Received: August 14, 2020. Revised: September 25, 2020.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

PUSR: Position Update Secure Routing protocol for MANET

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 is a self-organizing wireless network, which is formed by the wireless mobile devices without any centralized infrastructure. The mobile nodes in the network are mainly affected by the inherent characteristics such as unpredictable network topology and open wireless medium. Especially, the presence of selfish nodes in the network creates the packet loss and affects an entire communication system. In this paper, the hash function with position updating algorithm is proposed in the Ad hoc On-Demand Distance Vector (AODV) routing protocol for improving the security against the selfish nodes. The AODV routing protocol is used to transmit the data packets from the source to the destination. Therefore, the Prevention of Selfish Node using Hash Function (PSNHF) with position update algorithm is proposed for minimizing the packet loss through the network. The performances of proposed AODV-PSNHF method are analysed in terms of energy consumption, throughput, Packet Delivery Ratio (PDR), packet loss and normalized routing load. In addition, the AODV-PSNHF method is compared with the existing trust-aware ad-hoc routing protocol (T2AR). The selfish node identification using hash function and positioning update using AODV-PSNHF method provides reliable and secure data transmission under selfish nodes and shows better performance in terms of throughput, packet delivery ratio and packet loss. For 2% of malicious nodes the PDR of the AODV-PSNHF method is 89%, it is 9% higher when compared to the T2AR protocol whose PDR% is only 80% for the same.

Keywords: Ad hoc on-demand distance vector (AODV) routing protocol, Mobile ad hoc network (MANET), Hash function, Position update.

1. Introduction

Mobile ad hoc network (MANET) is a set of wireless nodes, which cooperatively creates the network without any configuration or administration [1]. The mobile nodes of the MANET have restricted communication range that extends over a few 100 meters. Consequently, the nodes in the MANET mainly depend on the adjacent nodes for communicating with the nodes that are not in the communication range [2, 3]. The nodes of MANET act like both the source and the router. The traffic is generated by the source node, whereas the packets are received in the router node and the received packets are switched to the adjacent nodes [4, 5]. This MANET is used in different real time applications such as vehicle networks, disaster recovery systems, military applications, maritime communications, etc. [6, 7]. The mobile nodes in the MANET are communicated through the directed wireless path or wireless multipath in the network transmission range [8].

The MANET has restricted resources by means of memory, computational, bandwidth and battery capacities. The multiple hops are used to transmit the data packets from the source node to the destination node. The route discovery is essential when the multi hops are required in the MANET for data transmission [9, 10]. Routing is considered as an essential operation in the MANET and this routing is challenging task due to the dynamic links, and broadcast nature of the communication and lack of infrastructure [11]. In addition, the restricted mobility energy capacity creates the link and node failure in network [12]. The characteristic of MANET such as unpredictable network topology and open wireless medium creates the difficulty while providing the

secure and trusted communication between the nodes [13]. In MANET, the mobile nodes are required to wait until pre-defined time interval between continuous data transmission. However, the selfishness and network congestion create the node misbehaviour which affects the MANET performance [14]. Moreover, the packet loss happens mainly due to the link error and malicious nodes [15]. Therefore, an effective routing topology is required to be developed for avoiding the selfish nodes in the MANET.

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

- The hash function is combined with the AODV routing protocol to avoid the malicious nodes during route generation. This PSNHF is used to minimize the packet drop in MANET.
- The proposed AODV-PSNHF method also used uses in position update to avoid the insecure paths, thereby that used to increase the number of packets that are received at the destination.

The overall organizations of the paper are given as follows: The literature survey about the secure data transmission in the MANET is given in the section 2. The problem statement and solution for this paper are specified in the section 3. Section 4 describes the secure data transmission through the MANET using AODV-PSNHF method. The results and discussion of the AODV-PSNHF method are shown in the section 5. Finally, the conclusion and future work are discussed in section 6.

2. Literature survey

Elmahdi [16] presented the modified ad-hoc on-demand multipath distance vector (AOMDV) protocol for delivering secure data transmission under blackhole attacks. The data were divided into different parts and this divided data were encrypted by using the Enhanced Homomorphic Cryptosystem (EHC) method. Next, the key distribution protocol namely Elliptic Curve Diffie Hellman (ECDH) algorithm was used to distribute the key from the EHC to the transmitter and receiver nodes. The developed AOMDV was provided better route discovery, when the network has link failure between the nodes. The process and security features of the EHC were increased the end to end delay in MANET.

