International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.3, September 2014

A Novel Approach for Preventing Black-Hole Attack in MANETs

Rashmi[1], Ameeta Seehra[2]

Department of Electronics and Communication Engineering, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India

ABSTRACT

A black-hole attack in the Mobile Ad-hoc NETwork (MANET) is an attack occurs due to malicious nodes, which attracts the data packets by falsely advertising a fresh route to the destination. In this paper, we present a clustering approach in Ad-hoc On-demand Distance Vector (AODV) routing protocol for the detection and prevention of black-hole attack in MANETs. In this approach every member of the cluster will ping once to the cluster head, to detect the peculiar difference between the number of data packets received and forwarded by the node. If anomalousness is perceived, all the nodes will obscure the malicious nodes from the network.

KEYWORDS

Mobile Ad-hoc Networks, Black-hole attack, AODV, Routing Protocols, Security, Clustering, Cluster-head.

I. INTRODUCTION

A MANET consists of several mobile nodes that are connected by wireless links and each mobile node acts not only as a host but also as a router to establish a route. When a source node intends to transfer the data packets to the destination node, then the packets are transferred through intermediate nodes, thus quick deployment of the nodes to establish a route is the important issue in MANET.

Routing protocols in MANET are mainly divided into categories Proactive and Reactive routing protocols and other type is Hybrid (Reactive/Proactive) routing protocols. Proactive Routing Protocols are also called table driven protocols which maintain the lists of all possible destination nodes in a table and periodically exchanges routing messages, in order to keep the information in the routing table up-to-date and correct. When transmission is required from one node to another, the route is already known and can be used. Examples of Proactive Protocols are Optimized Link State Routing Protocol (OLSR) Protocol, Distributed Sequenced Distance Vector (DSDV) Protocol [1]. On the other hand, Reactive Protocols like AODV and DSR protocols are on demand routing protocols i.e. invoke the route determination procedure only on demand [2]. When route is needed, some sort of Route Discovery procedure is employed, because these protocols assume cooperation between two nodes for packet forwarding, a malicious node may lead to routing attack in the network that disrupts the normal routing operations of MANET. Thus decentralized and dynamic nature of MANET may lead to various attacks in the network that can partition or destroy the network.

Generally there are two types of attacks in the MANETs, one is Passive attack and other is Active attack. In Passive attack, the intruder silently listen the communication channel without modifying or destroying the data packets [3]. But in Active attack, intruder can modify or destroy the original data. Due to minimal configuration and quick deployment, MANETs are suitable for emergency situations like Natural disasters rescue operation, hospitals, battlefield, conferences and Military applications. Thus data transfer between two nodes must require security. But the active attacks like

Black hole attack, Rushing attack, Wormhole attack have great impact on the performance of the network [4].

Black hole attack is a special type of attack that generally occurs in the Reactive protocols. A black-hole node is the malicious node that attracts the packets by falsely claiming that it has shortest and fresh route to reach the destination, then drops the packets. These Black hole nodes may perform various harmful actions on the network that are [5]:

- Behaves as a Source node by falsifying the Route Request packet.
- Behaves as a Destination node by falsifying the Route Reply packet.
- Decrease the number of hop count, when forwarding Route Request packet.

In this approach, if the ratio of number of packets received to the number of packets sent is less than threshold then the destination node start the detection process. The difference between number of packets received by a node and number of packets forwarded by it is significant then node is declared as the malicious node and is isolated from the network.

II. RELATED WORK

In [6-13] various security techniques and routing protocols have been proposed for the prevention of single and cooperative black hole attacks in the network.

