International Journal of Engineering & Technology, 7 (1.9) (2018) 6-9

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Securing cluster based routing against cooperative black hole attack in mobile ad hoc network

Pandi Selvam Raman [1] *, Shankar K [2], Ilayaraja M [2]

[1] *Assistant Professor & Head, PG Department of Computer Science, Ananda College, Devakottai, Tamilnadu, India*
[2] *Assistant Professor, School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, India*
**Corresponding author E-mail: pandiselvamraman@gmail.com*

Abstract

Mobile ad hoc networks (MANETs) are wireless infrastructure-less network consisting collection of autonomous nodes that communicate with each other in decentralized manner. Security remains major challenge due to its some unique characteristics like open medium, mobility and hence topology changes. Therefore, routing protocol for MANETs is much vulnerable to attacks. Black Hole is a type of attack, where malicious node falsely advertises itself having the shortest or optimal path to the destination node. This attack is more dangerous while a group of nodes are cooperating with each other. The objective of this paper is to design cluster based routing protocol and prevent it from the black hole attack. The simulation results show improvement in packet delivery ratio and control overhead.

Keywords: *Black Hole Attack; MANETs; Routing and Security.*

1. Introduction

MANETs are collection of mobile nodes constructed in highly dynamic manner without any pre-defined infrastructure. Thus their topology may change rapidly and unpredictably [1]. Nodes may leave or join the network at any point of time due to the absence of central administration. These non-trivial features make MANETs more attentive from vulnerability than the infrastructure or wired network [2]. Black hole Attack [3] is Denial of Service (DoS) attacks where the malicious nodes introduce itself having the shortest path to reach the destination node. Instead of sending the packets to next node on routing path it drops all or partial packets to affect the delivery ratio [4]. Routing is the process of exchanging information between nodes in the network. It broadly divided into Table-Driven (Proactive) and on-Demand (Reactive) based on how the nodes are updating routing information. On the other hand based on route construction routing may be Tree and Mesh [5]. Researchers have proposed a number of routing protocols for mobile ad hoc networks under the above classification [6]. Cluster Based Routing Protocol (CBRP) is a type of reactive routing where the mobile nodes are grouped into several clusters and managed by the cluster heads that are elected based on some criteria to maintain the local information in order to save the energy and bandwidth [7].

A lot of researches are going on the view of vulnerability to secure the routing protocol. Some of these are Intrusion Detection and Authentication techniques. Among various issues, we focused on secure routing in this paper. Several types of attacks are possible while transmission of packets on-demand and black hole attack is one among them. This paper proposed to secure the cluster based routing from black hole attack. This section is the brief introduction of this paper. Section 2 presents the related work of the underlying concept. Section 3 reveals the proposed approach as different phases. Section 4 exposes the experimental results and discussion followed by conclusions and future enhancement in Section 5.

2. Related work

2.1. Routing in MANETs

Routing in MANETs is fully different from traditional routing on wired or infrastructure network. It is very challenging due to the high mobility and frequent disconnections [8]. Many routing schemes are present in mobile ad hoc networks to route the data between nodes. On the basis of route discovery, these are classified into proactive and reactive. In proactive routing, nodes are always maintaining the routing information of the network. As result the network bandwidth continuously consuming to maintain the current routing information. Some example of this type of routing are: Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Fisheye State Routing (FSR), Optimized Link State Routing (OLSR). Reactive routing uses lazy technique, where nodes discover the route only on-demand or when require. Since consume less bandwidth compare to proactive routing protocol. Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA) are the reactive routing protocols.

2.2. Cluster based routing protocol

Mingliang Jiang defined an On-Demand Routing Protocol named as Cluster Based Routing Protocol [9]. The large network divided into several disjoint or overlapping clusters i.e. sub-networks in a distributed manner. Each cluster nodes are named with their current node status i.e. Cluster Head (CH), Cluster Member (CM) or Cluster Gateway (CG).

Cluster Head: A node which is elected based on the connectivity with other clusters and it has the complete knowledge to manage the cluster.