El-Semary and Diab [17] developed the Blackhole Protected AODV (BP- AODV) protocol for detecting and preventing the network from both the blackhole and cooperative blackhole attack caused while transmitting the data packets. Since, the BP-AODV protocol was developed by incorporating the chaotic map in AODV protocol. The chaotic map was provided the chaotic features for each source and destination node pairs to improve the security. But the security provided by the chaotic map was not sufficient due to its small key space and uneven distribution.

Gurung and Chauhan [18] presented the Mitigating Black hole effects through Detection and Prevention based AODV protocol in MANET. The developed MBDP-AODV protocol was mainly depends on the dynamic threshold value of destination sequence number to avoid the blackhole attack. The statistical features such as mean and standard deviation were increased when the network was affected by the blackhole attack. The SUSPECT packet was transmitted by source nodes during the detection phase and the blackhole node was detected based on the transmission of ALERT packet. But, this MBDP-AODV protocol has higher routing overhead due to the data transmission of multiple relay packets.

Kumar and Dutta [19] developed the dynamic trust-based intrusion detection technique to identify and protect the selfish nodes for improving network security. Here, the AODV was utilized for generating the transmission path from the source to the destination. The selfish nodes were identified preciously by considering the direct and indirect trust degree. Besides, the direct and indirect trust degrees were analysed from the direct communication interactions and recommendations of neighbour, respectively. The frequent network topology created the overhead during the data transmission.

Abirami and Sumithra [20] presented the Neighbour Credit Value based AODV (NCV-AODV) routing algorithm for identifying the selfish nodes in the network. The nodes in the MANET were maintained the neighbour credit table in the NCV-AODV algorithm. The credit value of the next hop was verified when the node was required to generate the route to the next hop node. Here, the node with less credit value was selected as an appropriate node for minimizing the packet drop in the network. The forwarded packets were dropped during transmission when the node does not have minimum credit value.

Abirami and Sumithra [21] developed the improved version of NCV-AODV (iNCV-AODV) protocol is developed for enhancing the MANET performances. The assumptions made in the iNCV-AODV were given as follows: the nodes in the network were basically not malicious nodes and only few new nodes cause the malicious behaviour over the network. The credit value was provided to the all member nodes for generating the neighbour credit table. Moreover, the credit values were updated only for the neighbour nodes not for the selfish nodes

which were used to improve the network performances. The message overhead was increased due to the transmission of dummy data by the one hop request.

Dhananjayan and Subbiah [22] developed the trust-aware ad-hoc routing (T2AR) protocol for improving the trust level of the nodes present in the network. The T2AR protocol was designed by considering different constraints in the AODV protocol such as mobility, energy, and trust rate. Here, trust rate was identified from the packet sequence ID from an adjacent node's log report and this identification of trust rate was used to avoid the generation of malicious report. In this T2AR, an authenticated node within the transmission range was detected by the received signal strength indicator. Moreover, the trust level was enhanced by using the direct and indirect trust observation schemes. The lack of positional update affects the connection establishment between the nodes.

3. Problem statement

Current issues related to the MANET are stated in this section and it also explains how the proposed method overcomes the problems faced in the MANET.

The chaotic map used in the BP-AODV protocol [17] does not provide enough security for the data transmission due to small key size and uneven distribution between the nodes. The data packets transmitted through the network was highly dropped, due to the lesser authentications between the nodes. The dummy data transmission using one hop request was increased the message overhead in the MANET [20]. Moreover, the connection establishment among the nodes was affected by the lack of positional updates during the data transmission [22]. The amount of data packets which is successfully transmitted at the destination was affected due to the inappropriate positional update and higher message overhead.

Solution:

In this proposed method, the hash function is combined with the AODV routing protocol to improve the security against the selfish nodes in the MANET. The hash function-based security is used to minimize the packet drop while transmitting the data packets to the desired destination node. The location of new nodes which is entered into the network is continuously updated by the AODV routing protocol which provides an effective location update between the nodes. Moreover, this AODV-PSNHF method does not need any dummy packet to identify the malicious node which is used to minimize the overhead through the network.

4. AODV-PSNHF method

In AODV-PSNHF method, the AODV routing protocol is used for transmitting the data packets from the source to the destination. The process of AODV is mainly categorized into two stages such as route discovery and route maintenance. The AODV routing protocol mainly uses three different control messages such as route request (RREQ), route reply (RREP) and route error (RERR) messages.

