Fuzzy Systems and Soft Computing
ISSN : 1819-4362

Detecting network layer attacks in MANETs using the AODV protocol

Biswajit Pradhan[1],Ranjan Kumar Samantaray[2]
Raajdhani Engineering College, Bhubaneswar,
[1]biswajitpradhan@rec.ac.in
[2]ranjankumarsamantaray@rec.ac.in

Abstract

The emergence of Mobile Ad hoc Networks (MANETs) presents a crucial concern within autonomous systems, characterized by mobile hosts establishing temporary networks devoid of fixed infrastructure. Lacking inherent self-defense mechanisms, MANETs are vulnerable to intrusion by potential attackers. This paper conducts a comprehensive examination of a primary category of network layer attacks, posing significant threats to ad hoc network security. Additionally, it outlines defensive techniques that can be employed to mitigate these threats

.***Keywords:*** *AODV, Attacks, Mobile Ad hoc Networks (MANET), RREP, RREQ.*

1. Introduction

A Mobile Ad hoc Network is a gathering of wireless nodes that are capable of communicating with each other without the need of fixed infrastructure. MANET is an autonomous system in which mobile host moves in a free and random manner. MANETs have some special features such as unreliable wireless media (links) used for communication betweenhosts, constantly varying network topologies and memberships, inadequate battery, lifetime, bandwidth and computation power of nodes etc. MANETs are susceptible to various types of attacks [1] [5].

A Mobile Ad hoc network is a collection of mobile hosts that roams and communicates with each other. MANET has Multi-hop commutation capability. There is no centralized administration or a backbone network to maintain it. In these types of networks each node works independent router. Each host uses wireless transceivers as network interface. Example

Applications of MANET are emergency search-and-rescue operations, meetings where users need to set up networks immediately without base stations or fixed network infrastructure [2]. Mobile ad-hoc networks are self organizing. They are fully decentralized means there is no central server exists in MANET environment. It is highly dynamic because topology of MANET changes rapidly. It has inadequate physical security as the broadcast nature of MANET lends itself to passive eavesdropping attacks without malicious nodes being detected. There are potentially repeated network partitions. This might imply that no path exists between nodes as the intermediate routing stations have moved too far apart [7].

2. Types of security Attacks

The Security attacks in MANET can be classified into two major categories.

2.1 Passive Attacks

The Passive Attack does not disturb the normal operation of the network, the attacker detect the data exchanged in the network without altering it. This intermediate attacker is also doing the task of network monitoring to examine which type of communication is going on [10]. Here the necessity of confidentiality gets violated. Detection of Passive attack is very complicated since the operation of the network itself does not get effected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thus making it impossible for the attacker to get valuable information from the data overhead.

2.2 Active Attacks

An Active Attack attempts to modify or destroy the data being exchanged in the network there by disturbing the ordinary functioning of the network. Active attacks are of two types: Internal or External. External attacks are accepted by nodes that do not belong to the network. Internal attacks are from those nodes that are part of the network. Since the attacker is previously part of the network, internal attacks are more rigorous and hard to detect than external attacks. In this paper we are discussing only active network layer attacks [9].

3. PROTOCOL used for MANET: AODV Overview

AODV (Ad hoc on Demand Distance Vector) is a reactive routing protocol in which the network generates routes at the start of communication. Each node has its own sequence number and this number increases when links adjust. Each node judges whether the channel information is new according to sequence numbers. Fig 1 illustrates the Route finding process in AODV. In this figure, node S is trying to establish a connection to destination D. In case where there is no routeto destination D, it sends Route Request (RREQ) message using broadcasting. RREQ SEQ_NO increases one every time node S sends a RREQ. Node M and N which have received RREQ create and repair the route to its previous hop. They also examine if this is a repeated RREQ. If such RREQ is received, it will be discarded. If M and N has a valid route to the destination D, they send a RREP message to node S. In case where the node has no valid route, they send a RREQ using broadcasting. The interchange of route information will be repeated until a RREQ reaches at node D. When node D accepted the RREQ, it sends a RREP to node S. When node S receives the RREP, then a route is recognized. In case a node receives multiple RREPs, it will select a RREP who's the destination sequence number (DEST SEQ) is the largest amongst all previously received RREPs. But if DEST SEQ were same, it will select the RREP whose hop count is least [3].

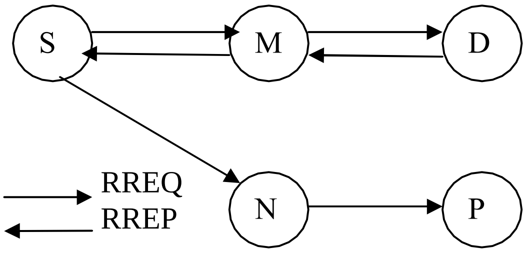

Fig 1: Route finding process

4. Network Layer Attacks

4.1 Black Hole Attack

In Black Hole Attack malicious nodes never send true control messages in the beginning. To carry out a black hole attack malicious node waits for neighboring nodes to send RREQ messages.When the black hole node receives an RREQ message, without checking its routing table,instantaneously sends a false RREP message giving a route to destination over itself, conveying a high sequence number to resolve in the routing table of the sufferer node, before other nodes send a true one.

