A Secure Routing Protocol for MANET using Neighbor Node Discovery and Multi Detection Routing Protocol

T.V.Suresh Kumar[#1], Dr.Prabhu G Benakop[*2]

[#1] *Research Scholar, Electronics and Communication Engineering, JNTUH Hyderabad, Telangana, India.*
[*2] *Principal, Methodist College of Engg & Tech., Hyderabad, Telangana, India.*

Abstract:

Mobile Ad hoc Networks is enormously used owing to its mobility in addition to flexibility in a widespread range of applications. Since, the mobile ad hoc network is an autonomous system which is generated by mobile nodes without any infrastructure support. The cooperative and dynamic nature of the MANET affects the data transmission through the network. Therefore, the secure routing protocol is required to develop for protecting the routing and application data. In this paper, a neighbor node discovery is developed for identifying the black hole nodes in the MANET. Additionally, the multi detection routing protocol is used to generate the routing path through the network. The key objective of this research is to generate the routing path without any interruption of black hole nodes. The performance of the proposed technique is analyzed in terms of energy consumption, lifetime, packet delivery ratio, throughput and end to end delay. Additionally, the proposed method is estimated with the existing method namely EIMO–ESOLSR. The energy consumption of the proposed technique is 115J for 10 misbehaving nodes which is less than the EIMO-ESOLSR

Keywords: *Black hole node, mobile ad hoc network, multi detection routing protocol, neighbor node discovery and secure routing protocol.*

I. INTRODUCTION

MANET is generally a pool of self-sustaining movable nodes that communicated over the wireless connections [1]. The nodes in the MANET has the responsibility for transmitting the data as well as the unpredictable MANET structure is created, when the nodes are randomly join or leave the network while transmitting the data packets [2]. The nodes of the MANET is act as source as well as a router [3]. Since, the MANET is operated in the infrastructure-less environment that doesn't has any central infrastructure to manage the network functions. The mobile node in the MANET has restricted transmission range i.e., a few 100 meters. Hence, the intermediate nodes are used to perform the data transmission, when the desired node is not in the transmission range [4] [5]. This is obtained by using the two kinds of MANET networks such as single-hop and multi-hop [6]. Generally, the routing protocols in the MANET is classified into three types such as proactive, reactive, and hybrid protocols [7]. The MANET is used in various applications such as smart agriculture, disaster recovery, military applications, scientific research and wildlife monitoring [8].

The major characteristics of the MANET are limited battery power, limited bandwidth and dynamic topology. This characteristic creates the difficulty while generating the transmission path in the MANET [9] [10]. The inherent characteristic of the MANET such as dynamic topology and open wireless medium causes the network as susceptible to security threats. Therefore, it is to deliver the secure and trusted communication over the MANET [11]. The selfish or malicious node affects or even rejects the data transmission of any node which present in the networking domain [12]. Besides, the packet drop through the network is mainly depends on the malicious node or threats [13][22]. Since, the network without any centralized infrastructure is required to be use the trusted certification authority or key distribution center for delivering the cryptographic keys to improve the authentication during transmission [14][23]. The security mechanism used in the MANET required to provide the integrity, authentication, non-repudiation, confidentiality and availability over data transmission [15][24]. The major aids of this research are given as follows:

- The black holes in network are detected by using the neighbor node discovery during communication. This neighbor node discovery is required to be used only once to detect the black holes. This helps to minimize unwanted energy dissipation through the network.
- A multi detection routing protocol is used to identify the shortest path through the network. Since, the information about the black hole

nodes are incorporated in the routing to mitigate the black hole nodes.
- Therefore, a secure data transmission is achieved in this MANET while conserving the energy consumption of the nodes.

The overall organization of this paper are given as follows: The literature survey about the secured routing techniques in MANET are given in the section 2. The developed neighbor node discovery and multi detection routing protocol for identifying the shortest path without any black hole nodes are clearly described in the section 3. The performance examination of the proposed technique is given in the section 4. Finally the conclusion is made in section 5.

