International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Random ID based Secure AODV to prevent Black Hole Attack in MANET

S. Sundar, Harish M.Kittur

Abstract*: Mobile Ad Hoc Networks (MANET) are typically wireless networks that do not have any fixed network architecture. This makes the task of routing layers difficult. A popular reactive routing protocol – Ad hoc On-demand Distance Vector (AODV) used in MANETs has certain vulnerabilities which make it susceptible to black hole attacks. This paper proposes an innovative technique to detect and prevent the possibility of a black hole attack in AODV based MANETs. Using the approach of detecting multiple Route Reply (RREP) messages, authentication of nodes is done by the use of a randomly generated id unique to each route discovery process. This method was tested using simulations in NS2 software and compared with previous attempts. The proposed method showed marked improvement in performance in the presence of malicious nodes.

***Keywords* : AODV, black-hole, MANET**

I. INTRODUCTION

The growing need for connectivity is putting a lot of pressure on establishing mobile networks efficiently and quickly. This makes Mobile Ad- hoc Networks (MANETs) the perfect candidate. MANETs are typically wireless networks that do not have any fixed network architecture. There are two reasons for this. Firstly, the nodes are wireless and mobile so their position is not fixed relative to each other. They cannot be arranged to form a ring network or star network like wired nodes. Secondly, the networks are ad-hoc. They have to be set up within short time and are usually temporary in nature. So it is not feasible to create a central base station which would communicate with other nodes similar to a client server architecture. Hence, MANETs usually have peer to peer networks. In such peer to peer networks, all nodes are of equal status and they share the responsibility of maintaining the connection and providing security. Under such circumstances, implementing certain network functions such as finding the shortest path for communication and dealing with the changes in location of the nodes becomes challenging as there is no central node keeping track of it. Several routing protocols for such situations have been developed. They are of two types – Table Driven (proactive) and On-demand (reactive).

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
S.Sundar*, Department of Embedded Technology, School of ElectronicsEngineering, VIT, Vellore, India. Email: sundar.s@vit.ac.in
Harish M.Kittur, Department of Micro and Nano-electronics, School of ElectronicsEngineering, VIT, Vellore, India.. Email: kittur@vit.ac.in

Proactive protocols are based on maintaining a record of neighboring nodes, routes and clusters and updating them periodically. This often requires large memory and is energy hungry. Reactive protocols on the other hand find routes only at the time when communication is required. Requests are flooded, replies are awaited and paths are established on demand. One such protocol which is popular among ad-hoc wireless networks is the Ad-hoc On demand Distance Vector (AODV) routing protocol. The AODV algorithm enables self-starting, dynamic, multi-hop routing between participating mobile nodes wanting to establish and maintain an ad hoc network. AODV allows mobile nodes to get routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. Sequence numbers, which is one of the key features of AODV, acts as a time stamp and ensures the freshness of routes. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.

II. NEED FOR SECURITY IN MANET - BLACK HOLE ATTACK

Routing protocols are quite efficient but are often vulnerable to impersonation attacks. Due to this reason, control messages such as Route Requests (RREQ) and Route Reply (RREP) need to be authenticated. When there is no authentication, a malicious node, if present in the network, can interfere in the route discovery process and potentially disrupt communication in the network. A typical example of such an attack is the black hole attack.

In a black hole attack, a malicious node listens for RREQ messages. Upon receiving one, it unicasts a fraudulent reply message as soon as possible which makes it appear as shortest route to the required destination. If this reply reaches the source before the actual honest reply, the source will be tricked into believing the fraudulent reply as it will ignore the honest reply or any subsequent reply for that matter. Once the malicious node establishes itself in the path, it will have access to all data packets in that path. Under such circumstances it may eavesdrop, corrupt data or at the very least, in case the data is encrypted, it can simply drop the packets. Since this malicious node can potentially suck all packets to itself and subsequently drop them, it is called black hole attack.