Therefore requesting nodes presume that route finding process is completed and ignore other RREP messages and begin to send packets over malicious node. Black hole node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a spot when they are not forwarding anywhere.

This is called a black hole similar to realmeaning which swallows all objects and matter.To succeed a black hole attack, malicious node should be placed at the centre of the wireless network. If malicious node masquerades false RREP message as if it comes from another sufferer node instead of itself, all messages will be forwarded to the sufferer node. By doing this, sufferer node will have to process all incoming messages and is subjected to a sleep deprivation attack [1].

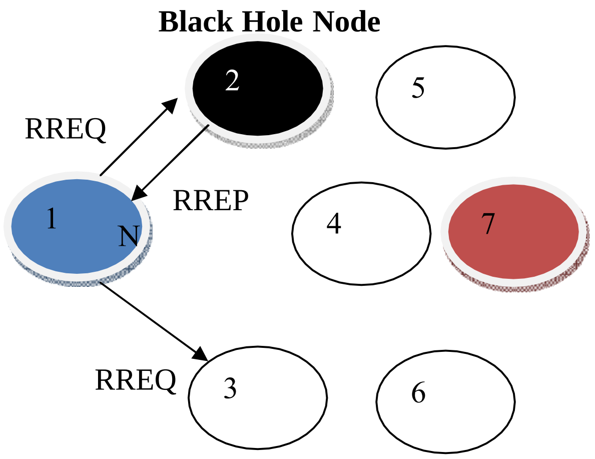

Fig 2: Black Hole Attack Scenario

In this Fig 2, we assume that Node 2 is the malicious node (Black Hole Node). Here shows node 1 as a sender node broadcast the route request packet to all radio range nearest neighbor, here node 2 malicious node certainly respond route reply packet to sender node 1 with maximum sequence number that means node 1(sender node) assume this sequence number sends by the Receiver node number 7, and sender node 1 sends data packets (UDP, TCP) for node 7 (receiving node) but middle node 2 (gray hole node) capture all the UDP data packet , and can't sends TCP ACK to sender node so that TCP has Block via the Black Hole Node 2 [1].

Detection of Black Hole Attack:

The work includes the fuzzy approach to prevent the Black hole attack in a wireless network. In this work each node is defined as an intelligent node that will keep the information about the neighboring nodes and perform the decision making based on statistical information of neighboring nodes. The basic decision taken here is on the basis of driven throughput and response time. As the node reply it Check if the response time is Greater than its estimated time then it will exclude the particular node from the list. The complete process is repeated node by node till the destination is achieved. Fuzzy Logic provides simple way to arrive at exact conclusion based upon vague, ambiguous, impressive or missing information [2].

Algorithm:

```
1. Define the network with N nodes with random topology and communication parameters.
2. Define the Source node Si and Destination node Di.
3. As transmission begins it will search for all intermediate node s and send data to it. Let the path is Si, N1, N2, N3...Nn, Di.
4. For i=1 to n [Repeat steps 5 to 10]
5. NList=FindNeighbour(i)
6. for j-1 to Length(Nlist)
{
7. Parameter1=Throughput(j)
   Parameter2=PacketDelay(j)
8. Fuzzify the Parameters
9. If (High (Parameter1) and Low(Parameter 2))
{The Attacker node is detected. Update Neighbor node Table & Routing Table for theintermediate node }
10. Move to next node
```

4.2 Wormhole Attack

A Wormhole attack requires two or more attackers-malicious nodes. The attacker creates low latency link (i.e. high bandwidth tunnel) between two or more attackers in the network. Attackers support these tunnels as high quality routes to the base stations. Hence neighboring nodes adopt these tunnels into their communication path, rendering their data. Once the tunnel is recognized, the attackers collect data packets on one end of the tunnel, send them using the tunnel and replay them at the other end [4] [11].