II. LITERATURE SURVEY

Khamayseh, Y.M., Aljawarneh, S.A. and Asaad, A.E [16] presented the energy-efficient detection method for increasing the network lifetime. The on-going data transmission over the network is observed by using a cooperative environment. The observer node is initialized to identify either the data is transmitted to the next hop node or not through the network. The observer node transmits the error message namely OERR to the source node. Hence, the middle node is marked as black hole, when the source node receives frequent OERR messages. This protocol avoids the link failure and reduces the overhead during communication.

Kasthuribai, P.T. and Sundararajan, M [17] developed the Particle Swarm Optimization Gravitational Search Algorithm (PSOGSA) algorithm for creating the secure and energy aware routing over the MANET. This approach helps to detect the multipath routes as well as it mitigates the network from selfish nodes or attackers. After processing more amount of transmissions, the route losses link quality. Subsequently, the cuckoo search procedure is used to select an appropriate path from the established routes. This PSOGSA selects energy efficient multipath routes through the network.

Jamaesha, S.S. and Bhavani, S [18] presented the location based routing with trusted security to transmit the data in the network. The cluster based routing among the nodes is used to accomplish the data transmission. In that clustering, the position of the cluster members is identified by using the PSO. Moreover, the malicious node is detected by exchanging the random number among the nodes. Since, the trust value is calculated from the neighbor table and the malicious node detection helps to decrease the packet loss. Additionally, the security of the data is improved by using the Elliptic Curve Cryptography (ECC) method.

Merlin, R.T. and Ravi, R [19] developed the Trust based Energy Aware Routing (TEAR) method for avoiding the Black Hole (BH) in route generation. The dynamic creation of multiple detection path is used for identifying the BH and the nodal trust is used for securing the data route. Therefore, the developed TEAR method effectively controls both the generation and exchanging of the multiple detection paths to detect the BHs. Here, the data and energy efficiency is effectively improved by detecting the TEAR method without wasting the energy.

Kanagasundaram, H. and Kathirvel, A [20] presented the energy-aware routing model for MANET that includes Enhanced Intellects-Masses Optimizer (EIMO) to handle energy efficient issue with the secure optimized link state routing namely EIMO–ESOLSR. Here, a particular node namely Multi-Point Relay (MPR) node is used to detect the shortest route for transmitting the data in OLSR. Since, an effective MPR is selected by using the EIMO as well as this MPR selection is mainly depends on the Composite Eligibility Index (CEI) and willingness value. The network lifetime is improved based on the effective MPR determination.

III. PROPOSED METHOD

In this proposed method, an energy and fault aware routing is developed to mitigate the malicious attacks while preserving the energy consumption of nodes in data transmission. Since, the attacks caused in the routing protocols are classified into external and internal attacks. The external attack is created from the router which doesn't contribute in the data routing process. But this external attack is act as authenticated router which either floods the false service requests or transmits the false routing information. Additionally, the internal attack is caused from the malicious, misconfigured, faulty, compromised router existing in the network. Here, the black hole occurred in the network is mitigated while transferring the data packets over the network. Additionally, the dynamic multi-detection routing protocol is developed to identify the transmission path through the network. The overall flowchart of the suggested method is shown in the Figure 1.

