Black Hole Attack Prevention on AODV Routing Protocol using Clustering Approach (CBAODV) in MANET

Pandi Selvam Raman
Assistant Professor & Head, Department of Computer Science & IT
Ananda College, Devakottai, Tamilnadu,India
pandiselvamraman@gmail.com

***Abstract*—Mobile ad hoc network (MANETs) is a type of wireless network and that are organized without any predefined infrastructure and centralized administration such as base station or access points. Generally, MANETs nodes can communicate directly if they are in each other transmission range; else the relay nodes are forward the packets to receivers in a multi-hop fashion. Due to some nature of ad hoc networks characteristics such as open medium, infrastructureless and dynamic topology, providing security is particularly difficult than other networks. Black Hole attack is one of the major attack and this detection and prevention is still considered as a challenging task in ad hoc networks. The objective of this paper is to measure black hole attack impacts on AODV routing protocol through clustering approach in MANETs. The performance results of the proposed approach compared with AODV to prove the better performance in terms of delivery ratio, throughput and control overhead.**

***Keywords*—** MANETs, Routing, Security, AODV, Black Hole Attack

I. INTRODUCTION

MANET is a decentralized network where the nodes are dynamically changing their topology rapidly and unpredictably [1]. Hence, nodes can leave and join the network at any time [2]. Routing defines exchanging information from one location to the other locations of the network and it can be broadly classified under the routing information update mechanism (routing scheme) such as Table-Driven(Proactive) and On-Demand(Reactive)Approach and route construction mechanism such as Tree and Mesh [3]. Based on this classification several routing protocols such as AODV,DSDV,DSR and CBRB were proposed by IETF for mobile ad hoc networks [4]. In which Ad hoc On-demand Distance Vector (AODV) is a reactive routing protocol and combine the use of DSDV and DSR. It discovers route only when there is demand from mobile node [5]. Security is a primary concern for all kind of networks. However, MANETs are much attentive against vulnerability because of its non-trivial challenges such as lack of fixed infrastructure, dynamic topology, link variation and energy constraints [6]. So, each and every node in the network has to prepare for attacks at any point of time. And also as there is no central based controlling identity for the participating nodes; the attacks are much easier to launch in MANET. Black hole Attack [7] 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 [8].

A. Goal

In this paper, simulation-based study to be conducted to prove the effect of black hole attack on AODV routing protocol through clustering approach in MANETs. The main reason is to judge the black hole attack is that the DoS. Malicious node detection is done at two levels: Using cluster heads and Using check points to show how the black hole attack affects the network performance.

B. Reading Roadmap

This paper starts with this section, which gives a brief introduction and goal of this paper. Section II presents the survey of the underlying concept of this work. The objective explore as improved model in Section III. Section IV exposes the experimental results and discussion followed by conclusions and future enhancement that are in Section V.

II. LITERATURE SURVEY

Many researchers have provided different solutions to detect and prevent the black hole attack on AODV routing protocol. Few of them have also considered clustering algorithm. In this section, we discuss some of these works.

Ayesha Siddiqua et. al. [9] proposed secure knowledge algorithm to detect and prevent the black hole attack. The authors mainly considered on the view of data delivery to receiver and found the reasons regarding packet drops before declaring a node as a black hole node.

Miss Bhandare A.S. et. al. [10] proposed an approach called detection and defense mechanism against Co-operative Black hole attack. This anti-prevention system checks route reply against fake reply. The significant advantage of this method is that decision about unsafe route is taken independently by source and no any additional overhead required.

Nidhi Choudhary et. al. [11] identified the black hole by maintaining each node with a trust value for its neighbor node. If the trust value decreases the nodes are indexed in the blacklist table.

Ali Dorri et. al. [12] checks the Next_Hop_Node and Previous_Hop_Node of the RREP in order to check the malicious nodes in the path. Data Routing Information table is maintained by the source node to identify the malicious nodes from the network.

Ashish Kumar Jain et. al. [13] modified the AODV routing protocol by ignoring the first RREP packet reaching the source node through RREP caching mechanism.