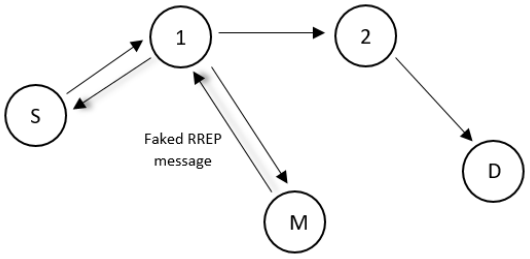

Fig. 1.Route discovery process in the presence of malicious node.

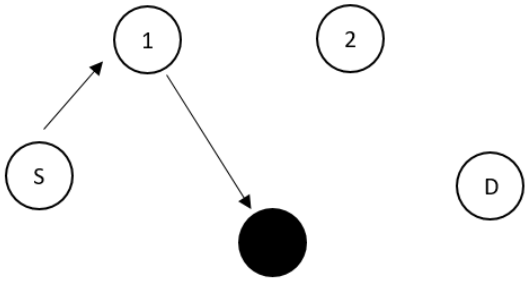

Fig. 2. Data packets getting lost into malicious node after successful black hole attack.

For example, when the node S wants to communicate with node D in Fig. 1 it sends out a request which also reaches the malicious node M through node 1 due to flooding. Upon receiving the request, M immediately sends a fake reply which reaches the source before any other reply. The source thinks the shortest path to D is through 1 and M and this path gets established. As a result all data packets are sent to M which does not forward them as shown in Fig 2. Thus M has attacked the network as a black hole.

III. LITERATURE REVIEW

Several methods and ways have been suggested in the past in order to secure the process of route discovery in AODV based networks. These can be broadly classified into the following approaches or categories.

A. Encryption

Message authentication codes have been used in order to prevent various impersonation attacks [1]. The keys were pre-distributed and not during run time so that overheads are minimized. Routing protocols suggested in [2]-[3] try to secure the route based on Public Key Infrastructure (PKI) and hence the network has to rely on a third party for authentication. The problem with such techniques is that they produce large computational overheads, the processing power for which, may not be easily available all the time.

B. Thresholding Sequence Numbers

The source node and the destination node check the sequence numbers in the RREQ and RREP messages and then, depending on certain defined thresholds, decide whether or not to establish a connection with a destination node for sending data [4]. However, the method may fail if malicious nodes use sequence numbers below the thresholds.

C. Behavior monitoring

A secure knowledge algorithm is proposed which tries to detect and prevent a black hole attack by examining the reasons for packet drop in promiscuous mode [5]. As per the mechanism in [6], parameters like stability of a node defined by its mobility and pause time, remaining battery power etc. are used to determine the trust of every node in the network. This determines the selection of the most reliable route for communication. In case of a malicious node, the ratio of number of RREQs sent to the number of RREPs sent is very low [7]. A modified algorithm utilizes this fact to look for a black hole attack. Two additional fields are used namely request weight and reply weight. Request weight in routing table indicates the number of RREQs that are forwarded by the corresponding node. Similarly Reply weight indicates the number of RREPs forwarded. The method has two processes updating request/reply weights and collecting feedback. An algorithm in which nodes directly measure their neighbor's delivery ratios instead of advertising that of their own [8]. The solution given in [9] was one of the earliest to propose a method for identifying multiple black hole nodes. They introduced a Data Routing Information (DRI) table and a mechanism for cross checking. In all the methods of this category, if a large number of nodes are present, more memory is required to keep database of packet drop reasons; mobility, pause time, etc.; RREQ and RREP ratio; delivery ratios or DRI table.

