International Journal of Advance Research in Science and Engineering
Vol. No.5, Special Issue No. (01), February 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

A STUDY ON SPECIFIED AND CO-OPERATIVE ATTACKS IN MANETS

Vandana N.S[1], Mrs Bharathi M[2], Dr. Mydhili K Nair[3]

[1]PG Student, 1V Sem M.Tech, S J C Institute of Technology, Chickballapur, Karnataka (India)

[2]PHD Research Scholar, [3]Professor, Dept. of ISE, MSRIT College of Engineering,
Bangalore, Karnataka (India)

ABSTRACT

Mobile Adhoc Network [MANET] is a connection less oriented, it is basically a communication between two or more devices with the help of radio waves. As technology goes on increasing number of newer technologies had been introduced which helps the user to reach their goals easily. But the security issues are also raising as big problem. In MANET battery saving, failure of network suddenly causes the work to lead back. Many types of attacks will be there in MANET ,for example masquerade attack, relay attack, black hole attack etc. Black hole attack means when a packet is sent from source to destination , intruder may damage the packet, so that packet will be lost with out reaching to destination. The attack may be on single node(route request) or co-operative attack. In this paper we are going to discuss in brief how single node and co-operative attack occurs and to over come it by using Encryption, decryption, Dynamic Source Routing Protocol (DSR) .

Keywords: Black hole, Routing protocols, DSR protocol.

I. INTRODUCTION

As discussed MANET is connection less oriented, the main challenge is maintaining data availability even at worst traffic situations. Black hole attack is type of active attack. Attacks are basically classified into following types,

1) Active attack
2) Passive attack
3) Internal attack
4) External attack

1. Active attack: If any data related to operation need to be downloaded means, it does not care for the currently going operation/task, it disturbs entire network and gets the data from network.

2. Passive attack: These will not directly download the data, but will act indirectly on network and access the data. This leads to confidentiality damage.

Consider for example, In bank a person wants to with draw money from his account from online, the other side intruder will be observing the process that is going on, but person will not know about the intruder, once the actual person gets his money from bank which is processed in online. The intruder will be ideal for some time and again send the request to draw money from account. Here actual person does not know the cash with drawl from intruder until he gets the alert by means of message.

3. Internal Attack: It can be caused silently in a group or any organization, so leading to disturb entire organization. Here the intruder may delete his attack once he has interrupted, further it does not know about the interrupt that has occurred because of removing the evidences. The best way is to introduce Intrusion Detection System (IDS) and configure to scan, so once intruder attacks the log of attacking should be viewed.

4. External attack : These includes attacks like Trojan horse attack, viruses, worms etc. these are not usually solved by software's that are installed, because there behavior will be entirely different from the software that user have installed.

II. ROUTE REQUEST PATH (SPECIFIED PATH BLACK HOLE ATTACK)

Usually source will be given one common or specific path to reach to destination. There may be chances of occurring black hole attack such that , intentionally dropping, delaying the packet to reach to the destination called as DOS attack. Once the packet is reached to the destination, the source user will ask to destination user to send the packets that it had sent, the destination packets will be compared with the source packets, if there is no variation in packets, then no black hole attack has occurred.

III. DOS ATTACK

This attacks makes temporarily to loose the packet to reach destination. It also keeps on sending fake requests along with real requests and confuses entire network. The examples for DOS includes hacking user’s bank password, ATM card password, Debt card password and so on.

IV. OVERCOMING DOS ATTACK

Attacks can be of different ways, there will be other techniques to over come,

1) Using encryption and decryption.

2) Using public key and private.

1. Using encryption and decryption : Once the user selects the packet that need to be sent to destination, the user on source side should encrypt his data. That is the packets which will be in the form of characters, words or numbers will be converted to binary (0’s and 1’ns) format. So the attacker in middle may not understand the packet information. Once the packet is delivered to destination, the destination user can decrypt the encrypted packet data.

