International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 08 | Nov-2015 www.irjet.net p-ISSN: 2395-0072

Period Based Defense Mechanism Against Data Flooding Attacks

C.R.Dhivyaa[1], R.Sudhakar[2]

[12]*Assistant Professor/ CSE Nandha College of Technology, Erode,Tamilnadu ,India.*

Abstract: ***MANET is an emerging research area with practical applications. However MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed co-operation. One of the main challenges is to provide a path with secure robustness in wireless ad hoc networks. In this article we analyze in detail one type of attack-data flooding that can be easily employed against AODV [Ad-hoc On Demand Distance Vector Routing] in MANET. We propose a novel mechanism to secure AODV protocol from data flooding attack.***

Keywords - MANET, AODV, dynamic topology.

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure. Instead each node participates in routing by forwarding data for other nodes and the determination of which node forwards the data is made dynamically based on the network connectivity. This means that a formed network can be de-formed on-the-fly without the need for any system administration. The term "ad-hoc" tends to imply "can take different forms" and "can be mobile, standalone, or networked". Ad-hoc nodes or devices should be able to detect the presence of other such devices and to perform the necessary handshaking to allow communications and sharing of information and services. Routing in ad-hoc networks has been a challenging task ever since wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree in node mobility. In order to establish routes between nodes, which are farther than single hop specially configured routing protocol are engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology. A number of protocols have been developed for accomplish this task. Ad-hoc On-demand Distance Vector (AODV) is one of the widely used routing protocol that is based on distance vector routing, but the updates are shared not on a periodic basis but on as per requirement basis.

The remainder of this paper is organized as follows: Section 2 describe an overview of AODV protocol. In Section 3 introduction to Data Flooding attack is given, Section 4 presents related work on MANET security. In Section 5 describes proposed work and Section 6 describes the result analysis and Section 7 describes the conclusion.

2. AODV OVERVIEW

2.1 ROUTING PROTOCOLS IN MANET

Routing is an activity or function that connects a call from origin to destination in telecommunication networks and also plays an important role in architecture, design, and operation of networks. MANET routing protocols are classified as

i) Table Driven Routing Protocols

A proactive routing protocol is also called "table driven" routing protocol. Using a proactive routing protocol, nodes in a mobile Ad Hoc network continuously evaluates routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. Therefore, a source node can get a routing path immediately if it needs one.

Here all nodes need to maintain a consistent view of the network topology. When a network topology change occurs, respective updates must be propagated through the network to notify the change. Some of the table driven routing protocol are Destination Sequence Distance Vector (DSDV), Optimized Link State Routing (OLSR).

ii) Reactive Routing Protocols

Reactive routing protocols for mobile Ad hoc networks are also called "on-demand" routing protocol. On demand protocols create routes only when desired by source nodes. When a node requires a route to destination, it initiates route discovery process within the network. This process is completed once route is found. Some of the reactive protocols are Dynamic Source Routing (DSR), AODV.

2.2 WORKING OF AODV PROTOCOL

AODV is an on demand protocol as it finds the routes only when required by the source node for transmitting the data. AODV has two phases, the route construction phase and route maintenance phase. In the route construction phase a route must be created from source node to destination node. While in the maintenance is to rebuild a route between source and destination since the previous found route may be broken due to the nodes movement.

i) Construction Phase

In the construction phase, when a source node needs to send packets to destination node and if there is no valid route between the source node and destination node, the source node initiates a path discovery process to locate the destination node as shown in Figure 1. The source node will broadcast a route request (RREQ) packet to explore a route to the destination. The source node employs destination sequence number to identify the most recent path. A route request carries source identifier (srcID), the source sequence number (srcseqnum), the destination sequence number (destseqnum), the broadcast identifier (broadcast Id) and time to live (TTL).Destination sequence number are used to identify the most recent path and the freshness of the route is also accepted by the source. A node updates its path information only if the destination sequence number of the current packet received is greater than the last destination sequence number stored at the node.