Mohanapriya and Krishnamurthi in [14] presented a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. The source node selects the first shortest path to the destination, to intimate the no. of data packets it sends to the destination. The source node then selects the second shortest path for actual transmission of data. Then packet count and transmitted data both are compared. If difference is significant i.e. abnormality is detected the nearby IDS node broadcast a message informing all nodes to obscure all nodes from network. In [15], a new Routing Security Scheme based on Reputation Evaluation (RSSRE) is proposed. The reputation evaluation mechanism is built on the basis of correlation among nodes that need to be evaluated. It has the mechanism to promote the cooperation of cluster members for forwarding data packets to execute improved routing when there are malicious nodes in hierarchical Ad Hoc networks. In [16], authors proposed checkpoint-based Multi-hop Acknowledgement Scheme, for detecting selective forwarding attacks which can select the intermediate nodes randomly as checkpoint nodes which will generate acknowledgements for each packet received. Intermediate node has to send the acknowledgment for every packet that it is receiving; the algorithm has to suffer from overhead. Moreover, the channel is assumed perfect. Gao and Chen [17] proposed three security algorithms such as full proof algorithm, check-up algorithm and diagnosis algorithm. The full proof algorithm was for creating proof and the check-up algorithm was for checking up source route nodes; and the diagnosis algorithm was for locating the malicious nodes in the network. In approach [18], Jaisankar et al. presented that each node should have Black hole Identification Table (BIT) that contains source, target, current node ID, Packet received count (PRC), Packet forwarded count (PFC). If difference between PRC and PFC is significant, then the node is identified as malicious and is isolated from the network. In [19], Chavda and Nimavat proposed an algorithm to remove black hole attack at the cost of overhead. The source node continues to accept RREP packets from the various nodes and compares RREP (RREP R1, RREP R2) which actually compares the destination hop count of two route replies and selects the route reply with high destination hop count if the difference between two hop counts is not significantly high. In [20] Wang et al. proposed an approach to improve the scalability and efficiency of MANETs by arranging the nodes on the basis of trust mechanism. In our method, the trust value is calculated on the basis of cooperation between nodes. In [21] Yang proposed Anti Black Hole mechanism (ABM). Suspicious value of a node is estimated by ABM, on the basis of amount of significant

difference between RREQs and RREPs transmitted by the node. If an intermediate node i.e. not the destination node receives a RREQ, but do not forward it for a specific route, but forward RREP for the route, then its suspicious value is increased by 1 in the suspicious node table of neighbor IDS node. If suspicious value of a node exceeds its threshold value, then IDS node broadcasts a block of message to all the nodes to isolate suspicious node from the network. But the gray-hole nodes participate in the process of route discovery.

III. PROPOSED METHODOLOGY

Our model is based on following assumptions: (A) All nodes are identical in their physical characteristics. (B) Cluster head is selected as a node located at the centre of cluster. (C) All the black-hole nodes will drop exactly the half of total number of data packets. (D) The source nodes and the destination node are taken as trusted nodes by default.

Protocol Description

In AODV protocol, the source node broadcasts RREQ packet to find the path to reach the destination. The destination node having the path will send the RREP to the source node in response. Figure 1(a) shows the black-hole nodes will also participate in Route Discovery process and will claim for the shortest route to the destination. If the route is chosen through the black-hole node, then it can drop the data packets as shown in Figure 1(b). Thus to prevent the black-hole attack, a novel approach is drawn. In this approach the deployed nodes are divided into clusters such that each cluster will have a cluster head and the remaining nodes are called the members of that cluster. The cluster head can be chosen randomly from each cluster. Some check-points are deployed in the network so as to check whether the no. of data packets received by the nodes and no. of packets sent by the nodes are equal. Transmissions can take place within the cluster or from one cluster where the source is located to another where destination is.

Procedure1: Cluster Member level presence of Black-hole nodes

When the source node and the destination node are located within the same cluster data transmission will take place from the source to the destination which is at 1 hop distance away from the source. First the source node will send QREQ (Query REQuest) packet to all the neighbors, the destination node which is at single hop distance from the source will send QREP (Query REPly) packet in response. Every member of the cluster will ping once to its cluster head, the member that does not ping is considered as malicious node and cluster head move it into the suspected list. The nodes that are correct can participate in data transmission. But here only source and destination