Cluster Gateway: A node which is use to communicate with adjacent cluster. I.e. gateway between the clusters.
Cluster Member: All nodes within the cluster except cluster head. Each member must belong at least one cluster.
In cluster based routing the communication may be done within the same cluster or among the clusters. The source (s) and receiver (s) are in same cluster, cluster head manages the cluster and simply they can share the information. On other hand the communication done through the gateway of each cluster while the source and receivers are in different clusters.

2.3. Black Hole attack in CBRP

Black hole attacks are also called packet drop attack [10] which is more vulnerable to drop the packets by introducing false reply. A single malicious node may participate in the network to tap the packets called single black hole attack. In contrast more than one malicious node are cooperatively work together in order to tap maximum or all packets called cooperative black hole attack. During route discovery process the malicious nodes can take advantage when receives RREQ packet, sends fake RREP packet as having optimal path to the destination. The malicious nodes do not check whether it has the path to destination since the source node receives reply of malicious node. Finally, the malicious nodes tap all or partial data packets and hence diminish the delivery ratio.

2.4. Literature review

Research related to ad hoc networks covers many areas such as designing routing protocol, managing resources like infrastructure and battery, providing robustness, QoS and secure communication. For past decades, researchers are actively involving for secure communication in various directions. This section gives brief discussion of some of the existing approaches that are related to the topic of this paper.
Author in [11] presented a scheme to secure DSR to provide robust routing against black hole attack. This scheme conform the authenticity of node with by verifying the packet. The resulting parameters such as delivery ratio, throughput and control packet overhead are proven the efficiency of the approach.
Author in [12] proposed a secure route discovery mechanism to prevent the black hole attacks by verifying the sequence number in request and reply messages. The simulation results demonstrate the improvement in delivery ratio.
Author in [13] proposed an approach namely coordinate based algorithm to detect the misbehaving nodes while a node move one cluster to another cluster. The results prove that the proposed is effective while varying the mobile nodes.
In our previous work [14] black hole attack are prevented on AODV routing protocol by clustering approach and the results are compared with AODV routing protocol to show the better performance.
Some of the existing approaches consider only single or cooperative attack with two malicious nodes. In addition these approaches increase packet overhead and suffer the delivery ratio. Therefore, these are all substantial factors to decrease the network flexibility.

3. The proposed approach

The proposed approach consists the following phases such as cluster formation, fresh route construction and route maintenance.

3.1. Cluster formation

We proposed a novel algorithm in our previous work [15], called Weight Based Clustering Algorithm (WBCA) to selects the appropriate node as cluster head. The cluster head manage the nearby members and to prevent the flood of unnecessary packets. In this algorithm every node calculates own weight with their neighbors that are within 2-hop connectivity. After the weight calculation is done, each node compares the weight with its neighbors within two hops for cluster head election. The largest weight node will declare it as cluster head and send a HEAD_ANNOUNCE_MSG to the neighbors and acknowledged with receiving JOIN_HEAD_MSG for joining the cluster. The cluster head does not send the HEAD_ANNOUNCE_MSG to the neighbors in the particular time interval then treating that head as a malicious node. In this situation the next largest node will be head of the cluster.

Algorithm: Cluster Formation
Step 1: Deploy mobile nodes in the network
Step 2: Calculate weight of each node
Step 3: Compare the weight with each other
Step 4: Largest node declare itself as CH
Step 5: If CH does not send the *HEAD_ANNOUNCE_MSG* to its neighbors immediately go to Step 6 else go to Step 7
Step 6: The CH treated as malicious and the next largest node will act as CH.
Step 7: If any members does not acknowledge with *JOIN_HEAD_MSG* after receiving *HEAD_ANNOUNCE_MSG* go to Step 7
Step 8: CM treat as malicious node not take part in communication.

3.2. Fresh route construction

Route construction states, connection between all pairs of nodes. The communication in clustered network can be classified into two types. i.e. intra-cluster routing and inter-cluster routing. Intra-cluster routing is the communication of nodes within the same cluster. Therefore, the cluster head only maintains the cluster member information as well as local topology. The inter-cluster routing is responsible when the receiver and the source are in different clusters. In this situation, the gateway of the cluster forward the data packets between clusters. The source node broadcasts RREQ_MSG to the receiver by the cluster member and gateway nodes of each cluster. After receiving RREQ_MSG, the multicast receivers send the RREP_MSG along the same route. Once the RREP_MSG reaches the cluster source, the route connects the source with multicast receiver(s).