D. Detecting Multiple RREP

A defense mechanism makes use of the Machine Access Code (MAC) address of the destination to validate each node in its path thereby providing a direct negotiation for secure route [10]. The RREP message in normal AODV is modified to include the unique ID of the destination itself to find the Black Hole node RREP and this is termed the Modified RREP (MRREP). Hashing of this MRREP is done to enhance security. The source is configured to accept many MRREP messages and store them into a table. The Black hole node can be easily found out using comparison method. The proposed solution in [11] is to ignore the first RREP packet reaching the source node. To implement this solution, there is a provision to count the RREP packet messages by implementing RREP packet caching mechanism. The malicious node can store the hashed MAC address of destination node and use it in future route discovery processes [10]. If only one route exists then it will be ignored [11].

Among the various approaches mentioned above, the technique of analyzing multiple RREP messages before finalizing the path provides scalability, little computation as well as memory overhead. The main vulnerability of the protocols previously suggested in this category is the event of a malicious node accessing and storing information in messages that are not meant for it and using it in

IV. RANDOM ID BASED SECURE AODV (RISAODV)

As concluded in the previous section, the approach of detecting multiple RREP messages is a promising one provided there is some safeguard to nodes from maliciously using the information present in messages that are not meant for them in spite of the messages being accessible to them. This happens typically in the case of unicasting in wireless networks.

When a node wishes to unicast a message to a specific node in range, all other nodes in that range also hear it even though it is not meant for them. It is this phenomenon that malicious nodes can exploit in [10] where the messages are authenticated using MAC id. Any malicious node in range of the destination node can listen to the RREP and learn the MAC id. It is not feasible to set up an encrypted communication each time just for the purpose of sending routing messages as it would consume a lot of time and make any communication impractical. Therefore, an innovative solution – RISAODV has been suggested in this paper by which nodes can detect presence of malicious nodes without having to encrypt routing messages. In this method, a randomly generated id is used instead of the MAC id as proposed in [10].

In RISAODV, a randomly generated Id is used to ensure security during each communication session. Whenever a route discovery takes place, the source broadcasts a RREQ message. When the RREQ eventually reaches the destination, it must send a RREP message. The proposed method - RISAODV, requires that the destination node append an additional field in the RREP containing a randomly generated number of sufficient size such as a 32 bit unsigned integer as shown in Fig. 3.

There shall be a unique random number for each route discovery process. The source node waits for a reply for a fixed time period after sending a request. During the wait, if the source receives a reply, RISAODV requires the source node to start a timer during which it shall listen for other replies. The timer value maybe adjusted according to the scale of the network. All replies are stored in table called the Reply Buffer Table (RBT).

RREP fields
Reply Destination
Reply Destination Sequence Number
Hop Count
Reply Source
Random Id (additional field)

Fig. 3. Important fields in RREP. (Note: RREP messages contain some more fields apart from those shown in figure).

Once the timer expires, the replies are processed to detect the presence of any malicious nodes and subsequently select the safest and most eligible reply. The steps to be followed while processing are given below.

Step 1: Count the number of replies received and let it be denoted by NREP.

Step 2: If NREP > 1, go to Step 4. Otherwise, go to next step.

Step 3: No malicious node is present. The only reply received is selected. Process ends.

Step 4: The random Id of the replies are analysed to see how many different sets of random Id(s) have been received. There may be more than one reply having the same random Id. These correspond to the same reply reaching the source through different paths.

Step 5: Count the number of different random Id sets let it be denoted by NRSET.

Step 6: If NRSET > 1, go to Step 8. Otherwise, go to next step.

Step 7: No malicious node present. The reply with least hop count is selected. Process ends.

Step 8: The set of replies with lowest sequence number is selected. Among them, the reply with least hop count is selected. Process ends.

Since every route discovery has a new unique random ID, intermediate nodes are not allowed to reply when they receive a request even though they may know a valid route to the destination. Also, intermediate nodes must forward all replies of the same route discovery process unless the reply has a sequence number that lies outside a certain range. The range can be set according to the network scale and performance.

V. SIMULATION RESULTS

The proposed method – RISAODV was simulated using the software Network Simulator 2 or NS2. NS2 is an open source software, a discreet event simulator that is widely used for wired and wireless network research.