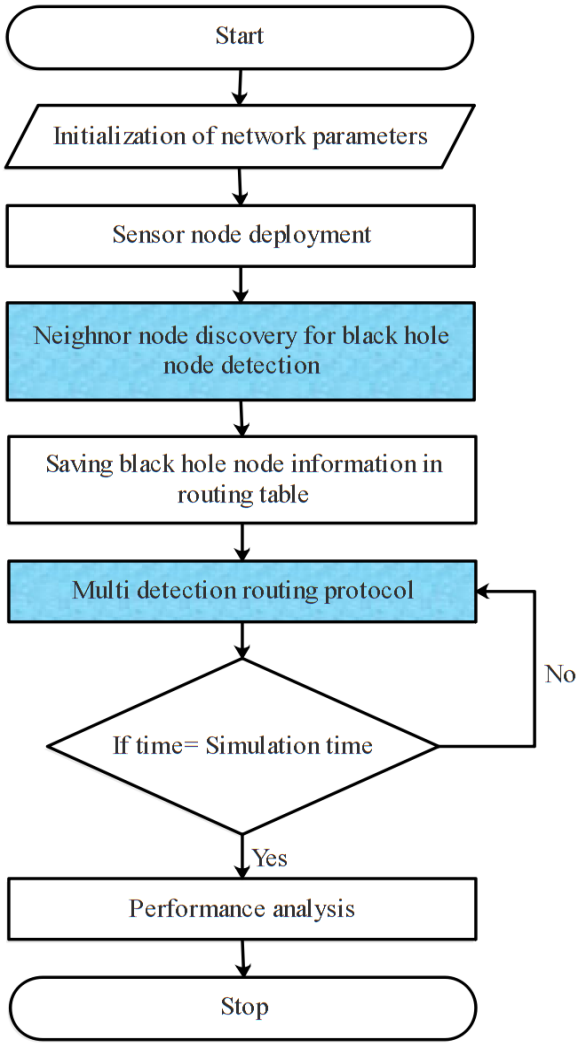

Figure 1. Flowchart of the suggested technique

A. *Neighbor node discovery for avoiding the black hole nodes*

In this proposed method, scan based random algorithm is used in the neighbor node discovery for discovering the black hole nodes. The scan based algorithm used for black hole node detection is namely Completely Random Algorithm (CRA). The CRA doesn't have any knowledge about the information of nodes. Therefore, the node information of energy level and distance among the nodes are given as the input to the CRA. Since, the CRA used in the network is direct discovery algorithm which utilizes the directional antenna for transmitting and receiving the data packets. Here, all the nodes in the network to be synchronized with the CRA. This algorithm splits the time frame as three slots. The node states are given as follows:

Transmit

Listen

Sleep

In the first mini slot, the sensor is decided to be in any one of the following state. By using these states, the black hole nodes exist in the network are detected to reduce the packet drop through the network. In transmit mode, the node sends the DISCOVER message at 1st mini slot and waits for the ACK in the 2nd mini-slot. Subsequently, the confirmation is collected by the receivers at 3rd mini slot. The DISCOVER message is received in the 2nd mini-slot, when the sensor is in listen mode. Subsequently, the ACK signal is transmitted to the transmitter, when it successfully receive the DISCOVER message. Additionally, the confirmation message from the transmitter is received at 3rd mini slot. The structure of time slot is shown in the Figure 2.

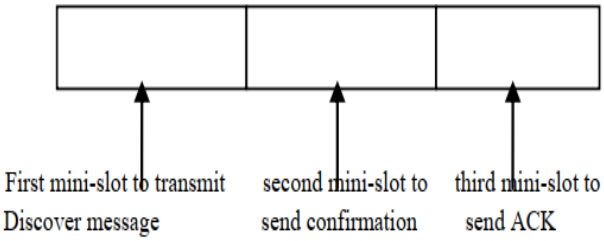

Figure 2. Structure of time slot

In this CRA algorithm, the transmitter is experienced by the collision during the 2nd mini slot, when the transmitter is discovered by the one more adjacent node. Therefore, the transmitter is drop out itself for the successive rounds of neighbor node discovery. The information about detected black nodes are saved in the routing table and it is given to the routing protocol to mitigate the black hole node.

B. *Dynamic Multi-detection Routing Protocol*

At first, the source node chooses an concealed neighbor node for creating the detection path through the network. A huge path length is considered as ω and this routing path is tried to decrease its own length till it reaches to 0. On the other hand, the length of route is minimalized by one hop till the total length is reduced to zero. Here, the multi-detection routing packet as six parts such as packet-head, packet-type, source node-ID, highest length of the detection route, acknowledgement collected by the source node for each hops (μ) and packet-ID which is shown in the Figure 3.

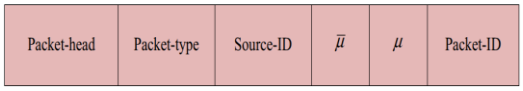

Figure 3. Structure of multi detection route packets

Algorithm

For initiating the detection path, an undetected node is elected by the sourcenode. Since, the undetected node is adjacent node that is nearer to the destination node.

