ISSN No:-2456-2165

Security Scheme for MANET Based on Echoing and Path Changing

J. Nithyapriya, R. Anandha Jothi
Research Scholar, Department of Computer Applications,
Alagappa University, Karaikudi, Tamilnadu.

V. Palanisamy
Professor and Head, Department of Computer Applications,
Alagappa University, Karaikudi, Tamilnadu.

Abstract:- Ad hoc networks are those that have mobile nodes. They do not have a static topology and dynamically changing by nature. Mobile Ad hoc Networks (MANET) do not have a centralized administrator too. For this nature MANET is much prone to security attacks such as DoS, Eavesdropping, black hole, gray hole, worms etc. In this paper, we have a glance on all types of attacks on MANET and we provide a scheme which focuses on security of MANETs by echoing and path refreshing by detecting black holes. We also introduce an algorithm for the same based on echoing of neighboring nodes. The proposed algorithm is successfully attempted to detect and remove black holes in MANETs.

Keywords:- *MANET, Byzantine attack, black holes, worms.*

I. INTRODUCTION

Ad hoc networking somewhat differs from traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in the networks. Wireless nodes network among themselves even when the access to the internet is unavailable. From instant conferencing between notebook PC users to emergency and military services that must perform during harshest conditions ad hoc helps. Ad hoc networks have a unique set of challenges. i)Ad hoc networks face challenges in secure communication. The resource constraints on nodes like power consumption in ad hoc networks limit the cryptographic measures that are used for secure messages. ii) Mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. ii) Static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like DoS (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information. This paper talks about various byzantine attacks on MANETs consequently we also put forth an algorithm that better detects and solves the black hole attack on MANET.

II. VULNERABILITIES OF MANET

The unavailability of security boundary in MANETs makes it a treat to the intruders. The notable attacks are eavesdropping, active interfering and leakage of secret information, data tampering, message replay, message contamination and Denial of Service. Most of the attacks on MANET are by the compromising nodes. Attacks by the nodes inside the network are more dangerous than the nodes outside the network. These attackers gain control over the entire network by some unrighteous means and slowly corrupt the network using the compromising nodes which reside inside. This is highly dangerous as said. A good example for this is byzantine failure. In that the nodes from inside acts as if they are legitimate nodes and they seemingly behave well. But they silently smell the flaws and inconsistencies of the routing protocol and undetectably destroy the routing information then misroute the packets to a non-existent link, provide fake link state information or create network traffic. Since MANETs do not have a centralized administrator called server, it is tedious to manage traffic of the entire network. MANETs are also behaving benign to the attacks for the same reason of not having a server. Power consumption is also a notable issue of MANETs due to which complex cryptographic schemes cannot be applied.

- *Attacks In Ad Hoc Networks*

Among the numerous attacks there are two main classifications [1] such as Internal attacks and External attacks. In external attack, the attacker aims to cause congestion, provides fake routing information by the way disturbs nodes from gaining services. In internal attack, the attacker gains control over the network by impersonation as a new node or by a compromising node inside to execute its malicious behavior. There are also two other categories of attacks namely attacks on routing protocols and attacks targeting packet delivery. Attacks on routing include network partition; route loop resource deprivation and route hijack [1]. Attacks targeting packet delivery try selfishness and denial of service.

III. RELATED WORKS

Here in our current work we try to resolve the byzantine attack black holes. On the way we see some related works. The goal of byzantine attack is to reap the benefit of the existent network by spending its own resources for it. In MANETs the following types of byzantine attacks can occur: Black hole attack, Gray hole attack, Flood Rushing and

Wormhole attack [1]. Black hole is a basic byzantine attack, the intruder stops forwarding data packet still participates in routing [6]. Gray hole is a special type of black hole attack where the intruder selectively drops some packets not all [9]. Wormhole attack needs the co operation of more than one node. There will be a canal formed among the participating nodes which is called the worm. And any packets travelling through this tunnel will be colluded [1]. Ample number of researches is going on detecting black holes. There are also schemes that offer cryptographic techniques for this false node detection. But those techniques are found to be complex and energy consuming [8]. We propose an algorithm to detect the black holes in a quick, simple and energy efficient manner.

IV. PROPOSED WORK - ECHOING ALGORITHM

Our proposed work is based on packet delivery ratio, reconfiguration of the network when an intruder is detected, echoing of every node participating in transmission and time set for every transmission.

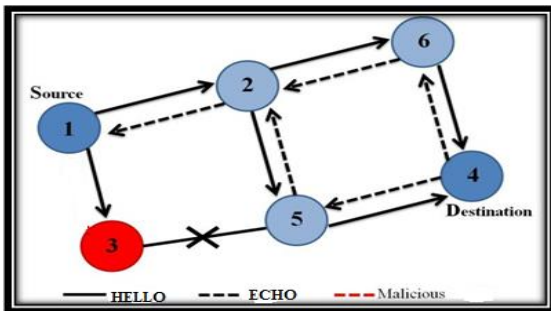

Fig 1:- Demonstrating echoing

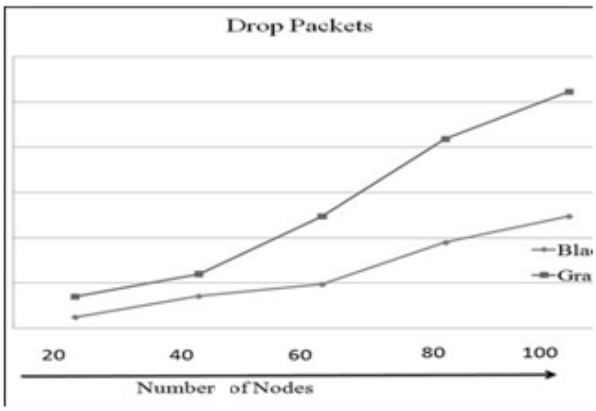

Fig 2:-Packet drops due to black hole and worm hole

The algorithm is formulated as reconfiguring MANET whenever a node enters in or a node exits from the network. Echoing is checked by the corresponding predecessor node to ascertain the successor node for transmission. If more than one neighbor is there one hop away, an arbitrary selection of a neighbor is done. However the other nodes' information would also be saved by the predecessor node for future use. When problems like node failure, unexpected node exit or node misbehavior happens this information will be useful.

