54-59, 2018.

[6] X. Deng, L. He, Q. Liu, X. Li, L. Cai, and Z. Chen, "EPTR: Expected Path Throughput based Routing Protocol for Wireless Mesh Network", *Wireless Networks*, Vol. 22, pp. 839-854, 2016.

[7] Y. Chai and X. J. Zeng, "Delay- and Interference-Aware Routing for Wireless Mesh Network", *IEEE Systems Journal*, Vol. 14, No. 3, pp. 4119-4130, 2020.

[8] A. A. Saadi, R. Setchi, Y. Hicks, and S. M. Allen, "Routing Protocol for Heterogeneous Wireless Mesh Networks", *IEEE Transactions on Vehicular Technology*, Vol. 65, No. 12, pp. 9773-9786, 2016.

[9] J. Li, B. N. Silva, M. Diyan, Z. Cao, and K. Han, "A Clustering Based Routing Algorithm in IoT Aware Wireless Mesh Networks", *Sustainable Cities and Society*, Vol. 40, pp. 657-666, 2018.

[10] G. Akilarasu and S. M. Shalinie, "Wormhole-Free Routing and DoS Attack Defense in Wireless Mesh Networks", *Wireless Networks*, Vol. 23, No. 6, pp. 1709-1718, 2017.

[11] C. Zhang, C. Li, and Y. Chen, "A Markov Model for Batch-Based Opportunistic Routing in Multi-Hop Wireless Mesh Networks", *IEEE Transactions on Vehicular Technology*, Vol. 67, No. 12, pp. 12025-12037, 2018.

[12] X. Shao, R. Wang, H. Huang, and L. Sun, "Load Balanced Coding Aware Multipath Routing for Wireless Mesh Networks", *Chinese Journal of Electronics*, Vol. 24, No. 1, pp. 8-12, 2015.

[13] R. Matam and S. Tripathy, "Secure Multicast Routing Algorithm for Wireless Mesh Networks", *Journal of Computer Networks and Communications*, Vol. 2016, p. 1563464, 2016.

[14] U. S. Kushwaha, P. K. Gupta, and S. P. Ghrera, "Performance Evaluation of AOMDV Routing Algorithm with Local Repair for Wireless Mesh Networks", *CSI Transactions on ICT*, Vol. 2, pp. 253-260, 2015.

[15] Y. Tsado, K. A. A. Gamage, B. Adebisi, D. Lund, K. M. Rabie, and A. Ikpehai, "Improving the Reliability of Optimised Link State Routing in a Smart Grid Neighbour Area Network based Wireless Mesh Network Using Multiple Metrics", *Energies*, Vol. 10, No. 3, p. 287, 2017.

[16] A. K. Roy and A. K. Khan, "Privacy preservation with RTT-based detection for wireless mesh networks", *IET Information Security*, Vol. 14, No. 4, pp. 391-400, 2020.

[17] T. M. Navmani and P. Yogesh, "Trust based Secure Reliable Route Discovery in Wireless Mesh Networks", *KSII Transactions on Internet and Information Systems*, Vol. 13, No. 7, pp. 3386-3411, 2019.

[18] Q. Shi, L. Qin, Y. Ding, B. Xie, J. Zheng, and L. Song, "Information-aware secure routing in wireless sensor networks", *Sensors*, Vol. 20, No. 1, p. 165, 2020.

[19] A. K. Roy and A. K. Khan, "RTT based wormhole detection for wireless mesh networks", *International Journal of Information Technology*, Vol. 12, pp. 539-546, 2020.

[20] K. Haseeb, I. U. Din, A. Almogren, N. Islam, and A. Altameem, "RTS: A Robust and Trusted Scheme for IoT-based Mobile Wireless Mesh Networks", *IEEE Access*, Vol. 8, pp. 68379-68390, 2020.