IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 11, November 2014 ISSN 2321-5992

Detection of rushing attack by comparing energy, throughput and delay with AODV

Meena Bharti[1], Manish Goyal[2] and Rajan Goyal[3]

[1]M.Tech Thapar Univerisity,Patiala,India

[2]University College,Ghudda,Bathinda, India

[3] YCOE, Talwandi,Bathinda India

ABSTRACT

MANET consists of several nodes where each node is connected to one or more nodes. To secure the wireless ad-hoc network, we need to detect the various attacks. And this major objective is achieved by increasing more security to the nodes and providing the easy computation to each node and less complexity. The work is processed in a way to detect the attack by analyzing the various methods and finding out best and efficient method out of it. In this paper we are presenting a way to detect rushing attack by comparing energy, throughput and delay parameters with simple AODV protocol.

Keywords:- MANET, Rushing Attack, Mobility model, Types of attack in MANET

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. We can internetwork people and vehicles in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges. The nodes that not in the direct communication range use intermediate node(s) to communicate. As we can see that in these two situations, each node that has participated in the communication forms a wireless network automatically. Such type of communication in which each node participates to make a network can be viewed as mobile ad hoc network [10]. A self-configuring network which is formed by a collection of mobile nodes automatically without the help of a fixed infrastructure or centralized management is called mobile ad hoc network (MANET). In such a network each node contains a wireless transmitter and receiver, using which node communicates with other nodes which are in its radio communication range. Sometimes a node has to communicate with some other nodes which are not in its radio range. In that case, a node takes cooperation of other nodes in the network. Such type of communication is called multi-hop communication. So we can say that each node has to act as both a host and a router at the same time. As the nodes are mobile so these move in or out continuously form radio range of other nodes[4]. So, the network topology changes frequently. A Mobile adhoc network with the above described features was originally developed for military purposes, as in battlefield nodes are scattered and there is no infrastructure to help them form a network. With the advancement usage of mobile adhoc network is increasing day by day. It is used in many areas, ranging from military to civilian and commercial uses, because setting up such networks can be done without the use of any infrastructure or interaction with a human [1]. Some examples of MANET are: data collection, search-and-rescue missions and virtual classrooms and conferences where laptops or other mobile devices which share wireless medium and communicate to each other [7, 14].

2. Related Work

R. Kravets, S. Yi, and P. Naldurg, et al. [2] proposed a new technique of routing called Security-Aware ad hoc Routing (SAR). It contains security attributes which are used as parameters into ad hoc for route discovery. It is used to enable security as a negotiable metric so as to improve the relevance of the routes discovered by ad hoc routing protocols. Two-tier classification of routing protocol security metrics was developed and a framework is proposed to measure and enforce security attributes on ad hoc routing paths. Proposed framework enables applications so as to adapt their behavior according to the level of protection which is available on communicating nodes in an ad hoc network.

Satoshi Kurosawa et al. [5] proposed the solution to rushing attack keeping in mind that in MANET conditions changes dynamically. In AODV, to check the freshness of routing sequence present in message coming from node detections sequence was used. If attacker wants to attack it must generate its RREP with the destination sequence number greater than the destination sequence number of the destination node [5]. Attacker can use the RREQ packet to find the destination sequence number. In this case if other node tries to construct the route to the destination node which is not source node, then the destination node's sequence number will be become different from the sequence number of current destination**.**

P., K. Vinod et al. [15] discuss the various attacks on Mobile Ad-Hoc Networks (MANET). They define MANET as self- administered, self-configured, and self-organized network. In MANET, nodes are not connected to each other physically i.e. there is no wired connection between nodes, but nodes use transmission range of each other to communicate. As nodes in MANET have mobile nature. Due to which MANET changes its topology from time to time. MANET lacks fixed infrastructure and is more prone to malicious attacks. In this paper, the author discusses Blackhole Attack, rushing attack and various other attacks.