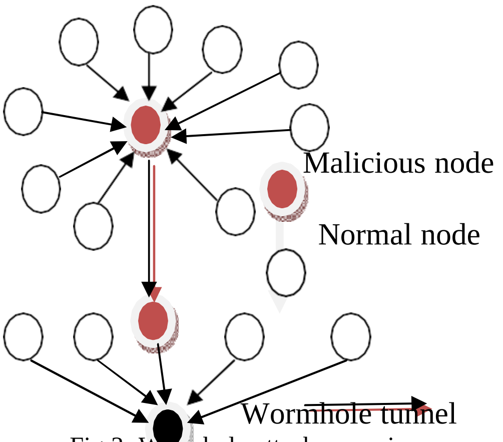

Fig 3: Wormhole attack scenario

Impact of Wormhole attack:

To show the impact of wormhole attacks, there are simulated arbitrarily distributed nodes in a rectangular region and used the shortest path algorithm to find the best route between any node pairs. If a wormhole is formed, some node pairs may find shortest path through the wormhole. In the first experiment, the base station is at the corner, on wormhole endpoint is near the base station and the other end point moves diagonally across the network. In the second experiment, base station is at the center, one wormhole end point is near the base station and another end point moves across the network. We are concerned in how many routing paths are affected by the single wormhole? [8]

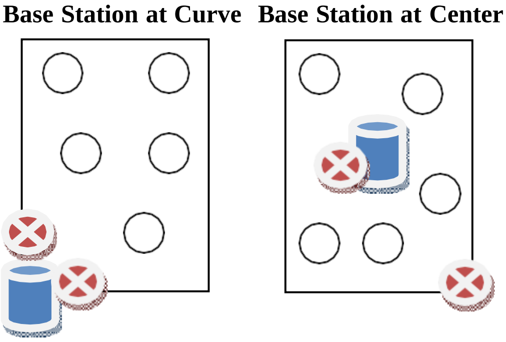

Fig 4: Impact of wormhole Experiment

If the base station is at curve, a single wormhole will be able to attract 30% of the traffic. When the base station is at corner, a wormhole withone endpoint near the base station and the other endpoint one hop away will be able to attract all the traffic. This indicates that single wormhole can greatly influence the performance of the network [8].

Modes of Wormhole:

The Wormhole Attack can be launched in two different modes.

1. Hidden mode: In this mode the attackers do not use their identities so they remain unseen from the legitimate nodes. The attackers act as two simple transceivers which capture messages at one end of the wormhole and replicate them at other end. In this way they can make a virtual link between two nodes. Clearly the attackers require no cryptographic techniques keys to launch the wormhole attack in hidden mode.
2. Participation mode: The attacker can launch a more powerful attack by using valid cryptographic keys. In this mode the attacker makes no virtual links between the legitimate nodes. In fact they participate in the routing as legitimate nodes and used the wormhole to deliver the packets with smaller number of hops [12].

Detection of Wormhole Attack using encapsulation:

Fig 5 presents an example of encapsulation based attack. Consider node S (Source) and D (Destination) try to determine shortest path between each other, in the presence of two malicious nodes M1 and M2. Node S broadcast an RREQ M1 gets the RREQ and encapsulates it in a packet destined to M2 through the path that exists between M1 and M2(P-Q-R). Node M2 turns the packet into its previous state and rebroadcast it again. Due to the encapsulation of the data packet, the hop count does not raise when RREQ travels between M1 and M2. At the same time another copy of the RREQ travels from S to D over the path that includes nodes E- F-G. Now there are 2 paths from S to D, the first one is four hops long (S-E-F-G-D) and second one is three hops long (S-M1-M2-D), while in reality it is six hops long (S-M1-P-Q-R-D). The destination chooses the second route since it appears to be the shortest path [4].

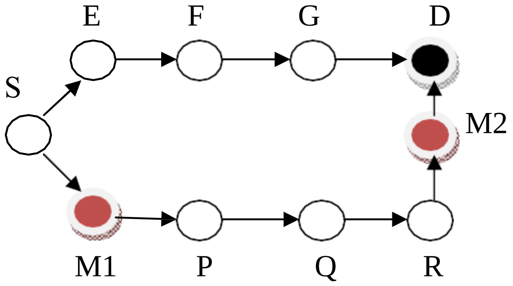

Fig 5: Wormhole attack using Packet Encapsulation

4.3 Flooding Attack

Flooding RREQ packets in the network will consume a lot of resources of network. To reduce congestion in a network, the AODV protocol adopts several methods. A node can not originate more than RREQ_RATELIMIT RREQ messages per second. After broadcasting RREQ message, a node waits for a RREP.

If a route is not received within Round-Trip Time, the node may strive again to discover a route by broadcasting another RREQ, up to maximum TTL value. The first time a source node broadcasts a RREQ, it waits round-trip time for the response of a RREP. If a RREP is not received within that time, the source node sendsa new RREQ.

When measuring the time to wait for the RREP after sending the second RREQ, the source node must use a Binary Exponential Back Off. Hence, the waiting time for the RREP corresponding to the second RREQ is 2 * Round-Trip Time (RTT). The RREQ packets are broadcast in an incrementing ring to minimize the overhead caused by flooding the whole network.

