An Improved Mechanism to Prevent Blackhole Attack in MANET

Akhilesh Singh and Muzammil Hasan

Abstract Mobile node having ubiquitous characteristics, collectively form a group, generally known as mobile ad hoc network (MANET). It has a wide range of applications due to its easy installation, no any central authority-based failure point, no fixed infrastructure and many more. Openness of ad hoc network leads to the wide range of security issues that need to be investigated as well as resolved. In this paper, we are proposing the solution to the blackhole problem that overcomes this issue in more fruitful way. In general, attacker sends a forged RREP with high DSN and low hop count to fraudulently showing the source node having shortest path. When data are transmitted through that route all packets have been dropped. As per our approach, destination sequence number (DSN) is compared with a threshold value and fake messages are discarded. The simulation work has been carried out to compare the proposed approach with the standard AODV routing protocol on the basis of packet delivery ratio (PDR), and it shows positive results.

Keywords MANET · Blackhole attack · Packet drop attack
Routing attack

1 Introduction

At present, wireless networks are widely used for the communication purpose. They are of two types, one which has an infrastructure and present of access point and other which doesn't have fixed infrastructure also called ad hoc network. In ad hoc network, any node can leave or join the network at any point of time. Every mobile node has equipped with a wireless transmitter and a receiver. Every mobile node of the network is responsible for operation, creation and maintenance of the ad hoc

A. Singh (✉) · M. Hasan
Department of Computer Science and Engineering, MMMUT, Gorakhpur, India
e-mail: akhilesh840@gmail.com

M. Hasan
e-mail: muzammil_hasan@yahoo.com

K. Saeed et al. (eds.), *Progress in Advanced Computing and Intelligent Engineering*,
Advances in Intelligent Systems and Computing 563,
https://doi.org/10.1007/978-981-10-6872-0_48

network. Confidentiality of data, availability of network can be achieved by removing the chances of attack on the network. MANET has feature like openness, varying topology, absence of central authority and no proper mechanism for defence, which cause security attacks on MANET.

Many types of security attacks are done on the MANET. One of them is blackhole attack in attacker node which sends forged information to the sender node and all the data packets are dropped by the attacker node. Many different mechanisms are used for the prevention of blackhole attack in MANET. Researchers use their different methodology to prevent this attack and secure the network from this attack. Some of them used destination sequence number which is known as DSN, some of them used cryptography mechanism to prevent the attack, some of them used trust-based mechanism and some of them used intrusion detection mechanism.

1.1 MANET

Ad hoc network is termed as independent basic service set (IBSS). In this type, communication between mobile nodes occurs without any access point. They directly send and receive messages from one node to another. Ad hoc network doesn't have any fixed infrastructure or central authority. Mobile nodes of the ad hoc network communicate with each other via wireless communication medium. In ad hoc network, nodes are free to roam, i.e. mobility is associated with the node, so such network is also called MANET that stands for mobile ad hoc network. Figure 1 shows the MANET with eight nodes [1].

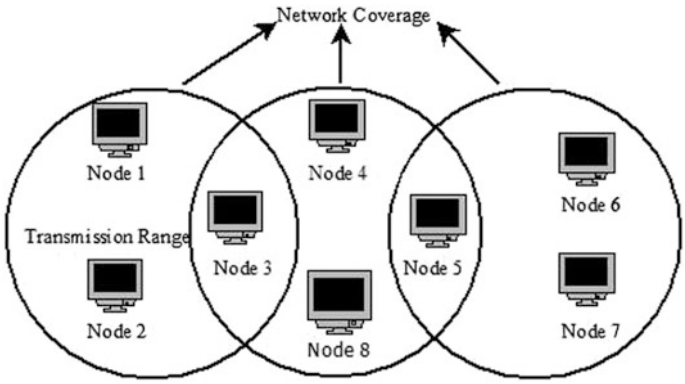

Fig. 1 MANET with eight nodes

1.2 MANET Characteristics

There are many characteristics which make MANET popular among the other communication network. These make MANET different from other networks.

Cooperative: If the source node wants to transmit data to the destination node and source and destination node are not in the range of communication. Then other nodes of the network cooperate with source and destination node for the communication.

Dynamic topology: Nodes in MANET are mobile in nature, so they roam throughout the network randomly and their location is unpredictable. This nature of the network creates complexity for the routing protocols.