Anand Aware et. al. [14] proposed a solution to identify the malicious node by using hash function and rejects first RREP from its neighbor and will select the second optimal path.

Kriti Patidar et. al. [15] proposed specification based intrusion detection technique in which every individual node monitor the routing behavior of their neighbors for detecting the malicious node.

Vishvas Kshirsagar et. al. [16] proposed method finds the un-trusted (packet dropper) node from the network, if any un-trusted node found, the performance of the network can be improved by eliminate that node using Bayes' Theorem and Prior probability. This mathematical model secure routing in an independent environment because of it uses heuristic rather than deterministic model.

Gayatri Wahane et. al. [17] detected cooperative Black Hole Attack using Crosschecking with TrueLink (Timing based countermeasure) in AODV. The simulation is conducted to prove the minimum routing overhead, delay and maximum throughput when number of nodes and pause time more.

Dhiraj Nitnaware et. al.[18] proposed DYMO (Dynamic MANET On-Demand Routing protocol) to mitigate the effects of Black hole attack on the performance of DYMO.

III. IMPROVED MODEL (BLACK HOLE ATTACK PREVENTION ON AODV USING CLUSTERING APPROACH)

The process of improved model can be visualized with two objectives. The primary aim is to design a stable and flexible clustering algorithm namely Weight Based Clustering Algorithm (WBCA) to elect the appropriate node as cluster head and to manage the nearby members. The secondary aim is to find the malicious node in the formatted clusters.

A. Cluster Formation

Cluster is a subset of nodes in a network. Clustering is a process of dividing the network into disjoint or overlapping clusters. Weight Based Clustering Algorithm (WBCA) is proposed to selects the appropriate node as cluster head to manage the nearby members and to prevent the flood of unnecessary packets. In this algorithm, the maximum hop distance from the cluster head to its farthest cluster member is two hops. Each non-cluster head node is managed by only one cluster head which is one of its neighbors within the two hops. For weight calculation, the weight function $w(p)$ is defined to calculate the weight of each node p as follows

$$w(p) = x \times a(p) + y \times b(p) + z \times c(p)$$

Where, $a(p)$ number of member nodes in one-hop, $b(p)$ number of member nodes in two-hop and $c(p)$ number of cluster member nodes within two-hops. According that, the values are assigned as $x = 3$, $y = 2$ and $z = 1$. 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 itself as cluster head. The cluster head send *HEAD_ANNOUNCE_MSG* to the neighbors and acknowledged with receiving *JOIN_HEAD_MSG* for joining the cluster.

B. Malicious Nodes Detection

The methodology of malicious nodes detections are done at two levels. These are.

- *Malicious nodes detection using Cluster Head:* After receiving *HEAD_ANNOUNCE_MSG* from the cluster head, if any member does not acknowledge with *JOIN_HEAD_MSG* it will treated as a black hole.
- *Malicious nodes detection using check points:* The cluster head does not send the *HEAD_ANNOUNCE_MSG* to the neighbors in the particular time interval *t* then treating that head as a malicious node. In this situation the next largest node will act as CH. These two levels are detects all the cooperative malicious nodes that are try to drop the packet in the network.

Algorithm:

Step 1: Deploy mobile nodes in the network

Step 2: Format the network into different cluster using WBCA

Step 3: Identify the cluster heads

Step 4: Assign check points for each cluster

Step 5: Introduce cooperative black hole in networks

Step 6: Level 1: Detection of black hole nodes using cluster head

Nodes acknowledge with *JOIN_HEAD_MSG* with CH. If yes go to Step 7 Else go to Step 8

Step 7: Level 2: Detection of black hole using check points

CH sends the *HEAD_ANNOUNCE_MSG* to the neighbours in the particular time interval *t*.

If yes go to Step 10 Else go to Step 9

Step 8: Assign node as malicious node and thus node not take part in communication

Step 9: Assign the CH as malicious node and go to Step 3

Step 10: Continue packet forwarding till destination is reached.

Step 11: End of the Algorithm.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. Simulation Setup

To analyze the performance, several simulations are run in NS2 version ns-allinone-2.26 under the Red Hat Linux version 9.0 operating system. The simulation composed with 100 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. 20 simulation runs are conducted for each scenario. 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.