3. CHARACTERISTICS OF MANET ARE

The characteristics of mobile adhoc network are as follow:

- Links between wireless sensor nodes are unreliable. There is a limited supply of energy in wireless nodes for mobility. So, links between mobile nodes lose their consistency for communication [6, 8].
- Constantly change in topology. As the motion of nodes is continuous, the change in topology of mobile ad hoc network is constant. The nodes continuously move so move in and out of range of other nodes in MANET and due to this routing information will change continuously [6, 11].
- Security features in statically configured wireless routing protocol has lack of incorporation which is not meant for adhoc network. It is because in ad hoc environment topology changes constantly. So, it becomes necessary for every pair of adjacent nodes to seek some issues of wireless network so that we can prevent our network from potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Due to features of MANET which are listed above, these mobile ad hoc networks are more prone to malicious attacks than the traditional wired networks. Therefore, there is more need to pay attention to the security issues in the MANET.

3.1 Security Goals

To providing a secure network environment the following services are required [19]:

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Availability
- Detection and Isolation

3.2 Authentication: Authentication is used to identify the identity of the mobile node and to be able to identify fake nodes. In infrastructure based wireless network, there is a possibility to implement a central node or an administrator node. But in Mobile ad hoc networks there is no central authority to control the system and providing authentication is the difficult task. To provide authentication in mobile ad hoc networks various encryption techniques are used [9].

3.3 Confidentiality: Ensures that information is never disclosed to unauthorized access. Confidentiality keeps the sent information unreadable to attackers. MANET uses the open medium, so mobile node communicates directly. To keep data confidential first way is to encrypt data by encryption techniques and to use directional antennas. This ensures that data is only accessed by the valid mobile nodes [12].

3.4 Integrity: Integrity ensures that message being transmitted was never corrupted i.e. data which was transmitted was never altered during transmission [12]. Integrity maintains the originality of messages.

3.5 Non repudiation: The sender cannot later deny sending the information and receiver cannot deny the reception. By producing signature for the message, receiver cannot deny the message. In cryptography where public key is used, a node A signs the message using private key [9]. All other nodes can verify the message using the A's public key and A cannot deny that message signed by A.

3.6 Availability: Ensures the availability of all nodes at all time. A node continues to provide services despite attacks.

3.7 Detection and Availability: Require the protocol can identify misbehaving nodes and render them unable to interfere with routing [13]. Various detection schemes are used to provide a smooth communication between the mobile nodes.

4. VARIOUS TYPES OF ATTACKS IN MANET

Attacks are categorized in two different modes in MANET passive attacks and active attacks.

4.1 Passive Attacks

In this type of attack malicious nodes are in passive mode. They do not modify the exchanged attacks but only listens. An attacker node does not disrupt properly the communication operation. During this attack violence of confidentiality is occurred when another attacks uses the information gathered by the passive attracters [1]. These types of attacks are difficult to detect because attackers does not involved as a part of communication process. These are only listeners. To prevent these attacks powerful encryption techniques can be applied so that attacker is unable to crack the security

4.2 Active Attacks

Active attacks are performed to alter or to destroy the information exchanged on the network. Active attacks are disrupting functioning of the network. These attacks are classified in two categories external attacks and internal attacks [1]. In internal attacks are performed by the nodes which are part of the network or showing that they are part of the network. Internal attacks are more difficult to detect because nodes are the certified in the network. On the other hand external attacks are launched by the external nodes which are not the part of the network. These types of attacks are prevented by using strong encryption techniques.