Algorithm: Fresh Route Construction
Step 1: Intra-cluster Routing: - Source node simply broadcast *RREQ_MSG* to the receiver(s) due to the local cluster
Step 2: Inter-cluster Routing:- Source node broadcast *RREQ_MSG* to the receiver through the gateway of each cluster
Step 3: Receiver reply *RREP_MSG* along the same route to the source.

3.3. Route maintenance

The route maintenance phase takes care of maintaining the route due to the frequent topological changes as to avoid the link failure and hence packet losses. In our approach every cluster head manage the link states of its cluster by updating the cluster information periodically. I.e. all the cluster members are known with each other by sending hello messages. If anyone of them moves away from its cluster more than 2-hop, that node cannot be a member of the original cluster. This is the method to maintain the local topology changes and to update message to the corresponding cluster head.

Algorithm: Route Maintenance
Step 1: Cluster members are known each other by Simply sending hello messages.
Step 2: If a node moves away from its cluster more Than 2-hop,that node cannot be a member of the cluster.

4. Experimental results and discussion

4.1. Simulation setup

We have simulated the protocol in NS2 2.35 under the Red Hat Linux version 9.0. The simulation composed with 70 nodes that are randomly placed in 500 m x 500 m transmission range within 1000 m x 1000 m area. Each simulation is carried out in 100 sec of simulation time. Nodes depend on random waypoint model and the traffic type is CBR. Each source sends 5 packets/sec and the packet size is 512 bytes.

4.2. Results and discussion

4.2.1. Packet delivery ratio for increasing clusters and malicious nodes

Packet Delivery Ratio (PDR) is the ratio of total number of packets delivered successfully at destination and number of packets sent at the source. The PDR of our proposed routing protocol drawn in Fig.4. for without and with malicious nodes. Drop ratio increases in the presence of malicious nodes as increasing cluster. As a result when there are no malicious nodes that the protocol achieves higher delivery ratio.

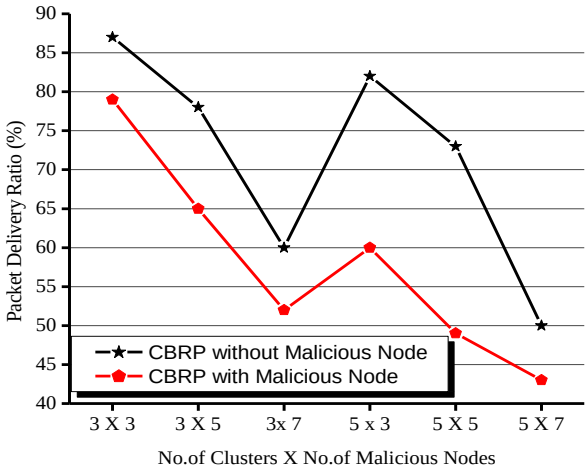

Fig. 4: Packet Delivery Ratio as A Function of Increasing Black Hole Nodes.

4.2.2. Routing overhead for increasing clusters and malicious nodes

Routing Overhead defines the consumed resources in routing process. The better routing protocol overhead must be downward to imply the improved performance. Routing overhead increases when the network malicious nodes are increases as shown in Fig.5. Moreover some additional packets are needed in our approach as to detect the malicious node. However, it is acceptable to provide adequate security feature.

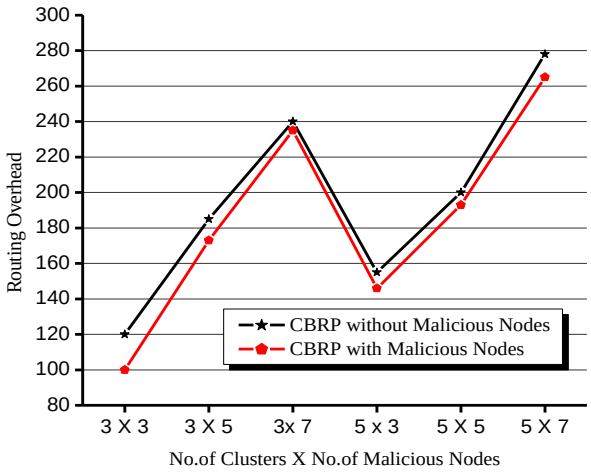

Fig. 5: Routing Overhead as A Function of Increasing Black Hole Nodes.