Here, the hash function is combined with the RREQ message of the AODV routing protocol for enhancing the security during the data transmission.

The major steps processed in this AODV-PSNHF method are given as follows:

- Initially, the mobile nodes are randomly deployed with the selfish nodes in the interested area.
- The route between the source and the destination is identified by using the AODV routing protocol.
- In this AODV-PSNHF method, the hash function is generated, and it is incorporated in the RREQ message to ensure the security between the source-destination pairs.
- Next, the data transmission between the source and destination node is accomplished, once the RREP message is received by the source node with the matching hash function.

The detailed description about the proposed method is given as follows and the overall flowchart of the AODV-PSNHF method is shown in the Fig. 1.

4.1 Hash key function algorithm

The proposed PSNHF algorithm generates a cryptographic hash key function to identify the node misbehaviour in MANET by carrying out mutual authentication between source and destination. The algorithm exhibits the two phases: Initialization phase and Hash key generation The initialization phase is executed by sending RREQ to all the neighbour nodes of Originator in order to find the routing path from source to destination which consists of Source address, Destination address, Sequence number, Hop count. The hash code is generated to identify selfish node by using the efficient technique called hash key function, which is expressed by Eq. (1),

$$H(n) = HK(M) \quad (1)$$

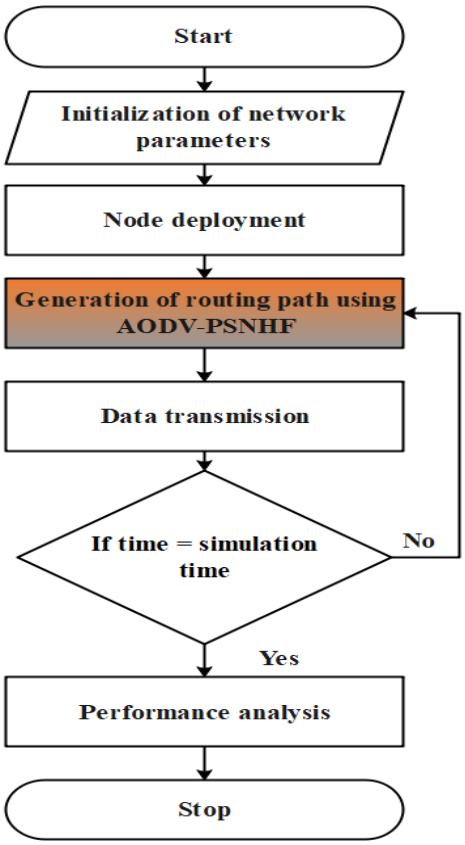

Figure. 1 Flowchart of the proposed AODV-PSNHF method

where $H(n)$ represent hash key function of nth node, M represent the message and HK represents the key. The product of original Message (M) and Hash function (H) with secret key produce the output called as Hash Key Function (HKF). Once the destination node receives the RREQ from source, it generates hash code by using the Eq. (1). Then the destination node sends a RREP to sender node via routing path in the network where the hash code is appended in RREP. The algorithm for selfish node identification is given below.

Algorithm I

Input: Ni = Number of Nodes, SN = Source Node, DN = Destination Node, CN = Current node, NN = Neighbour node, SFN = Selfish Node, SKHR = Sender Key Hash response, DKHR = Destination Key Hash response, NMN = Node Misbehaviour Notification, HKF = Hash Key Function and Xi, Yi = Position of node.

Step 1: Initialize nodes (Ni)
Step 2: Initialize node deployment (Xi, Yi)
Step 3: Initialize SN, DN
Step 4: SN Sends RREQ to NN
Step 5: If (CN = =Destination)
{
Go to step 7
}
Step 6: else
{
Check routing table
Forward RREQ to NN
Go to Step5
}
Step 7: Generate DKHR and append with RREP
{RREP, DKHR}
Step 8: Forward {RREP, DKHR} to SN
Step 9: Generate SKHR
Step 10: Check DKHR and SKHR
If (DKHR == SKHR)
{
DN node is legitimate node
Go to Step 3.
}
else
{
DN is selfish node (Misbehaviour Node).
Send alert to all nodes in network.
Update position and Modify routing path
}
Step 11: Go to Step 3

4.2 Prevention of selfish node using hash function

In PSNHF method, the hash function is incorporated for identifying whether the intermediate nodes are affected by any selfish node. The one-way hash function is frequently accomplished for generating the random hash chain which helps to improve the security while transmitting the data packets. The generated hash function is integrated in the RREP message for protecting the network from the selfish nodes.