2. Using public and private key: Source user and destination user will be having their own private address and public address. If source user sends the packet to destination, destination user will use his private key and senders public key to encrypt the data.

V. BLACK HOLE ATTACK IN CO-OPERATIVE NETWORK

Since Mobile Adhoc network [MANET] is dynamic in nature, there will be no fixed infrastructure to deal with it. The packet that need to be sent to destination attacked co-operatively(in group) and leads to packet failure. So how to over come the problem?.

In order to over come problem we have chosen Dynamic Source Routing (DSR) protocol techniques.

As the name specifies Dynamic means, not constant . Three methods we mainly follow to route the protocols.

1) Pro active or table drawn protocol
2) Reactive or On demand protocol
3) Hybrid protocol

1. Proactive or table drawn protocol: It follows the routing table. Each time when an entry is performed every thing will be maintained in the form of logs. Even though intruder deletes after attacking the packet, the attack will be scanned and maintained in the routing table.

Example, ADOV, DSR

2. Reactive or On demand protocol: It will be in active position when number of routing table entries have been increased.

Example, DSDV routing protocol

3. Hybrid protocol: The combination of reactive as well proactive protocol will be called as hybrid protocol.

Example, Zone routing protocol (ZRP)

VI. INTRODUCTION TO ADOV

ADOV(Adhoc On-Demand Distance Vector Algorithm). This algorithm does not require specific path to travel, does not take negative values. Source sends packets to destination, does not matter even if source fails. The packet forwarding depends on route request, the current packet sends the RREP to next node which is beside the current node, if the path is free it sends back the conform path to travel to next path. Every time when RREP is made it maintains RREP table. The RREP can be cross checked in routing table, because it needs verification such as whether the node has already used or it is fresh node to reach destination through it. No matter even the repeated RREP is used. Updating of RREP should be done when node is used more than once. Each routing table entry contains the following data.

1) Destination node
2) Next hop
3) Number of hops
4) Destination sequence number(for route freshness)
5) Active neighbors for the route
6) Expiration timer for the routing table entry.

VII. ADOV THEORITIC ALGORITHM

1) **Initialization :** Should give source to destination address. If no path assigned it will find secure route by route request (RREQ).
2) **Storing :** Saves the path specified or will search for neighbor node for network availability or will search for fresh route and stores in routing table.
3) **When Intermediate node generates RREP and sends to Next Hop Node:** Table contains entry for each neighbor and check which data is sent and which data is received from neighbor. If reply comes back collects IP addresses of all nodes and Updates route entry for destination and table is updated.
4) **Identifying and removing intruder:** Get the entry form routing table if destination sequence number is greater than source sequence number then it is discarded from routing table.
5) **Node selection :** pick the entries from routing table according to destination sequence number, select node ID with highest destination sequence number.
6) **Repeating above steps until packet is reached to destination:** Call RREP method of default AODV Protocol. This show malicious node is identified and removed.

   (1) The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process. (2) No delay = malicious node are easily identified

   (3) No modification is made in other default operations of AODV Protocol.

   (4) Better performance produced in little modification .

   (5) Less memory overhead occurs because only few new things are added.

   Below shows the co-operative routing algorithm in detail.

Algorithm to prevent cooperative black hole attack in MANETs

Notations :

S: Source IN: Intermediate Node

D: Destination NHN: Next Hop Node

FRq: Further Request FRp: Further Reply

Trustable Node: The node through which the S has routed data

DRI: Data Routing Information

ID: Identity of the node

```
S broadcasts RREQ
S receives RREP
IF (RREP is from D or a trustable node) {
    Route data packets (Secure Route)
}
ELSE {
    Do {
        Send FRq and ID of IN to NHN
        Receive FRp, NHN of current NHN, DRI entry for
        NHN's next hop, DRI entry for current IN
    IF (NHN is a trustable node) {
        Check IN for black hole using DRI entry
        IF (IN is not a black hole)
            Route data packets (Secure Route)
        ELSE {
            Insecure Route
            IN is a black hole
            All the nodes along the reverse path from IN to the node
            that generated RREP are black holes
        }
    }
    ELSE
        Current IN = NHN
} While (IN is NOT a reliable node)
}
```

VIII. SECURITY ISSUES

Many security issues need to followed in order to give reliable and secure adhoc network. The following methods detect, prevent and respond to security issues.