The route with highest length is denoted as $\bar{\mu}$ and it is minimized by one, when the node collects the detection packet.

Then the feed_back data packet is created with the standard of $\bar{\mu} = 0$ and the feed_back path is launched to the source node.

Subsequently, the $\bar{\mu}$ is initialized again to the initial value.

The same procedure is repeated for selecting the next hop node or else end the path, when $\bar{\mu} = 0$.

Moreover, the arrangement of a feed_back data packet is shown in the Figure 4 which contains 6 parts packet head, packet type, source-ID, destination node, detection packet-ID, and Packet-ID. Here, the data source node receives the feedback packet over the network. The node provides the information about the detection route and the feedback package is returned to the source node.

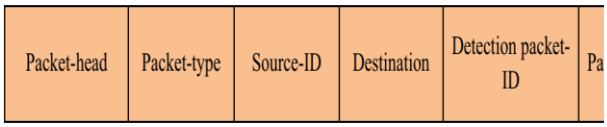

Figure 4. Structure of feed_back data packet

a. Data transmission

In this data transmission process, the data is transmitted from the source to the endpoint and this routing method is similar to the conventional routing protocols. The main difference between the conventional routing protocols and the developed multi detection routing protocol is that it enhances the success ratio of the data packets received by the destination node. Because, the developed routing protocol avoids the black holes during the data transmission. Moreover, this multi detection routing protocol discovers the shortest route through the network by adopting the features of conventional routing protocol. In the next hop selection, an adjacent node to the sink is considered to transmit the data. The feed_back failure is transmitted through the network, when the sensor fails to detect an appropriate next hop node. This helps to detect an optimal next hop node to create the data transmission path.

In this proposed method, neighbor node discovery is obtained by using the CRA method. This CRA receives the different node information such as energy level and distance among the nodes to identify the black hole nodes through the network. The information about the black hole nodes are saved in the routing table and it is given to the multi detection routing protocol. Based on this, a shortest path through the network is generated without any black hole nodes. This helps to achieve the secure data transmission over the MANET while maintaining the less energy consumption.

C. RESULTS AND DISCUSSION

The performance examination of the proposed technique is provided in this section. The implementation and simulation of the proposed method is done by the Network Simulator-2.35. In this proposed method, neighbor node discovery is used for detecting the black hole nodes through the network. Additionally, the multi detection routing protocol is used to identify the shortest path from the source to the destination. Here, the MANET is initialized with 50 nodes with over the area of $500 \times 500\text{m}^2$. The specification parameters used in the proposed method is given in the Table 1.

Table 1. Specification parameters

Parameters	Values
Number of nodes	50
Area	
Transmission range	100 m
Speed of the nodes	0 to 30 m/s
Packet size	512 Bytes
Data rate	100 kbps
Initial energy	100 J
Idle energy	0.01 J
Transmitting energy	0.042 to 0.084 J
Receiving energy	0.04 J

D. Performance analysis

The performance analysis of the proposed technique are taken in relations of energy consumption, lifetime, Packet Delivery Ratio (PDR), throughput and End to End Delay (EED). Additionally, the performance of the proposed method is assessed with one the existing method EIMO-ESOSLR [20]. This EIMO-ESOSLR [20] is also designed and simulated with the specifications mentioned in the Table 1. The results are taken in terms of number of node and number of misbehaving nodes.

i. Energy consumption

The energy depletion of the network is demarcated as the amount of energy used for transferring and receiving the data packets through the network.