The value of Time To Live (TTL) is fixed as equal to the highest value of hop count field that is expressed in the Eq. (2).

$$M = TTL \tag{2}$$

Where, the M specifies the highest value of hop count field.

The initial value of hash is equal to the random number generated from the one-way hash function which is shown in the Eq. (3).

$$Hash = h(V) \quad (3)$$

Where, V represents the random number generated by the sequence number and h represents the hash function.

The maximum hash field is computed by calculating hash function for TTL times that is expressed in Eq. (4).

$$Max\_hash = h^{TTL}(V) \quad (4)$$

Where, the maximum hash field is represented as Max_hash. The condition given in Eq. (4) is verified, when the node receives the RREQ/RREP from the adjacent node.

$$M_{hash} = h^{TTL-N}(Hash) \quad (5)$$

Where, the condition used for verifying the node is represented as M_{hash} and the number of hops connected to the respective mobile node is represented as N. The calculated M_{hash} is added in the structure of RREQ packet which is shown in the Eq. (6).

$$RREQ \rightarrow \{S, D, ID, Srcnum, Desnum, N, M_{hash}\} \quad (6)$$

Where, the address of the source and destination node are denoted as S and D respectively. RREQ's identification number is ID ; the source and destination sequence number are represented as the $Srcnum$ and $Desnum$.

4.2.1. One-way hash chain

The one-way hash chain is designed with the one-way hash function and the one-way hash function H maps any length of input into a fixed length bit string. Thus, $H: \{0,1\}^* \rightarrow \{0,1\}^\rho$, where the length in bits of the hash function output is represented as ρ. The random initial value is selected by a node used for generating the one way hash chain i.e., $x \epsilon \{0,1\}^\rho$ and determines the list of values $h_0;\ h_1;\ h_2;\ h_3; \ldots; h_n$, where $h_0 = x$.

Moreover, the generated hash function is incorporated into the RREP message for improving the security of the mobile nodes against the selfish nodes.

4.3 Process of route discovery using AODV routing protocol

Generally, the node in the Ad-hoc network maintains the information about the routing in the table and this information has the routing path from the node to the destination node. The data packets are forwarded to the destination when the route is available for the respective node. Otherwise, the AODV protocol transmits the hash function based RREQ packet for initializing the route discovery between the nodes which is shown in the Fig. 2. This hash function based RREQ packet is used to avoid the selfish node in the data transmission. The node which receives the RREQ is verified like whether the nodes are required destination node and the node transmits the RREP message when it is an appropriate node for data transmission. Additionally, the node checks whether it has any active route to transmit the data packets. If there is no active route, the intermediate node broadcasts the RREQ message for identifying the destination.

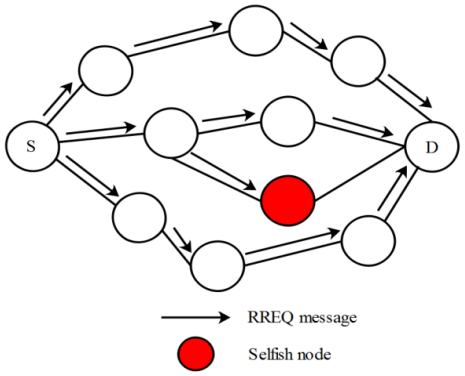

Figure. 2 Transmission of RREQ message in AODV-PSNHF method

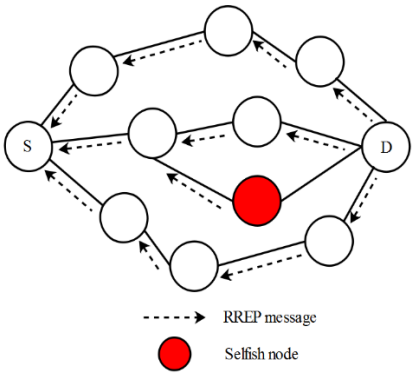

Figure. 3 Transmission of RREP message in AODV-PSNHF method

The Destination Sequence Number (DSN) is compared with the RREQ message, when the adjacent node in the network transmits the RREP message to the remaining nodes. The transmission of RREP message to the source node is illustrated in the Fig. 3. Furthermore, the data are transmitted to the destination node, when the neighbour node DSN is greater than the sequence number in the packet. If the link node failure is identified during routing, the RRER message is transmitted to the adjacent nodes

in the network. The detailed description of Position updating algorithm to avoid selfish nodes is discussed in section 4.3.1.

