Black Hole Attack Detection in MANET Using Mobile Trust Points with Clustering

Manjeet Singh(✉) and Prabhdeep Singh

Department of Computer Science and Engineering,
Guru Nanak Dev University, Amritsar, India
ms.bajwaa@gmail.com, prabhdeepsingh2991@gmail.com

Abstract. MANET is a set of mobile nodes in which communication occurs between them using wireless links. Infrastructure less, dynamical topology and Lack of central communication of nodes makes it vulnerable to various kinds of attacks. One of the major security problems is Black Hole attack in which node silently drops the packets in the network. In this paper, we propose a solution to mitigate this attack in MANET using mobile trust points with clustering. The proposed method uses some mobile trust points which monitor the activities of cluster heads to detect the attack and then generate alert in the network if any black hole node detected.

Keywords: MANET · Clustering · Black hole · Mobile trust points

1 Introduction

MANET (Mobile Ad hoc Networks) contains self organized mobile nodes without any infrastructure having dynamic topology. In MANET, Nodes can join and leave network anytime [1]. Nodes in the network can act as host or router. Nodes can route packet to help other nodes, thereby forming a network. Due to its simplicity and flexibility, MANETs are suitable for various applications such as emergency rescue operations, battlefield communication and vehicular communication. Lack of centralized management, dynamic topology and limited resources, make MANETs more vulnerable to various security issues than wired networks.

For routing in MANET various Protocols are used which control the way of packet transfer between source and destination [3]. Proactive, active and hybrid are three categories of protocol. In proactive, Routing tables are maintained for communication in the network. Continuously updating routing tables increases route availability but creates network overhead. Destination Sequenced Distance Vector (DSDV) is an example of Proactive Protocol [11]. Reactive protocol uses on demand route discovery process to calculate routes in the network which causes delays in the network. Dynamic Source Routing (DSR) and Ad hoc on demand Distance Vector (AODV) is an example of reactive protocol [10]. Hybrid protocol combines both reactive and proactive protocols to exploit efficient communication in the network. Zone Routing Protocol (ZRP) is an example of this routing protocol [12].

Passive and Active attacks are two categories of attacks in MANET. In Passive attacks, attacker gets the information from the network without doing any alteration [2]. Eaves

A. Unal et al. (Eds.): SmartCom 2016, CCIS 628, pp. 565–572, 2016.
DOI: 10.1007/978-981-10-3433-6_68

dropping, traffic control and monitoring are examples of Passive attacks. Active attack disrupted normal functioning of network by altering or destroying data. Black hole and worm hole are active attacks. In this paper, we tackle black hole attacks in AODV routing protocol. In black hole attack, malicious node falsely claiming shortest path to destination by replying to every route request and then drops every packet coming to it [4].

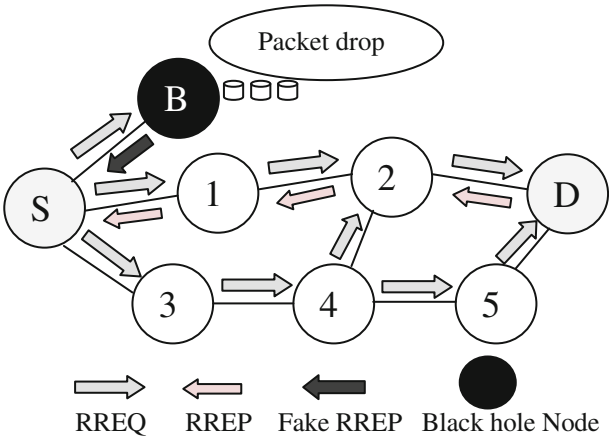

Fig. 1. Black hole attack

Figure 1 illustrates working of black hole attack in MANET. Black Hole node B falsely reply with Fake RREP claiming fresh route to the D (Destination Node) and node S (Source) starts sending data to node B. B (Black hole node) starts dropping all the packets.