4.3 Rushing Attack

First of all the dictionary meaning of 'RUSHING ATTACK' is "a sudden attack", or "to perform, accomplish, or complete with speed, eagerness, or violence". "RUSHING ATTACK" is also called as "novel attack" or "denial of service" attack in networking [2]. In AODV routing protocol, when source nodes flood the network with route discovery packets (RREQ, RREP) in order to find routes to the destinations, every in-between node process only the first non replica packet and throw-outs any replica packets that arrive at a later time. A rushing attacker utilize this replica repression mechanism by quickly forwarding route discovery packets with a malicious RREP on behalf of some other node skipping any proper processing in order to gain access to the forwarding group [9]. In rushing attack, an intruder will "rush" (transmit early) the RREQ packet to suppress any later legitimate RREQs as shown in the Fig. 5. The source node S broadcasts a RREQ for node 3 and node 2. Now, on hearing the RREQ, the malicious node 3 rushes the RREQ to suppress the later legitimate RREQ. The rushing may in the following ways [9]. Malicious node 3 ignores the request forwarding delay (this is a randomized delay used by the routing protocol to avoid collision of broadcast packets).

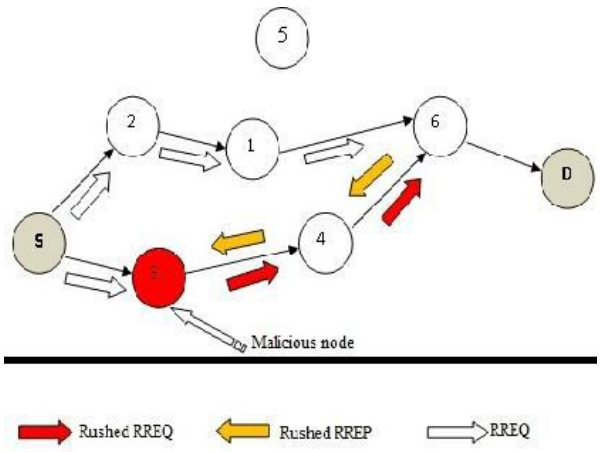

Figure 2: Rushing Attack [9]

Malicious node 3 rushes the RREQ with a higher source sequence number. This rushed RREQ from Malicious node 3 arrives first at node 6, and therefore node 6 will discard the legitimate RREQ from node 1 when it arrives later via 1, as shown in Fig. 5. Due to duplicate suppression, the actual valid RREP message from valid node will be discarded and

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 11, November 2014 ISSN 2321-5992

consequently the attacking node becomes part of the route. In rushing attack, attacker node, send packets to proper node after its own filtering is done, so from outside the network, the nodes behaves normally and nothing was happened. But it might increase the delay in packet delivering to destination node [2].In this section it is briefly detailed about the active attacks on the network layer with the examples. These researches on attack are concluded that the attacks degrade the performance of the network as fit as data packet transmission. In the next section it is discussed about development of the detection mechanism by various researchers to defend against the attacks.

5. EXPERIMENTAL ANALYSIS

To do experimental analysis we implemented simple AODV protocol and rushing attack. The screen shots of simple AODV and rushing attack is shown in Figure 2 and Figure 3.

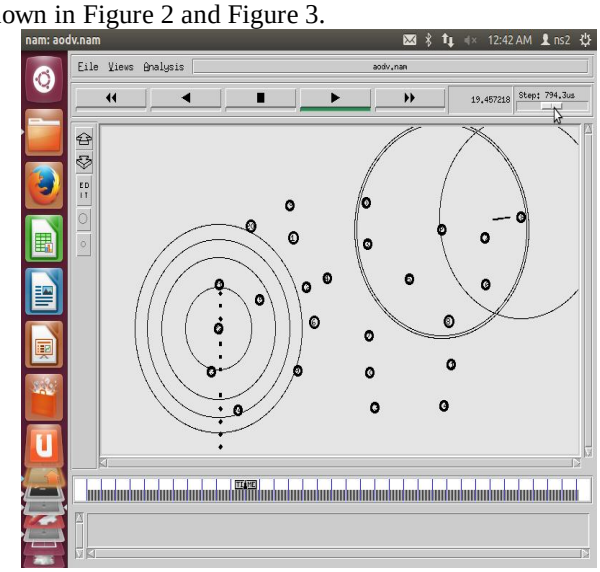

Figure 2: Simple AODV

In above figure we can see that there is no attacking node and each packet can transfer any path to reach destination from source.