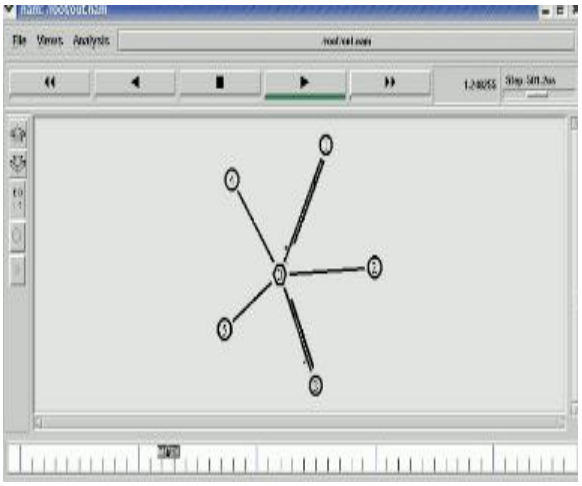

Fig 3:- Replying neighbor nodes

This scheme is based on the fact that the uncooperative node will surely not echo. The response is called echo. That way it is easy to omit the node from the transmission path.

➢ *Algorithm EREFPA*

Input: The current scenario of MANET with n nodes
Output: Familiar path with m< n nodes

//EREFPA-Echoing and Renewing Familiar Path
//n- Number of nodes available in MANET

- *STEP 1: HELLO MESSAGING*

```
for i-> 1 to n do
{
// Sending hello messages to neighbors that requests their IP
// The reply is known as echo and that would be saved by the requesting node
a[i] = neighboring IP(s)
}
```

- *STEP 2: EXTRACTING TRUE NODES*

```
for j -> 1 to m do
{
//m- number of echoing nodes
j-> j+1 // passing packets through the echoing nodes
}
```

- *STEP 3: GO FOR THE FAMILIAR PATH FOR EVERY TRANSMISSION*

// For every transmission between a sender and a receiver a Familiar Path (FP) is chosen

- *STEP 4: SETTING TIME FOR TRANSMISSION*

```
// TTT-Total Time for Transmission, TT – Time Taken
For k -> 1 to m do// source to destination
{
TT[k] =TT[k] +TT[k+1]
}
If TT [k ] > TTT
```

//Interrupt current transmission and check the path so far crossed
//do steps 1 and 2 continue step 3

- *STEP: 5 Renew FP and resume transmission*

According to this algorithm, every node counts the amount of time taken by all the previous nodes ie. TT. TTT is the total predicted time of the message to reach out the destination. If TT at any node reaches the total time TTT, the entire path the packet so far crossed will be checked and the delaying node would be removed.

V. RESULT AND DISCUSSION

Features	Justification
Time	Offering the familiar path for each transaction makes the scheme quick
Complexity	Simple. Less computational complexity.
Efficiency	Easy way of detecting non cooperative nodes. No severe damage caused like message tampering because of early detection
Energy consumption	Very low compared to cryptographic schemes

Table 1

VI. CONCLUSION

Ample number of researches is going on detecting black holes. There are also schemes that offer cryptographic techniques for this false node detection. Here in our current paper we propose a system which is strongly based on echoing. This algorithm detects black holes in an efficient way. The theoretical results indicate that the EREFPA works well and has the potential to detect the black holes and also it provides alternate to change the path of transmission by previously saving the neighboring node details. That way it is advocated to be a quick scheme. In future the scheme can be enhanced to detect gray holes as well the worm holes.

REFERENCES

[1]. "Analysis of Byzantine attacks in Ad hoc networks and their mitigation, Shabir Sofi, Eshan Malik, Rayees Baba,Hilal Baba,Roohi Mir, ICCIT, 2012.
[2]. Webopedia, An Internet Dictionary, http://www.webopedia.com./.
[3]. P.Yauh and C.J.Mitchell, "Security vulnerabilities in Ad hoc networks".
[4]. S.Seth and A.Gangotia, "DoS and detection methods in wireless sensor networks".
[5]. M.Medadian et al., "Routing misbehavior in MANETs", First Asian Himalayas International Conference, Nov.2009.
[6]. Karlof et al."Secure routing in wireless sensor networks", Elsevier, 2003.
[7]. "An Approach: False Node Detection Algorithm in Cluster Based MANET", Gaurav, Naresh Sharma Himanshu Tyagi , Volume 4, Issue 2, February 2014 ISSN: 2277 128X ,International Journal of Advanced Research in Computer Science and Software Engineering.
[8]. "Novel Security Scheme for Wireless Adhoc Network", Abhijit Das Soumya Sankar Basu Atal Chaudhuri, 978-1-4577-0787-2/11 IEEE 2011.
[9]. Improved Adaptive Acknowledgement Scheme for Intrusion Detection System in Adhoc through SCADA by G.Dharma prabha et al., IJCSITS, December 2014.
[10]. "Acknowledgment-Based Secure authentication Method for Manet" by Dr.J.Subash Chandra Bose et al.,IJIRCCE, March 2014.