The rest of the paper is organized as: Sect. 2 describes related work. Section 3 presents the proposed method and results are discussed in Sect. 4. Finally, conclusion and discussion is in Sect. 5.

2 Related Work

A number of works have been done to tackle black hole attacks in MANET. This section discusses some of these works.

In [5], network is divided into clusters and the trust value calculated between the nodes by their interaction behaviour. A secret key is distributed among various nodes by cluster heads to provide secure communication, only the nodes which know the key can decrypt the message. Another method is proposed by [6] in which TimerExpiredTable and CRRT (Collect Route Reply Table) are used. After the expired time all the entries in the CRRT table are checked. The RREP in which there is repeated next hop nodes are selected. It assumes that the path is correct. This Method is good only in those cases when more RREP packets arrive at source node to select a secure path. The limitation of this solution is that sometimes a secure and the shortest path gets eliminated at source.

Promiscuous mode is used to mitigate black hole and the alert of malicious node is generated in the solution discussed in [7]. In this method, after receiving RREP reply from an intermediate node, a node preceding the intermediate node switch on its promiscuous mode and sends a "hello" packet to the destination node using this node. If the destination receives the hello message from this node, then node and the route are safe to use. This method gives better results as database and extra memory is not required but have more average end-end delay than the normal AODV.

Secured and efficient protocol SAODV is implemented by [8]. In SAODV routing protocol destination is directly verified using the random numbers. SAODV can prevent black hole attack efficiently. But this protocol adds some burden to the network such as extra memory and calculations in route discovery phase. Another method detects the black hole in AODV and finds a safe route using wait and then checks the replies coming from the nodes [9]. The route is selected based on repliers of RREP. The activities of a node are noted by its neighbor nodes and send their opinion to the source node. After collecting all the opinions, a source node decides whether there is a Black hole node or not. The proposed method provides better performance but overhead is involved.

3 Proposed Method

In Proposed Method, network is divided into cluster form which contains mobile nodes, cluster heads and mobile Trust points.

3.1 Mobile Nodes

Nodes are free to move and can participate in communication with each other and cluster head.

3.2 Cluster Head

When the mobile node wants to communicate with any other node not within its range, it will send data packets using cluster head.

```
//Black Hole Detection at Cluster Head (CH) level
Prepare Black_hole_list

1. CH sends data to its member and waits for reply for maximum time tm.
2. Within time tm members send reply data packet to their CH except black hole nodes.
3. CH checks the nodes from its table which has not send data.
4. Add these nodes to the black_hole_list
```

```
//Black hole detection at Mobile Trust Point (MTP) level
Prepare Blackhole_list

1. MTP sends request to send black_hole_list to their cluster
heads and wait for reply for maximum time tm.
2. Within time tm, CH sends black_hole_list except the
clusters which are black hole.
3. MTP checks the Cluster head which has not send any list.
4. Add that CH to blackhole_list and elect any node in that
cluster as CH.
```

Procedure for Black hole detection

3.3 Mobile Trust Points

These are used to check the activities of cluster head and do communication with cluster heads after some time to detect whether cluster heads are Black hole or not.

4 Simulation Results

The simulations are performed using ns-2. A flat plane of 1000 × 1000 m is used where nodes are placed. The Two Ray Ground model is used for radio propagation. Nodes mobilize at random speed which is 10 m/s. For Media Access Control protocol 802.11 is used. Each node has 250 m communication range. There are total 100 mobile nodes with 10 cluster heads and 10 mobile trust points. The number of malicious nodes is between 5, 10, 15 and 20 respectively.

Various parameters considered are packet delivery ratio (PDR), end to end delay, average throughput and detection rate. Detection rate is number of Black Bole node detected to total number of black hole nodes.

Figure 2 shows the comparison of packet delivery ratio and malicious nodes. Proposed method is showing better packet delivery ratio after detection of Black Hole attack. By calculating results of packet delivery ratio under 5, 10, 15, 20 Black Hole nodes, packet delivery ratio remains consistent even after increasing number of Black Hole nodes. It shows the consistency of proposed technique.