Deficiency of fixed infrastructure: There is absence of central authority to monitor the ad hoc network. Traditional techniques of security are hardly applicable on MANET due to any presence of central authority, and it doesn't have any fixed infrastructure as the traditional networks have.

Resource constraints: MANET is a system of collective mobile nodes which have limited or low-power capacity. It also has limited memory, bandwidth, computation capacity, etc. So it is challenging to achieve a reliable and secure link of communication among the mobile nodes.

1.3 Routing Approaches Used in MANET

There are four types of routing approaches used in MANET. First is proactive routing, in which route are discovered before it is needed. It is also called table-driven routing. Some proactive routing protocols are given as follows: optimizes link state routing, destination-sequenced distance vector. Second is reactive routing in which routes are discovered when they are needed. Some reactive routing protocols are given as follows: dynamic source routing, ad hoc on-demand distance vector. Third is hybrid routing, which have some features of reactive protocol and some features of proactive protocol. Some hybrid routing protocols are given as follows: zone-based hierarchical link state routing protocol, order one MANET routing protocol. Fourth is hierarchical routing in which hierarchic level is maintained. Some hierarchical routing protocols are: cluster-based routing protocol, fisheye state routing protocol [1].

2 AODV Protocol

AODV is an important protocol among many routing protocols in MANET. In ad hoc network, every mobile node maintains a table which has routing information. That table information has the path from source to destination. When a node wanted

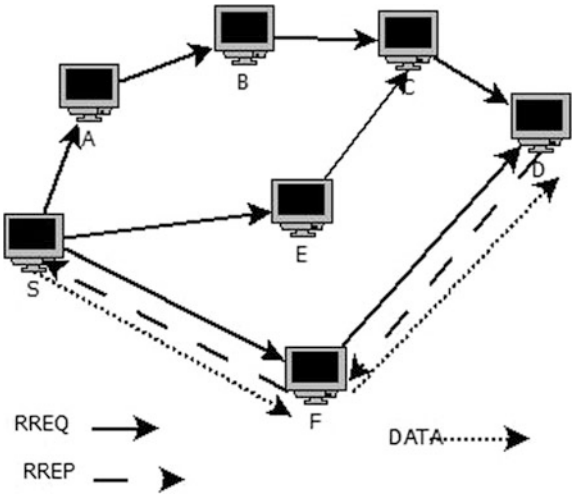

Fig. 2 AODV protocol

to transmit the data packet very first time, it checks the route in the route information table. If table contains the route for the desired destination then the node sends the data along with that route. If the node doesn't have the destination route then the node begins to discover a route by transmitting route request (RREQ) message to all its neighbours. All the nodes who get RREQ message check whether they have desired destination route, if they have route then send route reply (RREP) message to source node otherwise they broadcast RREQ message on behalf of source node [2] (Fig. 2).

Packet format of RREQ message is
<S_Add, SSN, B_Id, D_Add, DSN, Hop>

Packet format of RREP message is:
<S_Add, D_Add, DSN, Hop, Life_Time>

2.1 Blackhole Attack

Route discovery is a main task of AODV routing protocol where an attacker gets chance to attack on the network. When an attacker gets RREQ message and gives a prompt response of fake RREP message. After getting a RREP message source node forward data through that attacker node. When attacker node gets data from the source node, it drops all the data without forwarding data to destination node. This is considered as blackhole attack or packet drop attack [2].

Figure 3 shows an attack of blackhole attack on AODV network. In this network, S defines the source and D defines destination. When source node S wants to send data to the destination node D then it broadcasts RREQ messages to all its

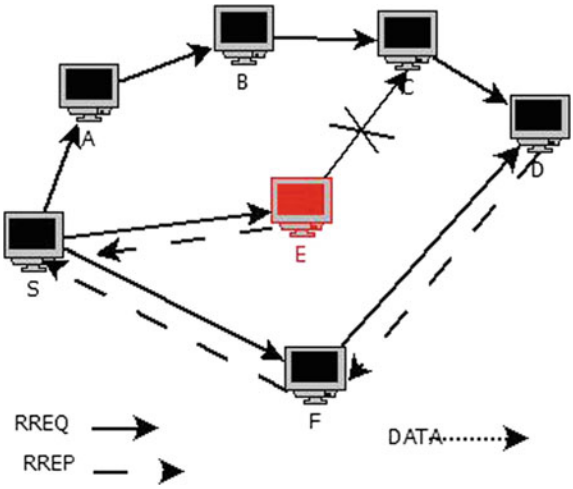

Fig. 3 Blackhole attack

neighbours. When attacker node E gets RREQ message, it immediately unicast fabricated RREP message with highest DSN and lower hop count. When S gets that fabricated RREP then it sends data through node E and node E drops all packets which come to this node.