4.3.1. Node positional update algorithm

The secured packet transmission between source and destination in MANET is a complex process. A secured routing protocol is required to identify and eliminate selfish nodes to avoid packet drops and to increase the throughput. Due to mobility of nodes, it is difficult for routing protocols to avoid insecure routing paths. The node position update algorithm provides a better solution for routing protocols by avoiding routing through insecure paths. Once the mutual authentication between nodes are successful, each node broadcasts a beacon to share its information such current position and velocity of movement. Each node in the network periodically broadcasts its current location information and updates its neighbour list based on its range of transmission, current location, angle of arrival of packets and the position updates received from its nearby nodes. This methodology helps the routing protocol to find out an efficient routing path for secured packet transmission.

Algorithm:

Input: Ni, SN, DN, CN, NN and SFN.

Step 1: Node Initialization
Step 2: Initialize node deployment (Xi, Yi)
Step 3: Broadcast node position Co-ordinates to network.
Step 4: Store NN Co-ordinates
Step 5: Load Routing Table
Step 6: Algorithm I Execution - Step 4 to step 10.
Step 7: If (SFN detected)
{
Update NN location co-ordinate in routing table
Generate alternate routing path
Broadcast current position coordinate
Go to step 4
}
else
{
Broadcast current position coordinate
Go to step 4
}

4.4 Route maintenance using AODV protocol

The HELLO message mechanism is developed in the AODV route maintenance for observing the neighbour node control message and for maintaining the adjacent node information. The HELLO message is frequently broadcasted to deliver the link information for guaranteeing the link symmetry that also utilized for identifying whether the link is invalid or not. Moreover, the RRER message is delivered, when there is a failure in the data transmission through the network.

5. Results and discussion

The experimental results and discussion of the AODV-PSNHF method is described in this section. The implementation and simulation of the AODV-PSNHF method is carried out in the Network Simulator (NS)-2.35. The AODV routing protocol is used to transmit the data packets from the source to the destination node. Next, the hash function is incorporated in the AODV-PSNHF method for improving the security against the selfish node. In the area of $500 \times 500m^2$, 20-100 mobile nodes are randomly deployed through the network. The mobile nodes in the network are initialized with the maximum mobility speed of 10 m/s. The simulation parameters considered for this AODV-PSNHF method are shown in the Table 1.

5.1 Performance analysis

The performance of the AODV-PSNHF method is analysed in terms of Energy consumption, throughput, Packet Delivery Ratio (PDR), packet loss and Normalized Routing Load (NRL). Here, the AODV routing protocol without PSNHF is used to evaluate the performances of the AODV-PSNHF method for different number of nodes and this AODV

Table 1. Simulation parameters

Parameter	Value
Area	$500 \times 500\ m^2$
Number of nodes	20-100
Routing Protocol	AODV
Maximum mobility speed	10 m/s
Mobility model	Random waypoint mobility model
Propagation radio model	Two ray ground
Channel	Wireless channel
Phy	Wireless phy
MAC layer	IEEE 802.11
Traffic type	CBR-UDP
Packet size	512 bytes
Simulation time	500

without PSNHF also implemented by considering the same specifications mentioned in the Table 1.

5.1.1. Energy consumption

Energy consumption is defined as the amount of energy consumed during the data transmission from the source to the destination and the energy consumption is expressed in the Eq. (7).

$$EC = E - ED \tag{7}$$

Where, the consumed energy of the nodes is represented as EC; total energy and energy drained during the data transmission are specified as E and ED respectively.

Fig. 4 shows the comparison of average energy for the AODV-PSNHF method and AODV (selfish) protocol. From the Fig. 4, shows that the AODV-PSNHF method has improved energy consumption than the AODV (selfish) protocol. Due to less authenticity of the AODV (selfish) protocol, the energy of the nodes is preserved by the selfish nodes. Therefore, the average energy of the nodes is high, when compared to the AODV (selfish) protocol. This higher average energy leads to improve the lifetime of the AODV-PSNHF method.