Next performance metrics is average end to end delay. Figure 3 showing significant delay occurs during communication under black hole in AODV. Under normal AODV delay is lesser and after applying the proposed method delay is almost similar to normal AODV. Results are clearly showing that proposed algorithm gives good result after detection of black hole attack.

Results in Fig. 4 are showing a good detection rate of black hole nodes. When detection rate calculated for 5 black hole nodes, all of them are detected using proposed method. Even after taking the number of black hole nodes as 10, 15 and 20, detection rate is almost 90%, which in itself shows how well this method is efficient to detect black hole nodes.

Average throughput is calculated for AODV, AODV under black hole attack and proposed method. There is decrease in network throughput in AODV under black hole

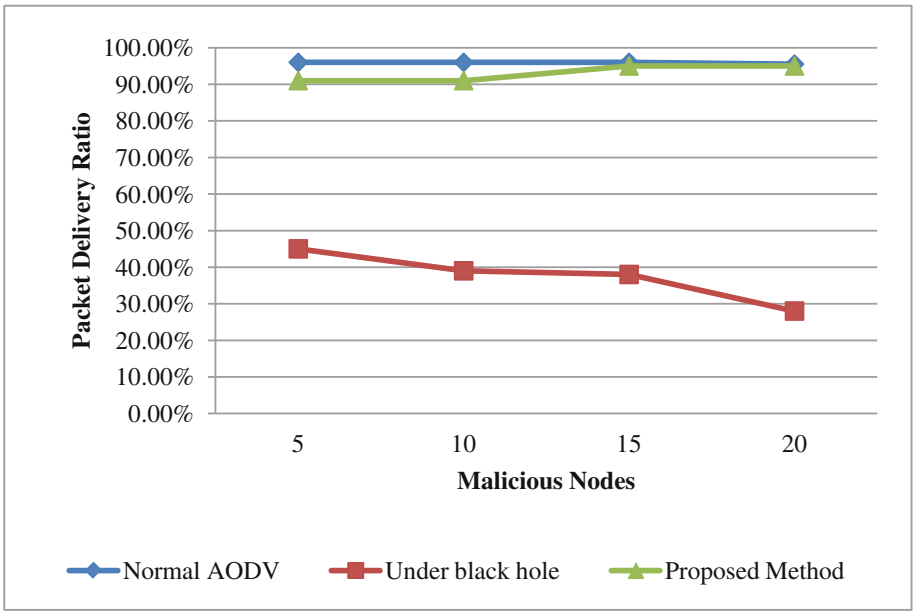

Fig. 2. Packet delivery ratio

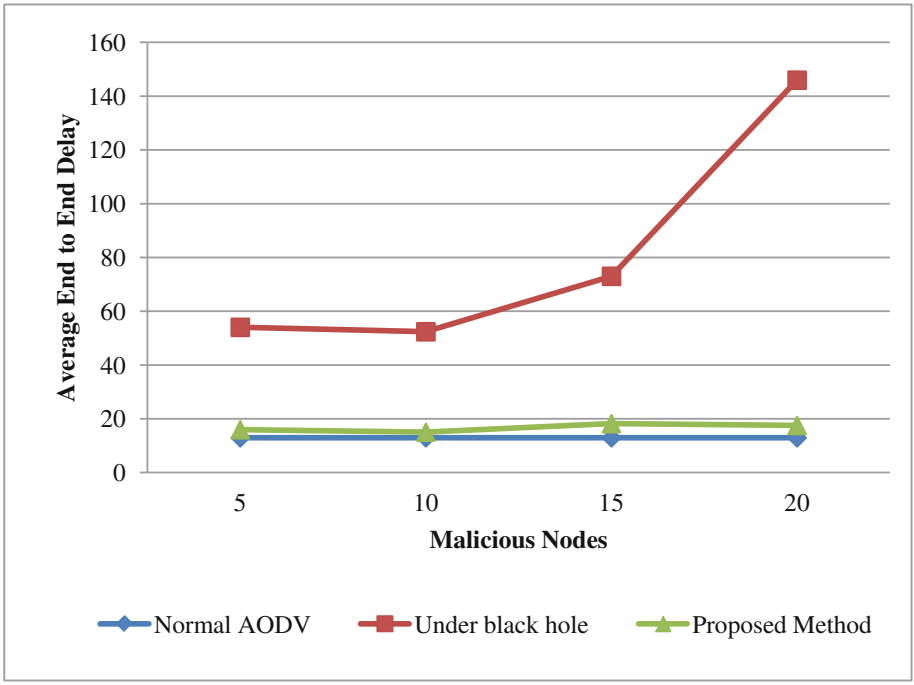

Fig. 3. Average end to end delay

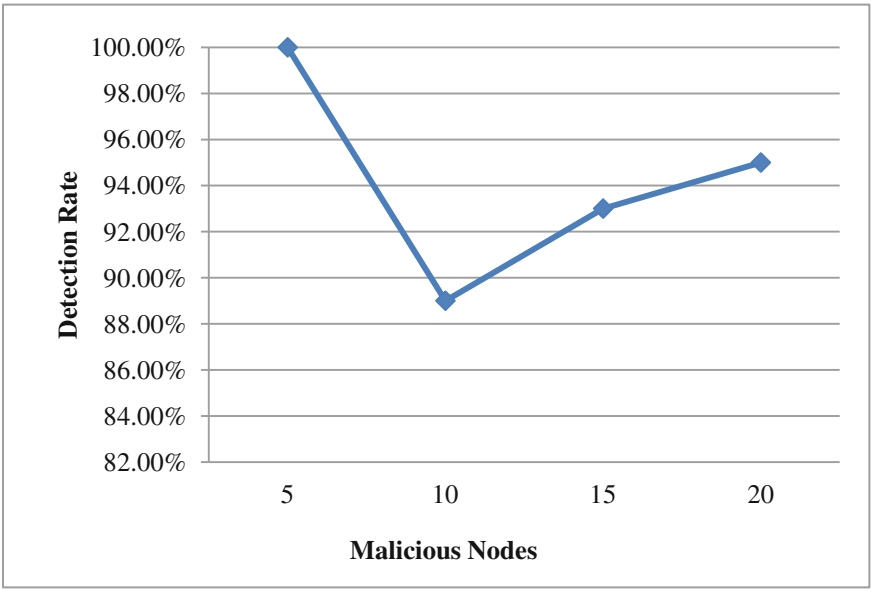

Fig. 4. Detection rate

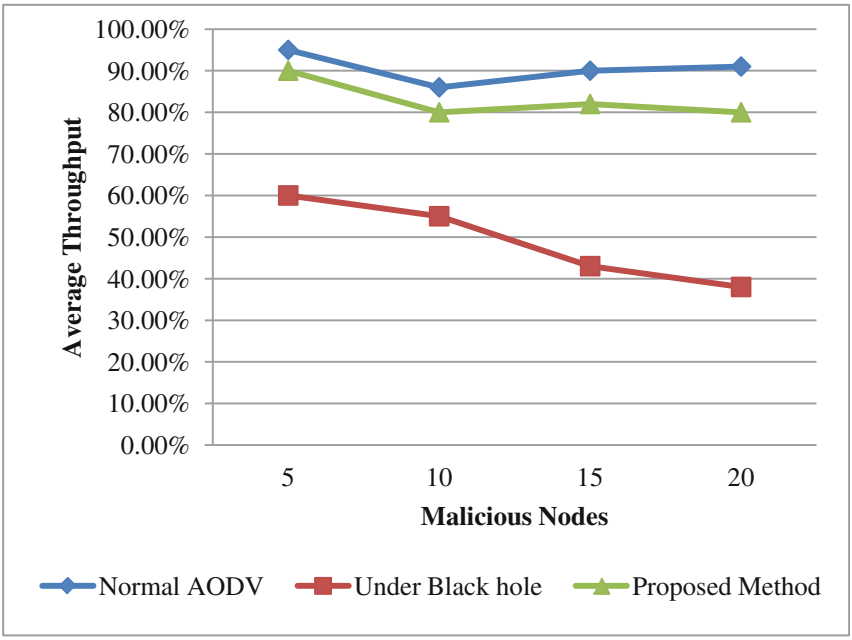

Fig. 5. Average throughput

attack but increases between 80 to 90%. So results in Fig. 5 are showing average throughput increases in proposed method.

5 Conclusion and Future Work