3 Literature Review

Pooja Jaiswal and Rakesh Kumar [3] proposed their mechanism to prevent network form blackhole attack. In their approach, difference between SSN and DSN is considered. If difference is very high then it comes from an attacker node.

Deng et al. [4] proposed their mechanism to prevent network form blackhole. In their mechanism, sender node searches for alternative path of destination node. If path exists then there is node attack. This approach does not prevent from cooperative blackhole attack.

Tarun Varshney et al. [5] proposed their mechanism to prevent network form blackhole. Their approach is called watchdog mechanism. In their approach, when node sends data, it sets a watchdog. This watchdog monitors that whether the forwarded packet is also forwarded from next node in the route.

Anand A. Aware and Kiran Bhandari [2] proposed an approach to prevent blackhole attack. In this approach, first RREP is ignored as it assumes that it is from attacker. When the source node sends the data packet they use SHA 1 hash function for the message digest. This solution has problem that it is not necessary that first RREP is from attacker, and this solution doesn't prevent cooperative blackhole attack.

4 Proposed Mechanism

In order to prevent the above-described problem, we propose a new mechanism to prevent the attack. This new mechanism prevents the blackhole attack.

4.1 Calculation of Threshold

Sequence number has min value 0 and maximum value is 32-bit arithmetic (2^{32}).

$$\mathrm{DSN}_{\min} = 0 \quad \mathrm{DSN}_{\max} = 4294967295$$

In the proposed approach, we are defining a threshold value for the elimination of malicious node. Malicious node sends very high sequence number, nearer to the $\mathrm{DSN}_{\max}$. So we are defining the threshold by the calculation of following formula:

$$Th = DSNmax \times 97\%$$

where Th is the defined threshold. By defining this threshold, actually we are eliminating 3% of maximum sequence number, because attacker used sequence number nearer to maximum sequence number.

4.2 Flow Diagram for Additional Processing

Once threshold is defined, RREP message is verified by using that threshold value. When source node gets RREP message for the RREQ message which the source node generates it verifies those RREP messages. Figure 4 shows the processing flow chart at the source node.

4.3 Improved AODV Mechanism

In AODV, source node broadcasts RREQ and this message is forwarded until it reaches to the destination. Destination generates RREP for that RREQ. Improved mechanism can prevent attack on network. Improved mechanism is shown below:

Symbolisation	
S	Source Node
D	Destination Node
I	Intermediate Node
Th	Threshold
DNS	Destination Sequence Number

(continued)

(continued)

Improved_AODV (input: RREP)	
1.	Begin
2.	S broadcast RREQ to all its neighbours
3.	I receive RREQ reply if have fresh route otherwise forward
4.	D receive that RREQ
5.	D generate RREP and unicast it through the route RREQ came
6.	When S receives RREP, S checks DSN of RREP
7.	If DSN less than Th
8.	Route established
9.	Else
10.	Discard RREP
11.	End if
12.	Encrypt data and transmit it to D
13.	D receives data and Decrypt
End	