ii) Route Discovery

In the route discovery process, each intermediate node that receives the (RREQ) packet will re-broadcast the packet to its neighbours as shown in Figure 2. The duplicate copies are discarded, if a route request is received multiple times which is indicated by (broadcast ID-source ID pair).Once the RREQ reaches the destination or the intermediate node with fresh route to destination is located, the destination /intermediate node will send a route reply (RREP) packet back to source along reverse route path. Every intermediate node while forwarding a route request enters the previous node address and broadcast ID. A timer is used to delete this entry in case a route reply is not receiving before time expires. This helps in storing an active path at the intermediate node. When a node receives route reply packet information about the previous node from which the packet was received is also stored in order to forward the data packet to the next hop towards the destination.

iii) Route Maintenance

If the route between source and destination may be broken since the nodes along the route will move from time to time. If a source node moves, it is able to reinitiate route discovery process where it can create a new route to the destination node. If an intermediate node along the route moves, its upstream neighbor will observe the move and propagate a Route Error (RERR) packet to its upstream neighbours and this process continues until source node is reached.

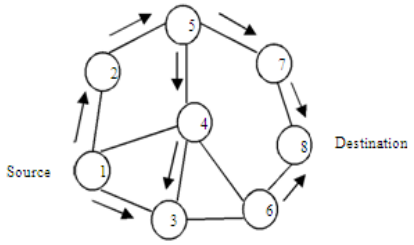

Figure 1 RREQ Request

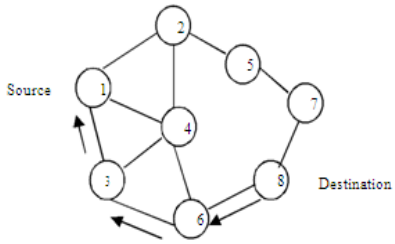

Figure 2 RREQ Reply

3. FLOODING ATTACK

Flooding attack, in which the attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power and network bandwidth will be consumed and could lead to denial-of-service will be dropped without forwarding.

i) Data Flooding attack

Data Flooding Attack in AODV protocol works as follows. At first, the attack node [3] builds up paths to all

nodes in the network. Then, the attacker sends large volumes of useless Data packets to all nodes along these paths, as shown in Figure 3, so that the data packets are forwarded at higher rate.

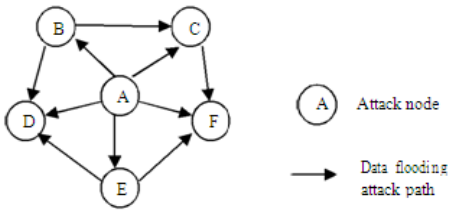

Figure-3 Data Flooding Attack

The mass useless DATA packets will exhaust the communication bandwidth in the network and the destination node will be busy for receiving the excessive useless data packets from the attack node and therefore cannot work normally.

4. RELATED WORK

Most of the previous works on security attacks and its countermeasures in reactive routing protocol such as AODV are specified.

In [2], M. Al-Shurman et al. proposed black hole attack that malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route the data packets through the malicious one

In [3], D.B. Johnson et al. introduced Worm Hole Attack that, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality.

In [4], Ashish D et al. Studied and showed the Gray Hole Attack which may forward all packets to certain nodes but may drop packets coming from or destined to specific nodes.

In [5], Y.C. Hu et al. proposed a new attack, which we call the rushing attack, which acts as an effective denial-of-service attack against all currently proposed on-demand ad hoc network routing protocols, including protocols that were designed to be secure

In [6], D.Raffo et al. proposed Link Spoofing Attack, in which a malicious node may advertise fake links with non-neighbours to disrupt the routing operations.

In [7], S.Marti et al. introduced Colluding misrelay attack, in which multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in MANET.

In [8], Bo-Cang Peng et al. proposed Forward Attack Path cutoff technique and Neighbour Suppression technique to prevent the data flooding attack by cutoff the path from the attacker node and drop the packets from the attacker node respectively.In [9], C.Sreedhar et al. proposed that Symmetric Cryptographic Techniques are used to avoid attacks on routing protocols.