B. Results and Discussion

Initially, both AODV and CBAODV routing protocol performance results are compared with no black hole nodes. As a result we observe that, under normal situation both performances are almost same in all situations.

1) *Packet Delivery Ratio Vs No.of Black Hole Nodes:* Packet Delivery Ratio (PDR) is the ratio of the number of delivered to the receivers and number of packet to be received by the receivers. The PDR of CBAODV protocol is compared with AODV protocol as depicted in Fig.1. When the protocols black hole nodes are increasing the CBAODV achieves better delivery ratio as compared to AODV.

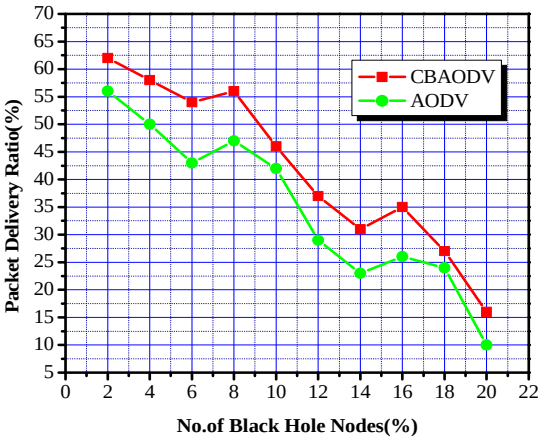

Fig.1. Packet Delivery Ratio as a function of increasing Black Hole Nodes

2) *Throughput Vs No.of Black Hole Nodes:* Throughput defines successful data transmission performed with in a time period and which is normally represented in bytes or bits per second. Throughput of the network is decreases while introducing a node to be black hole node. Although, Fig.2. shows that CBAODV better performances rather than AODV in presence of black hole nodes.

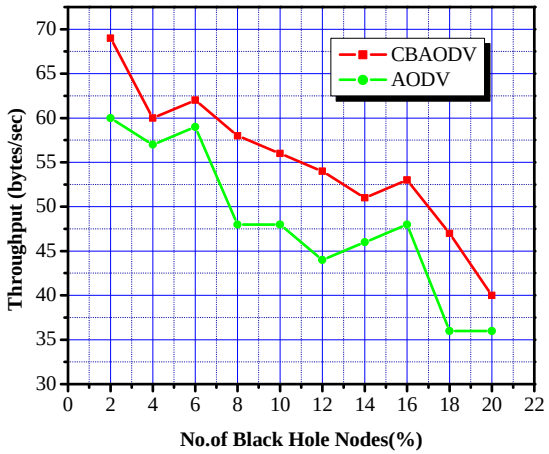

Fig.2. Throughput as a function of increasing Black Hole Nodes

3) *Routing Overhead Vs No.of Black Hole Nodes:* Routing Overhead describes consumed resources in routing process. The better routing protocol overhead must be downward to imply the improved performance. This metric totally depends upon the random topology of the network. We found in Fig.3. that the routing overhead of CBAODV is slightly more as compared to AODV due to the cluster formation. Although, this overhead is acceptable due to it's providing healthier and more affluent delivery ratio.