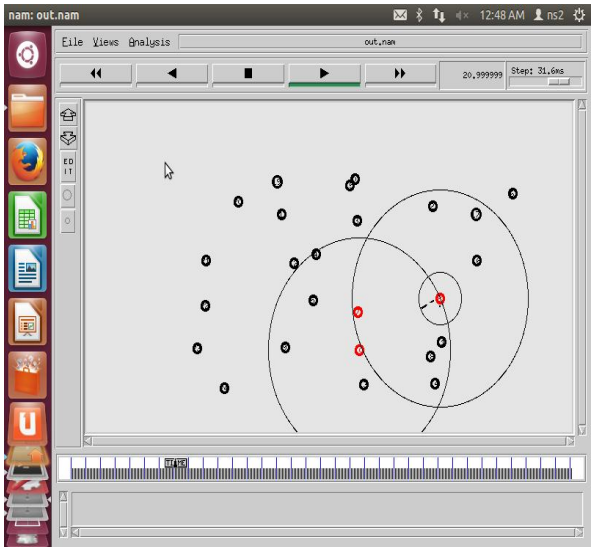

Figure 3: Rushing Attack

In above figure we can see that there are 3 attacking nodes. When packets go from source to destination it will pass through these attacking nodes as attackers increase speed of packets.

6. Results

After implementing AODV and Rushing attack we are comparing end-to-end delay, packet delivery ratio and throughput. Comparison of end-to-end delay is shown is Figure 4.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 11, November 2014 ISSN 2321-5992

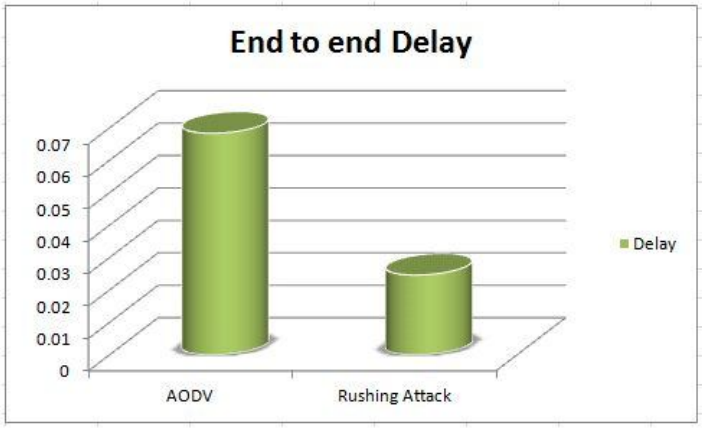

Figure 4: AODV and rushing attack end-to-end delay comparison.

In above figure we can see that end-to-end delay in rushing attack is less as compared to AODV. It is because in rushing attack packets move fast so delay decreases in rushing attack due to which all nodes start to send packets to send packets through these attacking nodes.

Comparison of packet delivery ratio is shown in Figure 5.

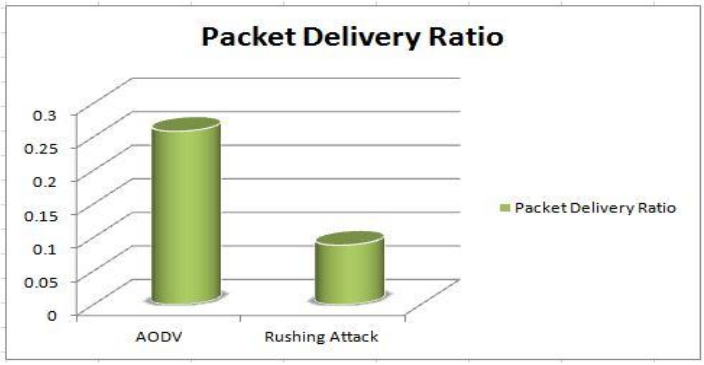

Figure 5: AODV and rushing attack packet delivery ratio comparison.