The packets are flooded in a limited area (a ring) first defined by a starting TTL (time-to-live) in the IP headers of packet. After Ring Traversal Time, if no RREP has been received, the flooded area is enlarged by increasing the TTL by a fixed value. The whole procedure is repeated until an RREP is received by the creator of the RREQ, i.e., the route has been found [6].

Detection of flooding attack:

The method of *Neighbor Suppression* is used to prevent RREQ Flooding Attack. MANETs are multi-hop wireless networks, and the node exchanged packets through its neighbor nodes. If all neighbor nodes around the node decline to forward its packets, the node cannot communicate with the other nodes in mobile ad hoc networks.

The node has been inaccessible from the network in practice even if it is still in the networks in location. Fig 5 shows that a topology of mobile ad hoc network. The node P communicates with the other node through node A, B, C and D. If neighbor node A, B, C and D refuse to receive packets from node P, node P cannot send anypacket to the other nodes [6].

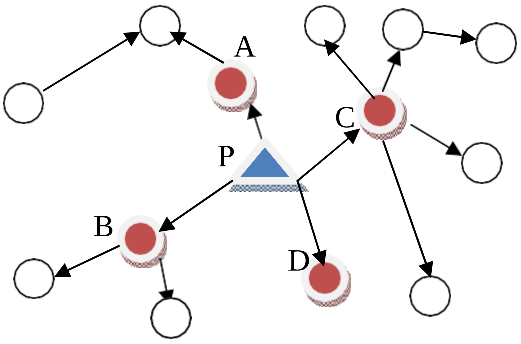

Fig 6: Neighbor nodes isolate attacker

```
Algorithm 1: calculate time of RREQ
Step1. Received a RREQ;
Step2. If the RREQ is forwarded then quit;
Step3. Look up node ID who sends the RREQ in the table of Rate_RREQ;
Step4. Find node ID and RREQ_time:=RREQ_time+1;
Algorithm 2: find the intrusion
For every item of Rate_RREQ do
If RREQ_time > threshold then put Node_ID into Blacklist and RREQ_time:=0;
Else RREQ_time:=0;
```

5. Conclusion

Several Network layer Attacks and their detection mechanism were described in this paper. Ad hoc on demand distance vector (AODV) protocol were used to describe these attacks. We have also kept a close look on the algorithms needed to mitigate the attacks and tried to bind the attacks into categories according to that. We will try to explore these algorithms in further research.

References

[1] Kamini Maheshwar and Diwaker Singh, “Black Hole Effect Analysis and Prevention through IDS in MANET Environment”, European Journal of Applied Science and Engineering and Scientific and Research, 2012.

[2] Poonam Yadav, Rakesh Kumar Gill, Naveen Kumar, “A Fuzzy Based Approach to Detect Black Hole Attack”, International Journal of Soft Computing And Engineering (IJSCE), Volume-2, Issue-3,July-2012.

[3] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto , "Detecting Black hole Attack on AODV based Mobile Ad hoc Networks by dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007 338.

[4] Majid Meghdadi, Suat Ozdemir and Inan Guler, "A Survey of Wormhole based Attacks and their Countermeasures in Wireless Sensor Networks", in Proceedings of IETE Technical Review, Volume 28, No.2, Mar-April 2011.

[5] Jaydeep Sen, "Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", Innovation Lab, Tata Consultancy Services Ltd, 2013.

[6] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong," A New Routing Attack inMobile Ad Hoc Networks", in Proceedings of International Journal of Information Technology, Vol. 11, No. 2.

[7] M.A.AL-SHABI, "Attacks and Defense in Mobile Ad hoc Networks", in Proceedingsof International Journal of Reviews in Computing, 31st December 2012, Vol 12.

[8] Sushil Kumar, Vishal Pahal, Sachin Garg, "Wormhole attack in Mobile Ad Hoc Networks: A Review", Engeering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No. 2, April 2012.

[9] Pradip M.Jawandhiya, Mangesh M.Ghonge, Dr. M.S.Ali, PROF. J.S Deshpande, "A Survey of Mobile Ad Hoc Network Attacks", in Proceedings of International Journal of Engineering Science and Technology, Vol2(9), 2010,4063-4071.

[10] Mohammad Wazid, Rajesh Kumar Singh, R.H. Goudar," A Survey of Attacks Happened at Different Layers of Mobile Ad- Hoc Network & Some Available Detection Techniques", Proceedings published by International Journal of Computer Application (IJCA), International Confrence on Computer Communication and Networks CSI-COMNET-2011.

[11] Vikas Solomon Abel, "Survey of Attacks on Mobile Adhoc Wireless Networks", Proceedings by International Journal on Computer Science and Engineering (IJCSE), Vol 3, No 2, Feb 2011

[12] Preeti Nagrath, Bhawna Gupta," Wormhole attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey",978-1-4244-8679-3/11/$26.00@2011 IEEE.