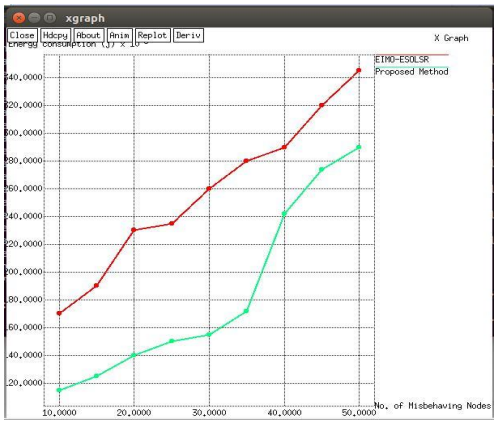

Figure 5. Performance analysis of energy consumption

Figure 5 shows the energy depletion of the proposed method with EIMO-ESOLSR [20] for different number of misbehaving nodes. From the Figure 5, knows that the energy feeding of the proposed system is less as compared to the EIMO-ESOLSR [20]. The proposed method achieves less energy consumption, because it uses the neighbor node discovery only once for identifying the black hole nodes. This helps to reduce an unwanted energy consumption during the data communication.

ii. Network lifetime

The amount of time that the all nodes in the network loses their through the network during data communication is specified as network lifetime.

Figure 6. Performance analysis of lifetime

The performance analysis of network lifetime for proposed method and EIMO-ESOLSR [20] is shown in the Figure 6. Additionally, the lifetime is examined by changing the number of nodes. From the Figure 6, knows that the lifetime of the network is improved when related towards the EIMO-ESOLSR [20]. The generation of the network is developed by preserving the energy feeding of the node. Since, the energy feeding of the nodes by identifying the shortest path using the multi detection routing protocol.

iii. Packet delivery ratio

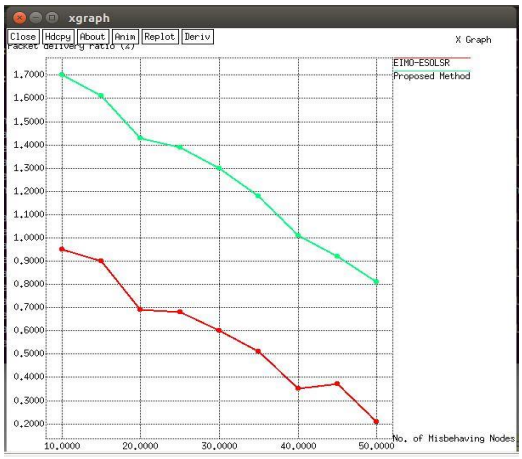

Figure 7. Performance analysis of PDR

Figure7 shows the PDR of the proposed method with EIMO-ESOLSR [20] for different number of misbehaving nodes. The PDR of the proposed method is high, after related towards the EIMO-ESOLSR [20]. The mitigation of black hole nodes using the neighbor node discovery is used to avoid the packet loss over the network. Therefore, the volume of packets successfully received by the destination node is increased over the MANET.

IV. CONCLUSION

In this paper, the CRA method is used for identifying the black hole node based on the information of nodes such as energy level and distance among the nodes. The detected black hole node's information is saved in the routing table. Therefore, the packet drop through the network is reduced by detecting the black hole nodes. Subsequently, the multi detection routing protocol is used to generate the data routing path from the basis to the destination. This helps to obtain a secure and reliable data transmission over the MANET. Additionally, the detected shortest path is used to minimalize the energy feeding while transmitting the data packets. The proposed method gives improved performance than the EIMO-ESOLSR in the MANET. The energy consumption of the proposed method is 115J for 10 misbehaving nodes, it is less when compared to the EIMO-ESOLSR.

REFERENCES

[1] Selvi, P.T. and GhanaDhas, C.S., 2019. "*A novel algorithm for enhancement of energy efficient zone based routing protocol for MANET*". Mobile Networks and Applications, 24(2), pp.307-317.