In above figure we can see that packet delivery ratio of rushing attack is less than simple AODV protocol. It is because it may happen that attacker node don't send all packets properly to destination.

Comparison of throughput is shown in Figure 6.

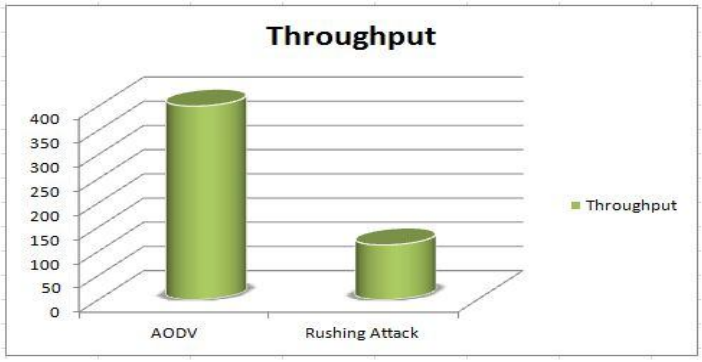

Figure 6: AODV and rushing attack Throughput comparison.

In above figure we can see that throughput is lower in case of rushing attack.

7. Conclusion and Future Scope

In this paper we have studied about MANET, its characteristics, security goals. And rushing attack is defined in detail. We have seen that in rushing attack, attacker node increase the speed of packet due to which acknowledgement received to sender becomes earlier then other nodes. So, end-to-end delay decreases in rushing attack. But also throughput and packet delivery ratio is decreases. This means that more packets are getting lost in way. In future work can be done on detection on various other attacks. Also the prevention of attacks can be done.

References

[1] K, Prasana Venkatesan T, Ramkumar R.," Security Attacks and Detection Techniques for MANET" Discovery, Volume 15(42), 89-93, April 10, 2014.
[2] R. Kravets, S. Yi, and P. Naldurg, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks", In ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001.
[3] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing", Kluwer Academic Publishers, Vol 353, 1996, pp. 153-181.
[4] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75
[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.
[6] Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.
[7] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia
[8] Gajendra Singh Chandel and Rajul Chowksi, "Study of Rushing attack in MANET," International journal of ucterion (IJCA), Vol. 79, No. 10, Oct. 2013.
[9] K. Udhayakumar, T. Prasanna Venkatesan and R. Ramkumar, "Security Attacks and Detection Techniques for MANET", Discovery, Volume 15, Number 42, April 10, 2014
[10] Nitesh Funde & P. R. Pardhi, "Analysis of Possible Attack on AODV Protocol in MANET" International Journal of Engineering Trends and Technology (IJETT) – ISSN: 2231-5381 Volume 11 Number 6 – May 2014
[11] Gwalani, S. ; Srinivasan, K. ; Belding-Royer, E.M. ; Kemmerer, R.A., " An intrusion detection tool for AODV-based ad hoc wireless networks" IEEE - Computer Security Applications Conference, 2004. 20th Annual, Page(s): 16 – 27, Dec. 2004
[12] Ipsa, De.,"Comparative study of Attacks on AODV-based. Mobile Ad Hoc Networks.", Calcutta Institute of Engineering and Management. India. ISSN : 0975-3397 Vol. 3 No. 1 Pg No. : 313-322 Jan 2011
[13] S. Özdemir, M. Meghdadi, and Ý. Güler. "A time and trust based wormhole detection algorithm for wireless sensor networks," (manuscript in Turkish), in 3rd Information Security and Cryptology Conference (ISC′08), pp. 139−4, 2008.
[14] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, Xiangke Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks" IEEE Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference, ISSN: 1092-1648, Page(s): 314 – 323, 2009.
[15] P., K. Vinod, "A Review on Detection of Blackhole Attack Techniques in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 4, Issue 4, April 2014.