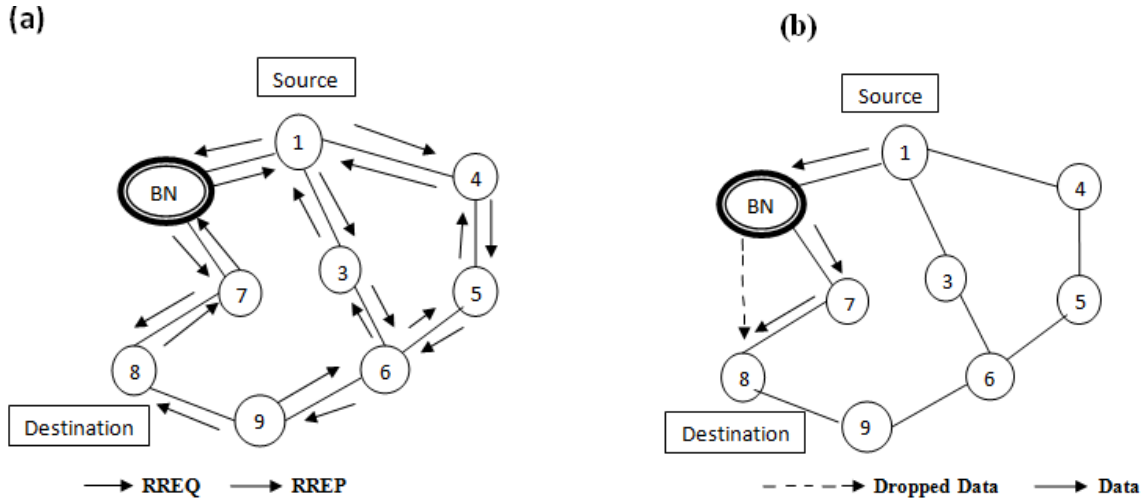

Figure 1: Route Discovery Process in AODV

nodes participate in transmission and are considered as trustworthy. Thus all the packets are transferred to the destination.

Procedure 2: Cluster Member level presence of Black-hole nodes

If the source node is the member of one cluster and the destination is the member of other then data transmission will takes place through there cluster heads. The cluster head of the one cluster will communicate with that of other. First the source node broadcasts Query REQuest (QREQ) packet to its cluster head (CH_1) through which it is transferred to the cluster head (CH_2) of another cluster of which the destination node is the member and last to the destination. Then a route (S, CH_1, CH_2, D) establishes as shown in figure 2. Check-point verifies whether the intermediate nodes (say CH_1, CH_2) are forwarding all the data packets correctly; it receives from the previous nodes. If not correct, the check-point moves intermediate nodes CH_1 and CH_2, into the suspected list. If correct, it means two nodes are participating correctly in data forward.

Let the no. of data packets forwarded by the source node S to the destination node D be N_s and (S, CH_1, CH_2, D) be the route for data forwarding. Check-point (CP) keeps count of the number of packets each node receives and forwards to the downstream. When the destination node receives the data packets from the source, check-point keeps the count of the number of packets the destination received. Let the destination D receives N_d number of packets. Then the probability of packets received at destination is as follows:

$$P_d = \frac{N_d}{N_s}$$

If P_d < T, then the check-point starts the process of detecting whether the malicious node is present in the route. If not, then it receives positive acknowledgment from the destination. Here packet loss threshold takes the value from 0 to 0.2. In this approach if the packet loss exceeds 20% of the total packets sent by the source node the check-point starts black-hole detection process. Source node will transmit next packet of data only after receiving the positive acknowledgement from destination.

Figure 2. Clustering Of Manet

IV. EXPERIMENTAL SET UP AND ANALYSIS

This paper is applied to ns-2 to validate the detection and isolation efficiency of the proposed method against black-hole nodes. In an area of $1500\times1500m^2$, 100 normal nodes executing AODV routing protocol were randomly distributed, and a couple of malicious nodes performing black-hole attack, and 4 Check-point nodes are randomly located. The major parameters of experiment are listed in Table1 and the data in this section is obtained by taking average value, which results from 10 experiments.