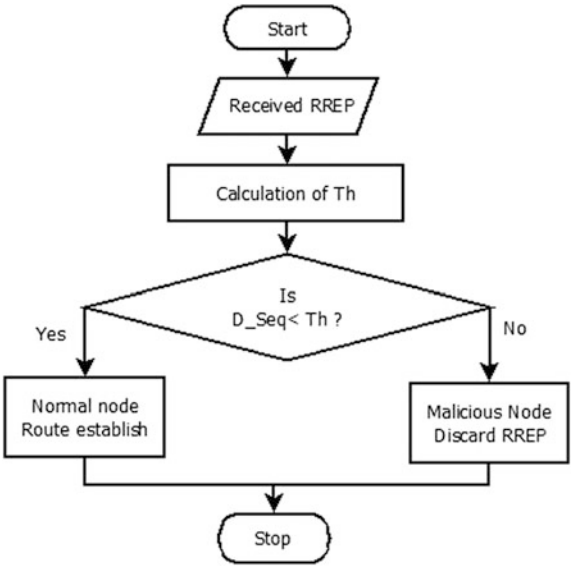

Fig. 4 Flow chart for additional process at source node

5 Simulation and Analysis

We have used network simulator 2 (NS2) for the simulation purpose. NS2 is a tool which provides implementation to different protocols. At the physical and data link layer usages IEEE 802.11 and network layer usages AODV routing protocol to route the packet. We are using 10–75 mobile nodes with transmission rate of 0.2 Mbps. The results of simulation are shown below (Figs. 5, 6 and Table 1).

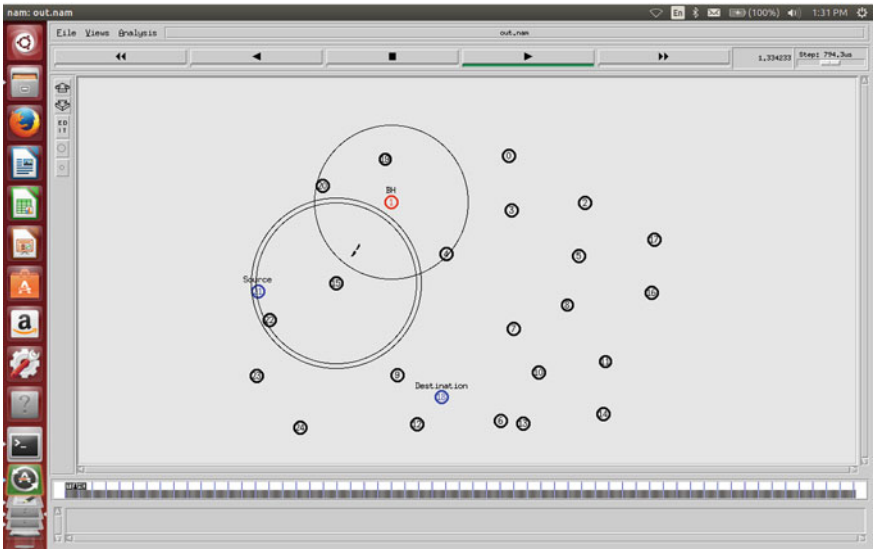

Fig. 5 Screenshot of blackhole attack

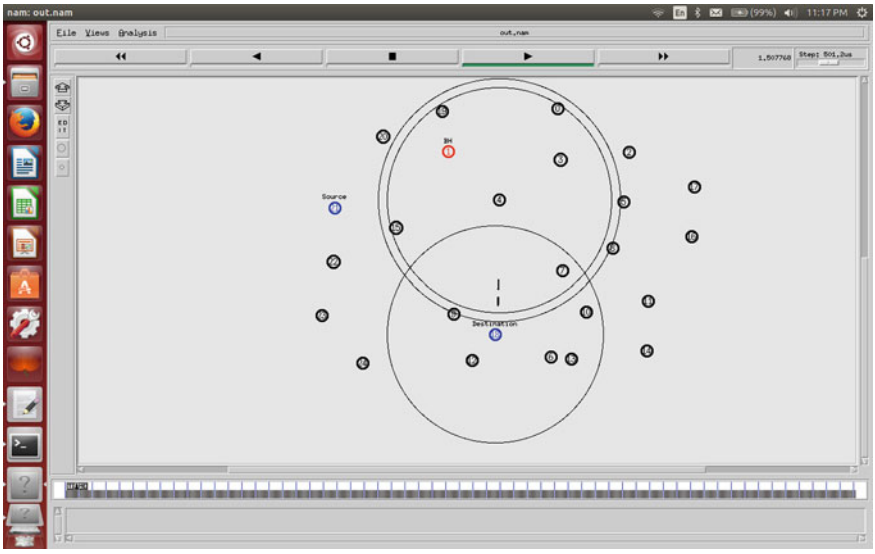

Fig. 6 Screenshot of prevention in case of single blackhole

Table 1 Simulation parameters

Constraint	Value
Simulator	NS2
MAC layer protocol	IEEE 802.11
No. of nodes	10–75
Routing protocol used	AODV
Simulation time	100 s
Traffic model	CBR
Terrain area	1000 m × 1000 m

5.1 Simulation Result

Simulation results are shown by the help of following graphs. These graphs show packet delivery ratio, throughput and delay with change of number of nodes in case of single blackhole and PDR with change of number of nodes in case of multiple attacker nodes are present means under cooperative blackhole attack.