For this paper, NS2 was used to simulate a MANET. A total of 50 mobile nodes were used out of which 2 were made to act maliciously. The simulation time was 100 seconds and a 2 dimensional topography of 800 square units was configured. The nodes were configured to generate User Datagram Protocol (UDP) traffic randomly and their movements were assigned using random waypoint model. The parameters measured include Packet Delivery Ratio (PDR) and throughput for varying mobility of nodes and varying pause time. The performance is compared among multiple different scenarios namely –

- Simple AODV based MANET without any malicious nodes present – normal
- AODV network with presence of malicious node - AODV with black hole
- Secure AODV as proposed in [10] based on MAC id authentication in presence of malicious node – MAC AODV
- Proposed Random ID based Secure AODV – RISAODV

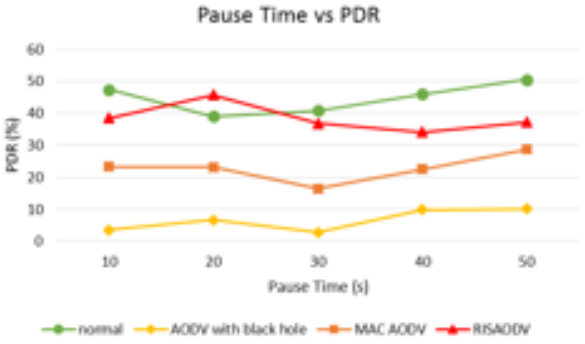

Fig. 4. Pause Time vs PDR.

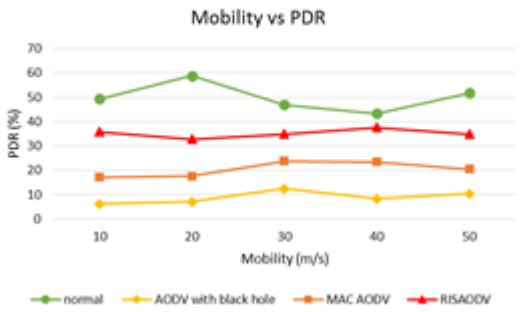

Fig. 5. Mobility vs PDR

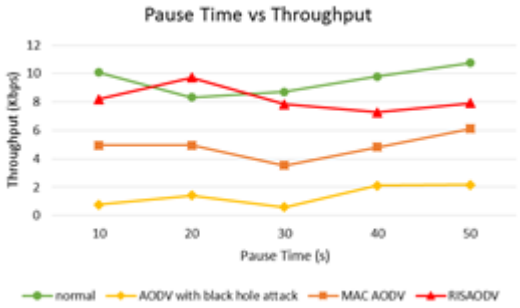

Fig. 6 Pause Time vs Throughput

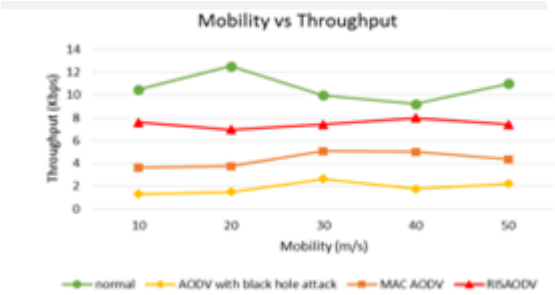

Fig. 7 Mobility vs Throughput

It can be observed from Fig. 4 through Fig. 8, that the performance is best when there are no malicious nodes (normal scenario). However, this may not always be the case. When malicious nodes are present they are able to easily attack the network and severely affect the performance. This is evident from the scenario of 'AODV with black hole attack' which showed worst performance in all four figures. When 'MAC AODV' scenario is followed, there is a small improvement in performance due to some level of authentication provided by MAC ID verification. However, it is much lower than the normal scenario. RISAODV provides best performance in presence of malicious nodes and is quite close to the normal scenario. This is because RISAODV uses unique random id for each route discovery and hence malicious nodes are not able to use that information for impersonation and black hole attack.