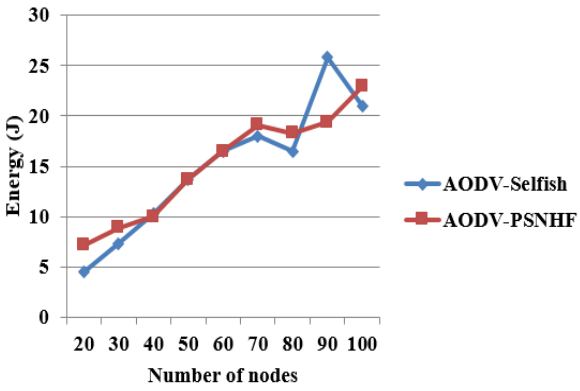

Figure. 4 Energy consumption under selfish nodes

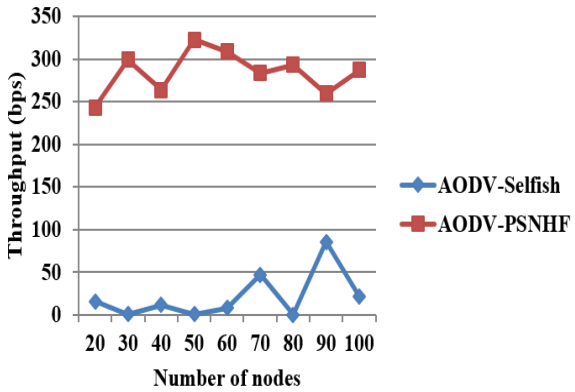

Figure. 5 Throughput under selfish nodes

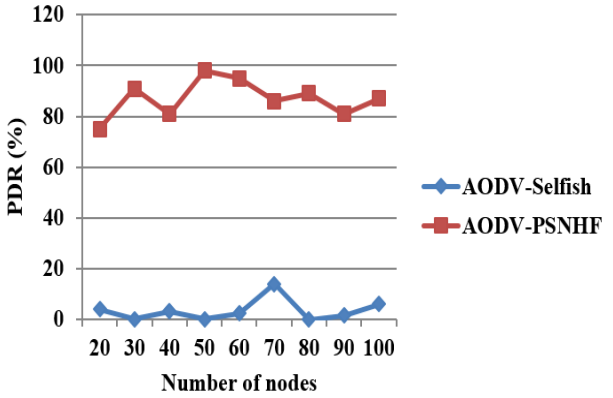

Figure. 6 PDR under selfish nodes

5.1.2. Throughput

Throughput is defined as the number of packets transmitted in the particular time. Generally, the throughput is calculated in the kilobits per second or megabits per second and it is expressed in the Eq. (8).

$$Throughput = \frac{R}{t} \tag{8}$$

Where, R is the amount of packets received by the destination node and t is the simulation time.

The throughput comparison of AODV-PSNHF method with AODV(Selfish) routing protocol is shown in the Fig. 5. The throughput of AODV-PSNHF method is high, when compared to the AODV (selfish) routing protocol. The main reason for the AODV-PSNHF method for higher throughput is that the mitigation of selfish nodes while transmitting the data packets. Because, the selfish nodes present in the MANET greatly affects an entire communication system.

5.1.3. Packet delivery rate

PDR is the ratio between the amount of successfully received packets in destination node and the amount of packets generated on the source side which is expressed in the following Eq. (9).

$$PDR = \frac{R}{T} \times 100\% \tag{9}$$

Fig. 6 shows the comparison of PDR for the AODV-PSNHF method and AODV (Selfish) protocol. From the Fig. 6, AODV-PSNHF method has a higher PDR than the AODV(selfish)routing protocol. The selfish node causes the packet loss during the data transmission. The PDR of the AODV-PSNHF method is increased by using the hash function to avoid the selfish nodes.

5.1.4. Packet loss

Packet loss is defined as the amount of packet loss occurred while transmitting the data packets through the network and this packet loss is expressed in the Eq. (10).

$$Packet\ loss = T - R \tag{10}$$

The packet loss comparison of AODV-PSNHF method with AODV (selfish) protocol is shown in the Fig. 7. The packet loss of AODV-PSNHF method is less, when compared to the AODV (selfish) routing protocol. The hash function based secure communication between the source node and destination node minimizes packet loss in the MANET. Meanwhile, the packet loss during the AODV (selfish) routing is increased due to malicious activities caused by the selfish node.

5.1.5. Normalized routing load

NRL is defined as the ratio of the total number of control packets to the packets received at the destination node and the Eq. (11) expresses the NRL.