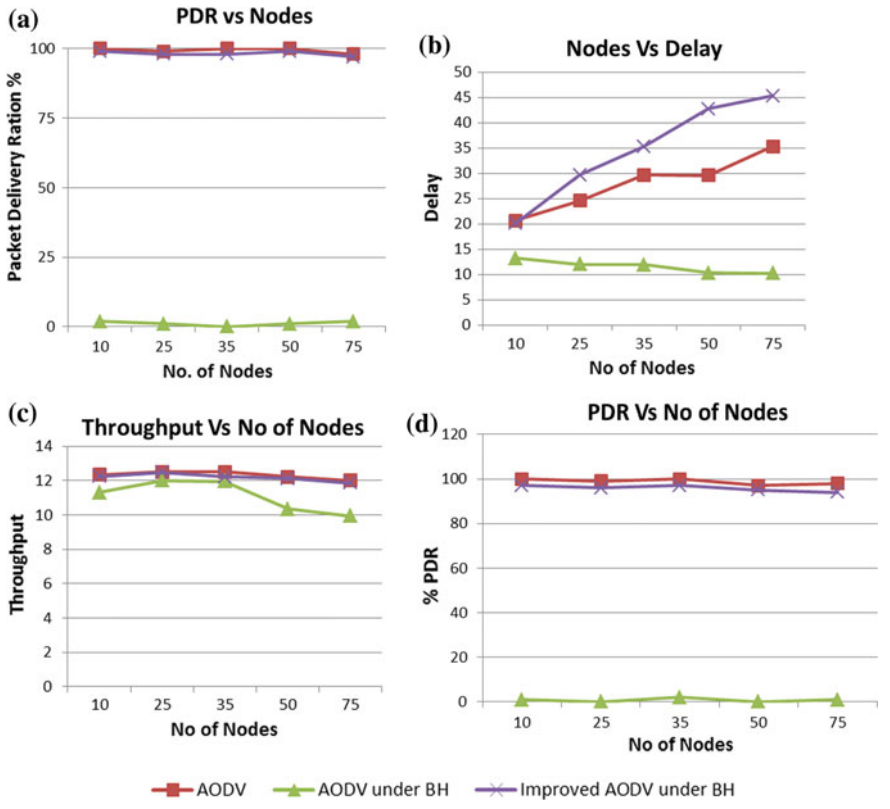

Fig. 7 **a** Effect of PDR with number of nodes. **b** Effect of time delay with number of nodes. **c** Throughput of the network with number of nodes. **d** Effect of PDR with number of nodes in case of multiple blackhole nodes

6 Conclusion and Future Work

MANET has a dynamic infrastructure and battery constraint. Complex computation consumes more battery power. Improved mechanism is capable for prevention of blackhole attack and increases the PDR and throughput of the network, and it does not have high complex computation. This improved mechanism is also capable for preventing cooperative blackhole attack.

In future, we are going to mitigate the time delay. We think there are some other directions which mitigate the effect of blackhole attack in a better way.

References

1. Singh, A., Hasan, M.: An analysis of prevention mechanism of blackhole attack. In: 2016 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS'16), Tamilnadu, vol. 1, pp. 117–122 (2016)
2. Aware, A.A., Bhandari, K.: Prevention of black hole attack on AODV in MANET using hash function. In: 2014 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), pp. 1–6. IEEE (2014)
3. Jaiswal, P., Kumar, R.: Prevention of black hole attack in MANET. Int. J. Comput. Netw. Wirel. Commun. **2**(5) (2012)
4. Deng, Hongmei, Li, Wei, Agrawal, Dharma P.: Routing security in wireless ad hoc networks. IEEE Commun. Mag. **40**(10), 70–75 (2002)
5. Varshney, T., Sharma, T., Sharma, P.: Implementation of watchdog protocol with AODV in mobile ad hoc network. In: 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), pp. 217–221. IEEE (2014)