Clustering and Mobile Trust Points based technique has been proposed for detection of black hole attack. Overview of some previous work is listed for prevention and detection of black hole. The approach is to monitor the activities of cluster head and the normal nodes and maintain a list of black hole nodes. Results are showing effectiveness and consistency to detect black hole nodes. Performance is measured and the results are proving the proposed method as promising one. PDR (Packet delivery ratio) and the average throughput increases in proposed method after detection of black hole attack. Also, average end to end delay is very less as compare to AODV under black hole attack. Detection rate of black hole nodes is around 90% in this technique.

In future, this work can be extended to scale the network to find performance and accuracy of this technique. It can also be implemented for detection of other types of attacks. The technique is promising to give good results in other attacks too.

References

1. Ramanathan, R., Redi, J.: A brief overview of ad hoc networks: challenges and directions. IEEE Commun. Mag. **40**(5), 20–22 (2002)
2. Li, W., Joshi, A.: Security issues in mobile ad hoc networks-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County (2008)
3. Hinds, A., Ngulube, M., Zhu, S., Al-Aqrabi, H.: A review of routing protocols for Mobile Ad-Hoc NETworks (MANET). Int. J. Inf. Educ. Technol. **3**(1), 1–5 (2013)
4. Jhaveri, R.H., Patel, S.J., Jinwala, D.C.: Dos attacks in mobile ad hoc networks: a survey. In: 2012 Second International Conference on Advanced Computing & Communication Technologies (ACCT), pp. 535–541. IEEE (2012)