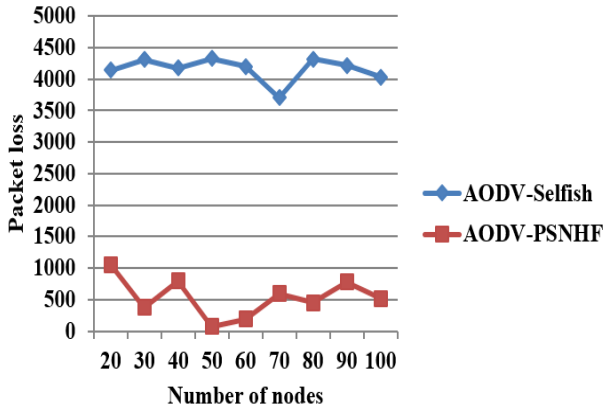

Figure. 7 Packet loss under selfish nodes

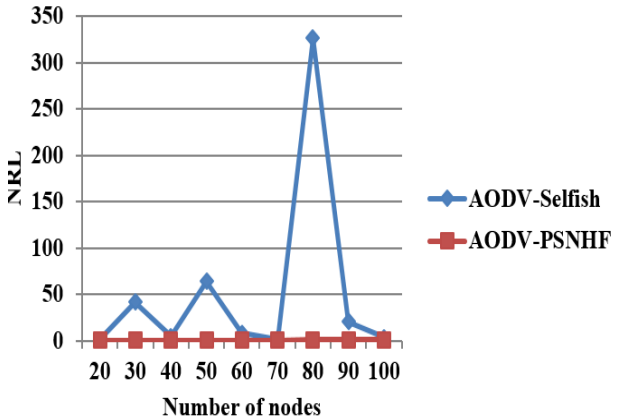

Figure. 8 NRL under selfish nodes

$$NRL = \frac{1}{D} \times \frac{\sum_{i=1}^{n} C_i}{\sum_{i=1}^{n} R_i} \tag{11}$$

Where, the number of experiments is specified as D and the amount of control packets through the network is represented as C.

Fig. 8 shows the comparison of NRL for the AODV-PSNHF method and AODV (selfish) protocol. From Fig. 8, AODV-PSNHF method has lesser NRL than the AODV (selfish) protocol. The routing load of the proposed AODV-PSNHF method is less by avoiding the selfish nodes during the communication.

5.2 Comparative analysis

The proposed AODV-PSNHF method is compared with T2AR [22] for comparative analysis. The area of $500 \times 500m^2$ with 100 mobile nodes are considered with 100 s of simulation time to compare with the T2AR [22]. Table 2 and 3 shows the comparative analysis of the proposed AODV-PSNHF method with T2AR [22].

The comparison of the AODV-PSNHF method and T2AR [22] is made by varying the percentage of malicious nodes from 1 to 6 and different network sizes. Whenever the percentage of malicious node is increased, PDR values are getting decreased and the dropped packets are increased for both the conventional and proposed algorithm.

Table 2. Comparative analysis of AODV-PSNHF method with T2AR

Percentage of malicious nodes	PDR (%)		Percentage of dropped packets (%)	
	T2AR [22]	AODV-PSNHF	T2AR [22]	AODV-PSNHF
1	90	93	1	0
2	80	89	11	9
3	75	82	35	26
4	70	76	40	33
5	60	71	45	41
6	60	68	49	47

Table 3. Throughput vs network size of AODV-PSNHF method with T2AR

Network Size	T2AR [22]	AODV - PSNHF
5 Nodes	0.99	0.790311
10 Nodes	0.96	0.803256
20 Nodes	0.9	0.910568
30 Nodes	0.88	1.037047
40 Nodes	0.84	1.073168
50 Nodes	0.8	1.073673
60 Nodes	0.78	0.924115

Initially, the AODV-PSNHF algorithm has less throughput compared to T2AR [22]. While increasing the network size as 30 nodes to 60 nodes, the throughput of the AODV-PSNHF algorithm getting increased. From the Table 2 and Table 3, it clears that the AODV-PSNHF algorithm achieved better performance compared to the T2AR algorithm [22].

The communication performance of the T2AR [22] is affected because of the lack of position information between the nodes whereas, in the AODV-PSNHF method the AODV routing protocol is combined with the hash function is used to avoid the selfish node in data transmission & also position update is done. The AODV protocol used in the MANET due to its low overhead, faster speed and lesser computation which leads to improve the MANET performances. Moreover, the hash function used in the AODV-PSNHF method obtains reliable and secure communication under selfish nodes.