5. PROPOSED WORK

In wireless ad hoc networks to conduct the data flooding attack attacker first sets up a path to the victim node because an attack can be performed after constructing the path. Then, the attacker forwards tremendous useless data packets along the path so that the victim node cannot process packets in normal fashion. So finally resources of the victim node are exhausted. In order to measure the effect of data flooding attack in wireless ad hoc networks we are going for Period Based Defense Mechanism [1].The PDM scheme checks data packet floods at the end of each period in order to enhance the throughput of burst traffic.

To prevent malicious data packet flooding attacks with enhancing the throughput of burst traffics, PDM checks data packet floods at the end of each period. It also guarantees the Quality of Service (QoS) of burst traffics. We denote v(nSpnDp) as the variance of the number of received data packets for the source node (nSp) to the destination node (nDp) during T(i-1)-T(i) where i is between 2 and ∞ as shown in Figure 4. The node initiates the period T(i) and h(nSp-nDp) according to its data type. h(nSp-nDp) is the variance coordinator for data packet floods from nSp to nDp to guarantee QoS. ave(all) is the average number of received all data packets during T(i-2)-T(i-1). Then, the variance limit of data packet floods from nSp to nDp, vlimit (nSp − nDp) = ave(all) + h(nSp − nDp).

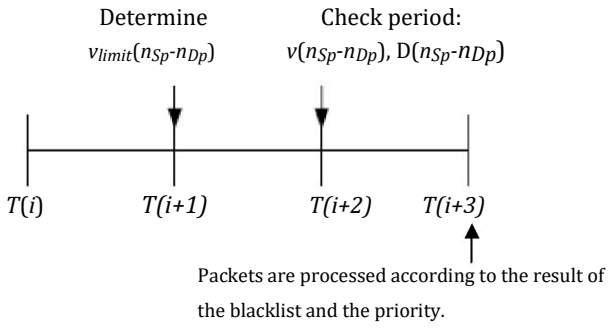

Figure 4 Procedures of each period in the PDM scheme

If the end of the period T(i), the node ni compares the variance of each received data packets according to its nSp and nDp pairs (v(nSp-nDp)) with its variance limit vlimit(nSp-nDp). If v(nSp-nDp) is greater than vlimit(nSp-nDp), it checks whether data packets for nSp-nDp (D(nSp-nDp)) are in the blacklist or not. If D(nSp-nDp) is in the blacklist, it is not transmitted until the next period (T(i+1)). If it is not in the blacklist, its priority is determined by the inversion of the number of received data packets. Then, it is processed according to its priority, and the node updates the blacklist by the greatest number of received data packets in the period.

Recently many users like to download and share the multimedia data, so we are extending our work to multimedia data transmission. For multimedia transmission we are going to give priorities to multimedia packets and these packets are transmitted faster than the normal packets. So that end to end delay for multimedia packets will get reduced and delivered faster than the normal packets.

6. RESULT ANALYSIS

To validate our analysis, we have to implement Period Based Defense Mechanism (PDM) in multimedia transmission in a simulator and by performing a serious of simulation based experiments to test its effectiveness.

Simulation parameters

Simulation time	15M
Number of nodes	20
Terrain dimensions	800,800)
Node placement	Uniform
Routing protocol	AODV

In Figure 5, we use AODV as the basis of routing protocol and compare its performance with that of our PDM scheme.

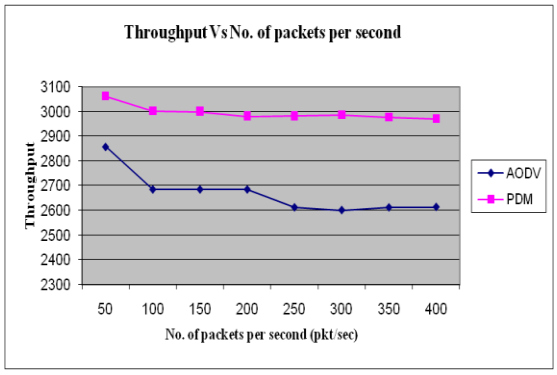

Figure 5 Throughput Vs No. of Packets per second

To investigate how much QOS is guaranteed, we have implemented flooding attack by increasing the no. of data packets per second from 20 packets per second to 400 packets per second by assuming that we have 5 attackers. When the no. of packets per second is high, AODV cannot process the packets because of the resource exhaustion.