It must however, be noted that the idea of using random id instead of MAC id for authentication proves fruitful only under the circumstance where communication happens between the same source and same destination more than once with a small time interval in between. Also, this method provides security specifically against black hole attacks. The network may still be vulnerable to other attacks such as worm-hole attacks.

VI. CONCLUSION

This paper proposes an innovative technique to detect and prevent the possibility of a black hole attack in AODV based MANETs. Using the approach of detecting multiple RREP, authentication of nodes is done by the use of a randomly generated id unique to each route discovery process. This method was tested using simulations in NS2 software and compared with previous attempts. The proposed method showed marked improvement in performance in the presence of malicious nodes.

REFERENCES

1. K. V. Arya and Shyam Singh Rajput, "Securing AODV Routing Protocol in MANET using NMAC with HBKS Technique," *International Conference on Signal Processing and Integrated Networks* (SPIN), Feb. 20-21, 2014, pp. 281-285.
2. A.Rajaram and Dr. S. Palaniswami,"Malicious Node Detection System for Mobile Ad hoc Networks," *International Journal of Computer Science and Information Technologies*, vol. 1, no. 2 , 2010, pp. 77-85.
3. Y.-C. Hu, D. B. Johnson, and A. Perrig, "Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," *The 4th IEEE Wksp. Mobile Computing Systems and Applications (WMCSA'02)*, June 20-21, 2002, pp. 3-13.
4. Seryvuth Tan and Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs," *IEEE International Conference on Embedded and Ubiquitous Computing*, Nov. 13-15, 2013, pp. 1159-1164.
5. Ayesha Siddiqua, K.Sridevi,and A.A.K.Mohammed, "Preventing black hole attacks in MANETs using secure knowledge algorithm," *International Conference on Signal Processing And Communication Engineering Systems (SPACES)*, Jan. 2-3, 2015, pp. 421-425.
6. Suparna Biswas, Tanumoy Nag and Sarmistha Neogy ,"Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET Sign In or Purchase," *Applications and Innovations in Mobile Computing (AIMoC)*, Feb. 27-31, 2014, pp. 157-164.
7. Rajesh Yerneni and Anil K. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc," *Third International Conference on Computing Communication Networking Technologies* (ICCCNT), July 26-28, 2012, pp. 1-5.
8. Kitisak Osthanunkal and Ning Zhang, "A Countermeasure to Black Hole Attacks in Mobile AdHoc Networks," *International conference on Networking, Sensing and control Delft*, Netherlands, April 11-13, 2011, pp. 508-513.
9. Sanjay Ramaswamy et al., "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," *International Conference on Wireless Networks* (ICWN), Las Vegas, Nevada, USA, 2003.
10. S.Sankara Narayanan and Dr.S.Radhakrishnan, " Secure AODV to Combat Black Hole Attack in MANET," *International Conference on Recent Trends in Information Technology* (ICRTIT), July 25-27, 2013, pp. 447-452.
11. 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), Jan. 8-10, 2015, pp. 1-6.

AUTHORS PROFILE

S. Sundar received his Bachelor's degree from Madras University in 1997, the Master's degree from Anna University and PhD from VIT Vellore, Tamilnadu, India. He is currently working as an Assistant Professor (Selection Grade) at the School of Electronics Engineering in VIT Vellore. He has authored many technical papers in journals. His research interest includes mobile ad hoc and wireless sensor networks

Harish Mallikarjun Kittur, received his BSc in Physics, Mathematics, and Electronics from the Karnataka University, Dharwad, India, in 1994; the MSc in Physics from the Indian Institute of Technology, Mumbai, India, in the year 1996; the MTech in Solid State Technology from the Indian Institute of Technology, Madras, India, in the year 1999, and the PhD in Physics from the RWTH Aachen, Aachen, Germany, in 2004. He has over 10 years of experience in research and teaching and is currently a Professor, Department of Micro and Nano-electronics, School of Electronics Engineering, VIT, Vellore, India.