6. Conclusion

MANET is vulnerable to the security attacks, because of the open wireless medium and unpredictable topology of the network. In this paper, hash function is used in the AODV for securing the data transmission from the source to the destination. The faster speed and lesser computation characteristics of the AODV routing protocol are used to find an optimal path to transmit the data through the network. The AODV-PSNHF method avoids the selfish node while performing the route discovery process. This AODV-PSNHF method provides reliable and secure data transmission under selfish nodes. The AODV-PSNHF method provides better performance than the AODV routing protocol T2AR. The PDR of the AODV-PSNHF method for 5% of selfish nodes is 71%, it is less when compared with the T2AR protocol. In the future, incentive technique will be introduced to motivate the selfish nodes to become normal nodes.

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] B. Muthusenthil and S. Murugavalli, "Privacy preservation and protection for cluster based geographic routing protocol in MANET", *Wireless Networks,* Vol. 23, No. 1, pp. 79-87, 2017.

[2] A. Anand, H. Aggarwal, and R. Rani "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks", *Journal of Communications and Networks,* Vol. 18, No. 6, pp. 938-947, 2016.

[3] D. Hurley-Smith, J. Wetherall, and A. Adekunle, "SUPERMAN: security using pre-existing routing for mobile ad hoc networks", *IEEE Transactions on Mobile Computing,* Vol. 16, No. 10, pp. 2927-2940, 2017.

[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] 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, 2016.

[6] R. M. Chintalapalli and V. R. Ananthula, "M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network", *IET Communications*, Vol. 12, No. 12, pp. 1406-1415, 2018.

[7] K. El Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETs", *IEEE Transactions on Mobile Computing*, Vol. 10, No. 9, pp. 1345-1358, 2010.

[8] V. S. Devi and N. P. Hegde, "Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer", *Wireless Personal Communications,* Vol. 100, No. 3, pp. 923-940, 2018.

[9] J. Sathiamoorthy and B. Ramakrishnan, "Design of a proficient hybrid protocol for efficient route discovery and secure data transmission in CEAACK MANETs", *Journal of Information Security and Applications,* Vol. 36, pp. 43-58, 2017.

[10] A. Hammamouche, M. Omar, N. Djebari, and A. Tari, "Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET", *Journal of Information Security and Applications*, Vol. 43, pp. 12-20, 2018.

[11] S. A. Thorat and P. J. Kulkarni, "Opportunistic routing in presence of selfish nodes for MANET", *Wireless Personal Communications*, Vol. 82, No. 2, pp. 689-708, 2015.

[12] G. Cervera, M. Barbeau, J. Garcia-Alfaro, and E. Kranakis, "A multipath routing strategy to prevent flooding disruption attacks in link state routing protocols for MANETs", *Journal of Network and Computer Applications*, Vol. 36, No. 2, pp. 744-755, 2013.

[13] W. Liu and M. Yu, "AASR: authenticated anonymous secure routing for MANETs in adversarial environments", *IEEE Transactions on Vehicular Technology*, Vol. 63, No. 9, pp. 4585-4593, 2014.

[14] S. Subramaniyan, W. Johnson, and K. Subramaniyan, "A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2014, No. 1, pp. 205, 2014.

[15] K. Vanitha and A. Z. Rahaman, "Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol", *Cluster Computing*, Vol. 22, No. 6, pp. 13453-13461, 2019.

[16] E. Elmahdi, S. M. Yoo, and K. Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks", *Journal of Information Security and Applications*, Vol. 51, p. 102425, 2020.

[17] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map", *IEEE Access*, Vol. 7, pp. 95185-95199, 2019.

[18] S. Gurung and S. Chauhan, "A dynamic threshold-based approach for mitigating black-hole attack in MANET", *Wireless Networks*, Vol. 24, No. 8, pp. 2957-2971, 2018.

[19] S. Kumar and K. Dutta, "Trust based intrusion detection technique to detect selfish nodes in mobile ad hoc networks", *Wireless Personal Communications*, Vol. 101, No. 4, pp. 2029-2052, 2018.

[20] 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. 60, 2018.

[21] K. R. Abirami and M. G. Sumithra, "Evaluation of neighbor credit value based AODV routing algorithms for selfish node behavior detection", *Cluster Computing*, Vol. 22, No. 6, pp. 13307-13316, 2019.

[22] G. Dhananjayan and J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET", *Springer Plus,* Vol. 5, No. 1, p. 995, 2016.