1) **Availability :**Ensures the network is made available all the time and should be available to all authorized users, the attack can be done at stage in MANET.
2) **Confidentiality :** The network should be such that data should be assigned only to authorized users not to unauthorized users.
3) **Integrity :** Ensures that is not interrupted nor altered in middle before reaching to destination. The data may get corrupted because of intruder attack.
4) **Authentication :** It enables anode to ensure the identity of the peer node it is communicating with. No authentication leads to loss of sensitive information.
5) **Non-repudiation :** Making use of compromised nodes. If A is sending request to B, where B is malicious, Non repudiation helps to compromise B node and make B node to receive data and convince other nodes that B node is compromised.

IX. CONCLUSION AND FUTURE ENHANCEMENT

We have discussed black hole attack in detail with respect to attack on specified node and also in co-operative attack. We have used encryption and decryption methods to over come the specified attack and ADOV routing algorithm to overcome the co-operative attack. By surveying on black hole, if we are capable to prevent attack on nodes, time complexity can be minimized/reduced, performance will be high. As future enhancement more algorithms need be introduced and the same can be implemented to over come black hole attack.

REFERENCES

[1] Samba Sesay, Zongkai Yang and Jianhua He, "A Survey on Mobile Ad Hoc Wireless Network", Information Technology Journal 3 (2): 168-175, 2004.

[2] Amandeep and Gurmeet Kaur, "Performance Analysis of Aodv Routing Protocol in Mantes", International Journal of Engineering Science and Technology, p.p 3620-3625, 2008.

[3] Charles E. and Elizabeth M., "Adhoc on Demand Distance Vector Routing", p.p 1-11.

[4] Irshad Ullah ,Shoaib Ur Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols" in Thesis no: MEE 10:62 in June, 2010.

[5] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007.

[6] Ankita singh Kushwah, Krittika Khator and Atul Singhal, "A Review on Prevention and detection Techniques for Black hole Attack in Manet", ISSN: 2319-6327, Vol. 2, No. I (2013), pp. 24-27.

[7] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc MobileWirelessNetworks",IEEEPersonalCommunications, Vol. 6, No. 2, pp. 46-55, April 1999. http://users.ece.gatech.edu/~cktoh/royer.html.

[8] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Ad Hoc Networks", Proc. 6th Annual Int‟l.Conf. Mobile Comp. and Net, Boston, MA. pp. 255-265. August 2000.

[9] S. Buchegger, C. Tissieres, and J. Y. Le Boudec. A testbed for misbehavior detection in mobile ad-hoc networks - how much can watchdogs really do. Technical Report IC/2003/72, EPFL-DI-ICA, November 2003. Available on:citeseer.ist.psu.edu/645200.html.

[10] S. Buchegger and J. Y. Le Boudec. A robust reputation system for mobile adhoc networks. Technical Report IC/2003/50, EPFL-DI-ICA, July 2003.

[11] "Cooperative and Reliable Packet-Forwarding On Top of AODV", www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005 .

[12] Tamilarasan-Santhamurthy;"A Comparative Study of Multi-Hop wireless Ad-Hoc Network Routing Protocols176-184.ISSN(online):1694-0814.

[13] P. K. Sehgal & R. Nath, "A Encryption Based Dynamic and Secure Routing Protocol for Mobile Ad HocNetwork", International Journal of Computer Science and Security (IJCSS), Volume (3) : Issue (1) 16

[14] A.Patcha and A.Mishra, Collaborative security architecture for black hole attack prevention in mobile ad hoc networks, Radio and Wireless Conference, 2003. RAWCON '03, Proceedings, pp. 75-78,10-13 Aug. 2003.