Also our approach is also compared with an existing approach proposed in [14]. In order to evaluate the performance of clustering approach following metrics have been measured:

Table1. Simulation parameters

Properties	**Value**
Simulator	ns2
Coverage area	1500×1500
Number of nodes	104
Simulation time	600 s
Mobility	Random way point model
Mobility speed	20 m/s
Number of black-hole nodes	5
Mobile check-point nodes	4
Traffic type	UDP-CBR

- **Packet delivery ratio:** Ratio of total number of packets received at the destination to the total number of packets sent.
- **Throughput:** The rate of successful delivery of packets over a communication channel. It is usually measured in bits per second (bps).

- **Detection rate:** Total number of suspected nodes over misuse and anomaly detecting nodes.

(a)Packet delivery ratio- Packet delivery ratio in our approach is 1 i.e. the number of nodes a source sends is same as the number of packets destination receives. Thus on comparing our approach with [14] we get PDR in both cases is same. In our approach, mobile checkpoints will detect the number of data packets forwarded to and by the nodes in the route and monitor the data packet loss.

(b)Detection Rate: is total number of nodes detected (whether these are malicious or not) from the overall network, therefore the detection rate should be high in mobile ad-hoc network. In the proposed approach, detection rate is about four times the approach [14]. Simulation results are shown in fig 4.

(c)Throughput: is number of data packets delivered per second. It is also expressed in number of bits per second. In our proposed approach throughput obtained is near about 1.5 times that in approach [14] as shown in fig 5.

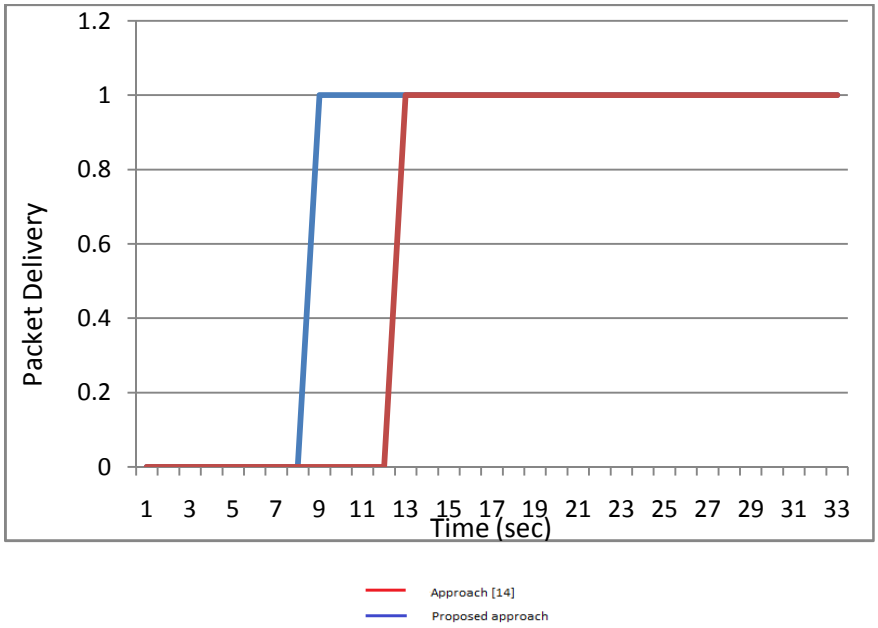

Figure 3. Packet Delivery Ratio (PDR)