[2] Dhananjayan, G. and Subbiah, J., 2016. "*T2AR: trust-aware ad-hoc routing protocol for MANET*". SpringerPlus, 5(1), p.995.
[3] Venkanna, U., Agarwal, J.K. and Velusamy, R.L., 2015. "*A cooperative routing for MANET based on distributed trust and energy management*". Wireless Personal Communications, 81(3), pp.961-979.
[4] Anand, A., Aggarwal, H. and Rani, R., 2016. "*Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks*". Journal of Communications and Networks, 18(6), pp.938-947.
[5] Hurley-Smith, D., Wetherall, J. and Adekunle, A., 2017. "*SUPERMAN: security using pre-existing routing for mobile ad hoc networks*". IEEE Transactions on Mobile Computing, 16(10), pp.2927-2940.
[6] Malathi, M. and Jayashri, S., 2016. "*Modified Bi-directional Routing with Best Afford Path (MBRBAP) for Routing Optimization in MANET*". Wireless Personal Communications, 90(2), pp.861-873.
[7] El-Semary, A.M. and Diab, H., 2019. "*BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map*". IEEE Access, 7, pp.95185-95199.
[8] Veeraiah, N. and Krishna, B.T., 2020. *"An approach for optimal-secure multi-path routing and intrusion detection in MANET*". Evolutionary Intelligence, pp.1-15.
[9] Rafsanjani, M.K. and Fatemidokht, H., 2015. "*FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs*". AEU-International Journal of Electronics and Communications, 69(11), pp.1613-1621.
[10] Satheeshkumar, S. and Sengottaiyan, N., 2019. "*Defending against jellyfish attacks using cluster based routing protocol for secured data transmission in MANET*". Cluster Computing, 22(5), pp.10849-10860.
[11] Liu, W. and Yu, M., 2014. "*AASR: authenticated anonymous secure routing for MANETs in adversarial environments*". IEEE transactions on vehicular technology, 63(9), pp.4585-4593.
[12] Elmahdi, E., Yoo, S.M. and Sharshembiev, K., 2020. "*Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks*". Journal of Information Security and Applications, 51, p.102425.
[13] Vanitha, K. and Rahaman, A.Z., 2019. "*Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol*". Cluster Computing, 22(6), pp.13453-13461.
[14] Annadurai, P. and Vijayalakshmi, S., 2015. "*Highly Reputed Authenticated Routing in MANET (HRARAN)*". Wireless Personal Communications, 83(1), pp.455-472.
[15] Chintalapalli, R.M. and Ananthula, V.R., 2018. "*M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network*". IET Communications, 12(12), pp.1406-1415.
[16] Khamayseh, Y.M., Aljawarneh, S.A. and Asaad, A.E., 2018. "*Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency*". Sustainable Computing: Informatics and Systems, 18, pp.90-100.
[17] Kasthuribai, P.T. and Sundararajan, M., 2018. "*Secured and QoS based energy-aware multipath routing in MANET*". Wireless Personal Communications, 101(4), pp.2349-2364.
[18] Jamaesha, S.S. and Bhavani, S., 2019. "*A secure and efficient cluster based location aware routing protocol in MANET*". Cluster Computing, 22(2), pp.4179-4186.
[19] Merlin, R.T. and Ravi, R., 2019. "*Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET*". Wireless Personal Communications, 104(4), pp.1599-1636.
[20] Kanagasundaram, H. and Kathirvel, A., 2018. "*EIMO-ESOLSR: energy efficient and security-based model for OLSR routing protocol in mobile ad-hoc network*". IET Communications, 13(5), pp.553-559.
[21] Dr. Ramesh.Vatambeti, N. B. D. B. V. (2020). *"Optimal Routing and Load Balancing based Congestion Avoidance in MANET using Improved Ad-Hoc On-Demand Distance Vector Routing*". International Journal of Control and Automation, 13(02), 110 – 127.
[22] Ramesh. Vatambeti, D.Pramodh Krishna, K.Sangeetha Supriya, (2020) "*A Novel Scheme for Energy Conservation and reduction in Routing Overhead of AODV for Wireless Ad-Hoc Networks*", International Journal of Advanced Science and Technology, 29(3), 5281 - 5287. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/6034.
[23] B.Nanditha, Dr V Ramesh, B.Veeramallu, "*Achieving Energy Efficiency and Increasing the Network Life Time in MANET through Fault Tolerant Multi-Path Routing*", International Journal of Intelligent Engineering and Systems, Vol.10, No.3, 2017 DOI: 10.22266/ijies2017.0630.18.