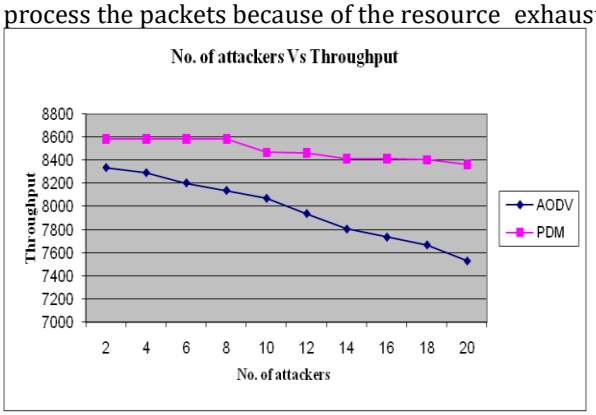

Figure 6 Number of attackers Vs Throughput

Figure 6 shows the throughput varying with the no. of attackers from 0 to 20 attackers. To compare the affect of the no. of attackers to the throughput, each node including attackers sends 20 packets per second.

Hence, the throughput of the PDM scheme is higher than AODV so that it can defend against malicious data packet flooding attacks.

7. CONCLUSION

The existing security schemes for wire networks cannot be applied directly to the MANET, which makes MANET much more vulnerable to security attacks. In this paper we have analyzed the routing attacks and countermeasures in MANET. Here we have shown that the data flooding attack paralyzes a victim node by consuming its resources. Hence, the throughput of the victim node is significantly reduced. Hence the Period-based Defense Mechanism (PDM) scheme is used in multimedia data transmission, to efficiently prevent the data flooding attack, as a result of which many data packets are forwarded at a high rate for the whole duration. Hence it enhances the throughput of the burst traffic.

REFERENCES

0. Hyojin Kim, Ramachandra Bhargav Chitti and JooSeok Song, "Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks," June 2010.

1. M. Al-Shurman, S-M. Yoo, and S.Park, "Black Hole attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conf. 2004.

2. Y-C. Hu, A.Perrig and D.Johnson, "Worm Hole Attack in Wireless Networks," IEEE JSAC, vol.24, no.2, Feb 2006.

3. Ashish D, "Gray Hole Attack in Mobile Ad Hoc Networks,".

4. Hu Y-C, Perrig A, Johnson D. "Rushing attacks and defense in wireless ad hoc network routing protocols". ACM Workshop on Wireless Security (WiSe 2003), San Diego, California, U.S.A., 19 September 2003.

5. D. Raffo et al., "Securing OLSR using Node Locations," Proc. 2005 Euro. Wireless, Nicosia, Cyprus, Apr. 10-13, 2005.

6. S. Marte et al., "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks," 6th MobiCom, Boston, MA, Aug.2000.

7. Bo-Cang Peng and Chiu-Kuo Liang, "Prevention Techniques for Flooding Attacks in Ad Hoc Networks,".

8. C.Sreedhar, Dr. S.Madhusudhana Verma, Prof. N.Kasiviswanath, "A Survey on Security Issues in Wireless Ad-hoc network Routing Protocols".

9. Sven Wietholter, Christian Hoene, "Design and Verification of an IEEE 802.11e EDCF Simulation Model in ns-2.26," Telecommunication Networks Group, Technische Universitat Berlin, Nov. 2003.

BIOGRAPHIES

C.R.Dhivyaa working as Assistant Professor in the department of computer science and engineering, Nandha College of Technology,Erode. She has three years of teaching experience. Her area of interest are Image Processing, and Data Mining. Her publications include five international journals.

R.Sudhakar working as Assistant Professor in the department of computer science and engineering, Nandha College of Technology, Erode. He has three years of teaching experience. His area of interest are Networks and Security. His publications include five international journals.