5. Conclusion and future work

Reactive routing protocols for MANET are best for communication but it is vulnerable to attacks like black hole. The black hole attack drops the packets surreptitiously. This paper secures the CBRP by identifying the malicious nodes that are tried to be act as cluster head or members in the network. The results are shown the protocol performances in terms of Packet Delivery Ratio with bearable overhead against black hole attack. This approach can be extended in future for the group communication i.e. multi-source multicast environment.

References

[1] Ram Ramanathan and Jason Redi, “A Brief Overview of Ad hoc Networks: Challenges and Directions,” IEEE Computer Magazine, pp.20-22, 2002.
[2] Sheltami Tarek, “Ad hoc Network Overview,” http://www.ccse.kfupm.edu.sa/~tarek, Ad hoc network Technology, 2003.
[3] Ranjan, Rakesh, Nirnemesh Kumar Singh, and Ajay Singh, “Security issues of black hole attacks in MANET,” International Conference on Computing, Communication & Automation (ICCCA), IEEE, 2015. https://doi.org/10.1109/CCAA.2015.7148419.
[4] Kishor Jyoti Sarma, Rupam Sharma and Rajdeep Das, “A Survey of Black Hole Attack Detection in MANET,” IEEE, 2014. https://doi.org/10.1109/ICICICT.2014.6781279.
[5] Changling Liu and Jorg Kaiser, “A Survey of Mobile Ad hoc Network Routing Protocols,” Univ. of Ulm, Tech. Rep.Series, 2005.
[6] Krishna Gorantala, “Routing Protocols in Mobile Ad hoc Networks,” M. thesis in Computing Science, Umea University, Sweden, 2006.
[7] S. Kalwar, “Introduction to reactive protocol,” vol. 29, pp. 34-35, IEEE, 2010.
[8] Geetha Jayakumar, and G. Gopinath, “Ad Hoc Mobile Wireless Networks Routing Protocols – A Review,” Journal of Computer Science 3 (8), pp.574-582, 2007. https://doi.org/10.3844/jcssp.2007.574.582.
[9] Mingliang Jiang, Jinyang Li and Y. C. Tay, “Cluster Based Routing Protocol (CBRP),” Internet Draft, draft-ietf-manet-cbrp-spec-01.txt, 1999.
[10] Mohammad Al-Shurman and Seong-Moo Yoo, “Black Hole Attack in Mobile Ad Hoc Networks,” 42nd Annual Southeast Regional conference, pp.96-97, 2004. https://doi.org/10.1145/986537.986560.
[11] Ashutosh Bhardwaj, “Secure Routing in DSR to Mitigate Black Hole Attack,” International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), pp.985-989, IEEE, 2014. https://doi.org/10.1109/ICCICCT.2014.6993102.
[12] Seryvuth Tan and Keecheon Kim, “Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs,” International Conference on High Performance Computing and Communications, pp.1159-1164, IEEE, 2013. https://doi.org/10.1109/HPCC.and.EUC.2013.164.
[13] Bhakti Thakre and S.V.Sonekar, “An Empirical Approach for the Detection of Malicious Node in Cluster Based Adhoc Wireless

Networks," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 3(6), pp.651 – 658, 2014.

[14] Pandi Selvam Raman,"Black Hole Attack Prevention on AODV Routing Protocol using Clustering Approach (CBAODV) in MA-NET," International Journal of Engineering and Technology(IJET), in press. https://doi.org/10.21817/ijet/2017/v9i6/170906306.

[15] R. Pandi Selvam and V.Palanisamy, "An Efficient Cluster-Based Multi-Source Multicast Routing Protocol in Mobile Ad hoc Networks," International Conference on Communication Control and Computing Technologies, pp.700-706, IEEE 2010. https://doi.org/10.1109/ICCCCT.2010.5670749.