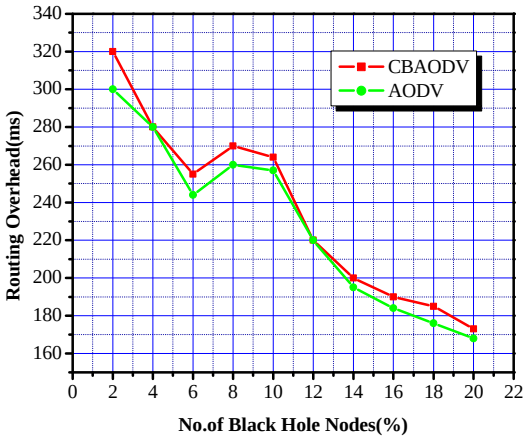

Fig.3. Routing Overhead as a function of increasing Black Hole Nodes

V. CONCLUSION AND FUTURE WORK

AODV routing protocol is one of the best reactive routing protocol for MANET but it is vulnerable to attacks, the major one is black hole attack. The black hole can drop the packets surreptitiously. The paper presents to prevent the AODV routing protocol black holes through Cluster Based Approach. The basic idea behind this approach is formatting the network nodes into clusters to prevent the impact of Black Hole attack regarding performance improvement of the network. The simulation results reveal that the proposed approach better performances in terms of Packet Delivery Ratio, Throughput and Routing Overhead. As a future work, it may extend to identify the attack positions: Malicious nodes are near sender, near receiver or anywhere within the network.

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] Changling Liu and Jorg Kaiser, "A Survey of Mobile Ad hoc Network Routing Protocols," Univ. of Ulm, Tech. Rep.Series, 2005.
[4] Krishna Gorantala, "Routing Protocols in Mobile Ad hoc Networks," M. thesis in Computing Science, Umea University, Sweden, 2006.
[5] Geetha Jayakumar, and G. Gopinath, "Ad Hoc Mobile Wireless Networks Routing Protocols – A Review," Journal of Computer Science 3 (8), pp.574-582, 2007.
[6] S. Kalwar, "Introduction to reactive protocol," IEEE, vol. 29, pp. 34-35, 2010.
[7] 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.
[8] Kishor Jyoti Sarma, Rupam Sharma and Rajdeep Das, "A Survey of Black Hole Attack Detection in MANET," IEEE, 2014.
[9] Ayesha Siddiqua, Kotari Sridevi, and Arshad Ahmad Khan Mohammed, "Preventing black hole attacks in MANETs using secure knowledge algorithm," International Conference on Signal Processing and Communication Engineering Systems (SPACES), IEEE, 2015.
[10] Miss Bhandare A. S., and S. B. Patil, "Securing MANET against Co-operative Black Hole Attack and its Performance Analysis-A Case Study," International Conference on Computing Communication Control and Automation (ICCUBEA), IEEE, 2015.
[11] Nidhi Choudhary, and Lokesh Tharani, "Preventing black hole attack in AODV using timer-based detection mechanism," International conference on Signal processing and communication engineering systems (SPACES), IEEE, 2015.
[12] Ali Dorri and Hamed Nikdel, "A new approach for detecting and eliminating cooperative black hole nodes in MANET," 7th Conference on Information and Knowledge Technology (IKT), IEEE, 2015.
[13] Ashish Kumar Jain and Vrinda Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile Ad hoc Networks," International conference on Pervasive computing (ICPC), IEEE, 2015.
[14] Anand A.Aware and Kiran Bhandari "Prevention of Black hole Attack on AODV in MANET using hash function," 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), IEEE, 2014.
[15] Kriti Patidar and Vandana Dubey "Modification in routing mechanism of AODV for defending blackhole and wormhole attacks" 2014 Conference on IT in Business, Industry and Government (CSIBIG), IEEE, 2014.
[16] Vishvas Kshirsagar, Ashok M. Kanthe, and Dina Simunic "Analytical approach towards packet drop attacks in mobile ad-hoc networks," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), IEEE, 2014.
[17] Gayatri Wahane, Ashok M. Kanthe, and Dina Simunic, "Detection of cooperative black hole attack using crosschecking with truelink in MANET," International Conference on. Computational Intelligence and Computing Research (ICCIC), IEEE, 2014.
[18] Dhiraj Nitnaware and Anita Thakur, "Black Hole Attack Detection and Prevention Strategy in DYMO for MANET," International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, 2016.

AUTHOR PROFILE

Pandi Selvam Raman working as Assistant Professor & Head of Department of Computer Science & IT, Ananda College,Devakottai,Tamilnadu. He has received M.Sc., M.Phil., and Ph.D. Degrees from Alagappa University in 2007,2008 and 2015 respectively. He has published over 12 International Journals (including IEEE & ACM) and presented papers in 20 International/National conferences in various areas. His research interest includes mobile computing, ad hoc wireless networks & security and computer algorithms.