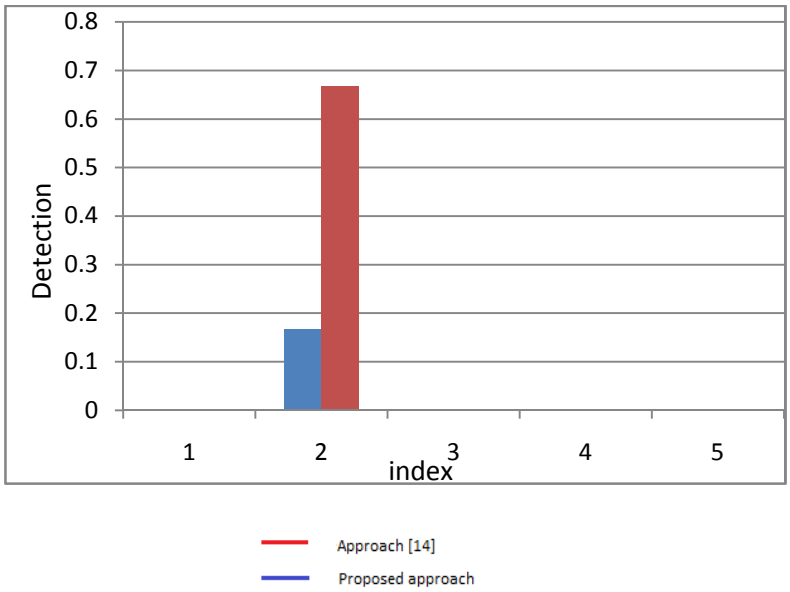

Figure 4. Detection Rate

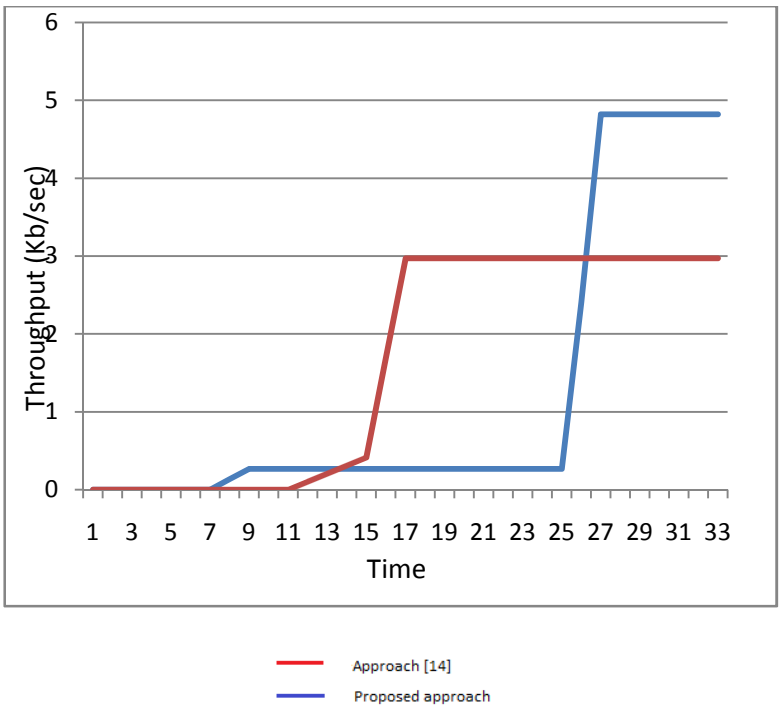

Figure5. Throughput

V. CONCLUSION

A light weight solution is proposed which is based on simple acknowledgement scheme to prevent black-hole nodes in MANET. It can be incorporated with any existing on demand ad hoc routing protocols. By the proposed approach, the mobile check-points detect the presence of malicious nodes in the source route and with the help of intrusion detection system the suspected nodes are obscured from the network.

The simulation results show that clustering approach is responsible for full delivery of packets even in presence of multiple black-hole nodes. Also the detection rate and throughput are improved by four times and 1.5 times respectively as compared to approach [14]. Thus our proposed approach is better and secure.

References

[1] Mehran, A. and Tadeuz, W., (2004) "A review of routing protocols for mobile ad hoc networks", International Journal on Ad hoc Networks, Vol. 2, No.1, pp.1–22.

[2] Johnson, D. B., Maltz, D. A. and C. Y. Hu, C. U., (2004) "The dynamic source routing protocol for mobile ad-hoc network (DSR)", IETF Internet Draft.

[3] Bar, R. K., Mandal, J. K. and Singh, M., (2013) "QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack", International Conference on Computational Intelligence: Modeling Techniques and Applications, India, pp. 530-537.