5. Savner, J., Gupta, V.: Clustering of mobile ad hoc networks: an approach for black hole prevention. In: 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 361–365. IEEE (2014)
6. Tamilselvan, L., Sankaranarayanan, V.: Prevention of blackhole attack in MANET. In: The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, AusWireless 2007, p. 21. IEEE (2007)
7. Singh, P.K., Sharma, G.: An efficient prevention of black hole problem in AODV routing protocol in MANET. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902–906. IEEE (2012)
8. Lu, S., Li, L., Lam, K.-Y., Jia, L.: SAODV: a MANET routing protocol- that can withstand black hole attack. In: International Conference on Computational Intelligence and Security, CIS 2009, vol. 2, pp. 421–425. IEEE (2009)
9. Medadian, M., Mebadi, A., Shahri, E.: Combat with black hole attack in AODV routing protocol. In: 2009 IEEE 9th Malaysia International Conference on Communications (MICC), pp. 530–535. IEEE (2009)

10. Mbarushimana, C., Shahrabi, A.: Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In: 21st International Conference on Advanced Information Networking and Applications Workshops, AINAW 2007, vol. 2, pp. 679–684. IEEE (2007)
11. Tuteja, A., Gujral, R., Thalia, S.: Comparative performance analysis of DSDV, AODV and DSR routing protocols in MANET using NS2. In: 2010 International Conference on Advances in Computer Engineering (ACE), pp. 330–333. IEEE (2010)
12. Kaur, R., Rai, M.K.: A novel review on routing protocols in MANETs. Undergraduate Acad. Res. J. (UARJ) (2012)