[4] Deng, H., Agarwal, P., (2002) "Routing security in wireless ad hoc networks", IEEE Communication Magzine, Vol. 40, No. 10, pp. 70–75, 2002.

[5] Lee, S., B. Han, B. and Shin, M., (2002) "Robust routing in wireless ad hoc networks", In: ICPP Workshops, pp. 73-79 .

[6]Dokurer, S., Erten, Y., and Erkin, C., (2007) "Performance analysis of ad-hoc networks under black hole attacks" In: Proc. of the IEEE South-east Conference, pp. 148–53.

[7] Tamilselvan, L., and V. Sankaranarayanan, (2007) "Prevention of black hole attack in MANET", In: Proc. of the international conference on wireless broadband and ultra wideband, communication.

[8] Tamilselvan, L. and Sankaranarayanan, V., (2008) "Prevention of co-operative black hole attack in MANET" International journal on Networks, Vol. 3, No.5, pp. 13–20.

[9] Satoshi, K., Hidehisa, N., Nei, K., Abbas, J., and Yoshiaki N. , (2007) "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method". International Journal on Network Security, Vol. 5, No. 3, pp. 338–346

[10] Luo, J., Fan, M. and Danxia, Y., (2008) "Black hole attack prevention based on authentication mechanism" In: Proc. of the IEEE international conference on communication systems, Singapur, pp. 173–177.

[11] Soufine, D., Farid, N. and Ashfaq, K., (2008) "An acknowledgment-based scheme to defend against cooperative black hole attacks in optimized link state routing protocol" In: Proc. of the IEEE international conference on communications, pp. 2780–2785.

[12] Lu, S. and Li, L., (2009) "SAODV: a MANET routing protocol that can withstand black hole attack", In: International conference on computational intelligence and security, IEEE Computer Society, pp. 421–425.

[13] Chao, C., and Yuh, T., (2011) "A context adaptive intrusion detection system for MANET', international journal on Computer Communications, Vol. 34, No. 4, pp. 310–318.

[14] Mohanapriya, M. and Krishnamurthi, L., (2014) "Modified DSR protocol for detection and removal of selective black hole attack in MANET", International Journal on computers and electrical engineering, Vol. 40, No. 2, pp. 530-538, Elsevier.

[15] Yao, Y., Guo, L., Wang, X., and Liu C., (2010) "Routing security scheme based on reputation evaluation in hierarchical ad hoc networks", IEEE Journal on Computer Network, Vol. 5, No. 4, pp. 1460-1469.

[16] Xiao, B., Yu, B., and Gao, C., (2007) "CHEMAS: identify suspect nodes in selective forwarding attacks" International Journal in Parallel Distributed Computer networks, Vol. 67, No. 11, pp. 1218–1230, Elsevier.

[17] Gao, X. and Chen, W., (2007) "A novel gray hole attack detection scheme for mobile ad-hoc networks". In: International Conference on network and parallel computing workshops, , pp. 209–14.

[18] Jaisankar, N., Saravanan, N. and Swamy, K. Durai., (2010) "A Novel Security Approach for Detecting Black Hole Attack in MANET", Proc. Business Administration and Information Processing Heidelberg, pp. 217-223.

[19] Chavda, K. S. and Nimavat, A. V., (2013) "Removal Of Black Hole Attack In Aodv Routing Protocol Of Manet", Proc. IEEE conference on computer networks, Tiruchengode, India, pp. 207-212.

[20] Wang, W., Zeng, G., Yao, J., Hanli, W. and Daizhong, T., (2012) "Towards reliable self-clustering mobile ad hoc networks" International Journal on Computer and Electronics Engineering, Vol. 38, No. 1, pp. 551-562.

[21] Su, M., (2010) "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems" IEEE Conference On Computer Communication.

[22] Kalia, N. and Munjal, K., (2013) "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, No. 3, pp. 529-533.

[23] Abid, S. and Khan, S., (2014) "Improving Performance of Routing Protocols Using MRP Framework" International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.1, pp. 1-8.