Security Issues and attacks in Network Layer On Mobile Ad Hoc Network

Isha Bhan [1], Prof. P.Prasanna [2]

[1]**M.Tech Student,** [2]**Associate Professor**

[1, 2] **Department of Computer Science Engineering**

[1.2] **P.E.S. College of Engineering, Mandya-571401**

Abstract- Mobile ad hoc networks (MANET) are a primary requirement for the establishment of communication. CBDS has a reverse tracking mechanism which checks all the stated issues. CBDS outperforms among nodes. The malicious nodes may lead to security concerns such as it may disrupt the routing process. Since it is a Manet, it can change its scale anytime so preventing or detecting the malicious node becomes a challenge. This paper tries to solve the issue by applying a dynamic source route mechanism which is also referred as cooperative bait detection scheme (CBDS). CBDS technique integrates the advantage of both proactive and reactive mechanisms much better than the previous mechanisms like BFTR, 2ACK.

Keywords-CBDS (Cooperative Bait Detection Scheme), DSR (Dynamic Source Routing), MANET (Mobile Ad Hoc Network), gray hole attack, black hole attack.

1. INTRODUCTION

With the emerge of mobile technology, wireless communication is becoming more popular day by day. MANETs are self-constructing mobile networks in which each device is free to move in any direction

.Ad hoc networks are useful in disaster recovery situations. Ad hoc network are useful in conferences where people participating in conference can form a temporary network without engaging in services of any pre-existing network [1]. Fig.1 shows the structure of MANET and Some of the vulnerabilities in MANET's are as follows

- No predefined boundary- Since there is no predefined boundary so the nodes are free to join and leave the wireless network. Attacks can be like DOS (Denial of Service), Eavesdropping etc.

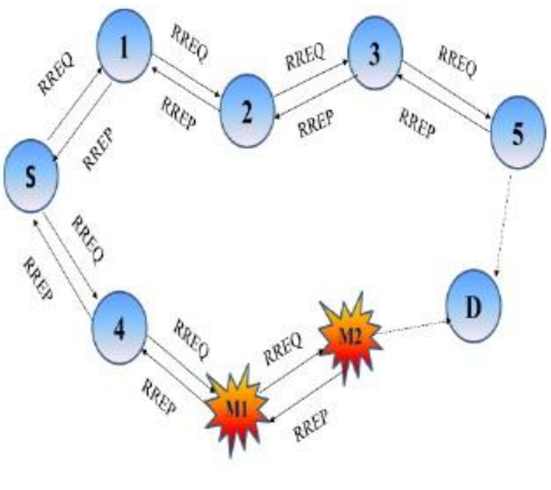

Fig1: Structure of MANET

- Limited Energy Source-Mobile nodes depend upon battery power for their operation. Major problem arises that the target nodes remains busy in handling all the traffic and hence consumes lot of power. Attacks have been classified into two categories, namely active and passive. Active attacks-Active attacks include like the information modification or information interruption. Passive attacks- Passive attacks are obtained by jorly focus on gray hole and changing the vital in-formation without disrupting the communication

- Many research works have focused on the security of MANETs and most of them deal with the prevention and detection schemes to combat the malicious node. Black hole attack occurs when a node transmits the malicious node, saying that it has the shortest route to the destination .It forges the Route Reply packet to falsely claim that it is the shortest route to the destination. This paper involves ma black hole attack.

2. RELATED WORK

Chin-Feng Lai et al, IEEE [2014]. In this paper the author [1] tries to solve the issues of black hole and gray whole attacks caused by malicious nodes by designing a Dynamic Source Routing (DSR) mechanism known as Cooperative Bait Detection Scheme (CBDS). It combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique. Cooperative Bait Detection scheme is proposed to detect malicious nodes in Manet for the gray hole and black hole at- tacks. [2]

A number of algorithms have been formulated to overcome the security issues related to the malicious nodes. Several security schemes which are there now to deal with the above described attacks.

- 2 ACK- In this scheme 2 hop acknowledgement packets are sent in opposite directions of routing path to indicate that data packets have been successfully received. This scheme belongs to the class of proactive schemes and hence produces the routing overhead.
- BFTR (Best Fault Tolerant Routing)-BFTR uses end to end acknowledgment to monitor the quality of routing path to be chosen by the destination node The main drawback of BFTR lies in the fact that the malicious node may still present in the newly chosen route.
- Cluster based intrusion detection-In this approach the whole network is organized as a set of clusters such that each node is number of one or more clusters. This approach leads to the complexity of networks.

3. PROPOSED SYSTEM

In the proposed work, we develop a new technique named ECBDS by enhancing the previous technique called CBDS. The main idea behind CBDS is that each node sends a route request signal (RREQ).The adjacent or the neighbor node receives the RREQ signal and then replies with a RREP signal. Then if there is any reply RREP from the destination then the reply packet verifier checks the previous alarmed malicious node list and malicious node detected list and rejects them with the help of packet rejecter and broadcasts alarm to other nodes. When all the nodes have updated their list of malicious nodes, the detected node is blacklisted and further communication to the node is stopped. Then it checks that whether the packet delivery ratio drops to the set threshold limit or not. If it has dropped, then the source node randomly chooses the cooperative bait address of the one hop neighbor to bait malicious node and sends the RREQ. But if there is any reply of any other node except x, reverse tracing program is triggered and test packets are sent and message is re- checked to detect the malicious node. Data flow diagram of the proposed system is shown in Fig.2.

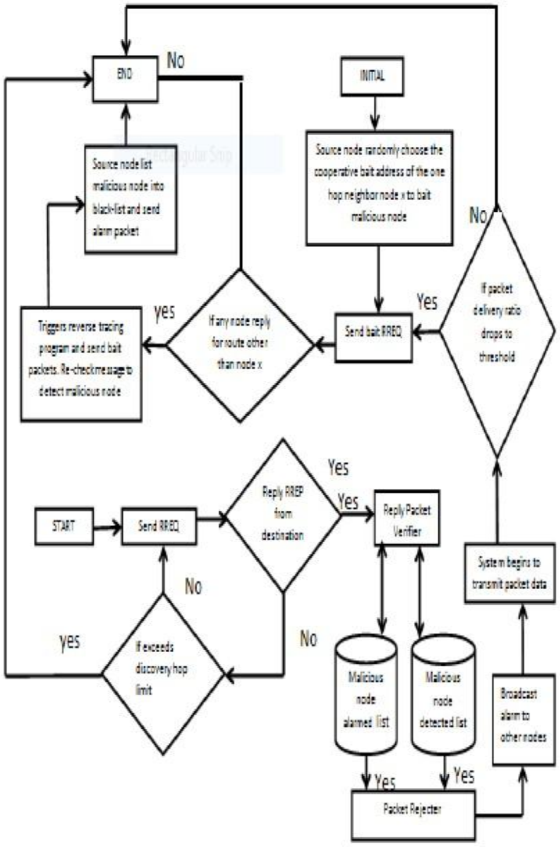
END
No
INITIAL
Source node list malicious node into black-list and send alarm packet
Source node randomly choose the cooperative bait address of the one hop neighbor node x to bait malicious node
No
If packet delivery ratio drops to threshold
Yes
yes
Triggers reverse tracing program and send bait packets. Re-check message to detect malicious node
If any node reply for route other than node x
Send bait RREQ
Yes
Yes
START
Send RREQ
Reply RREP from destination
Reply Packet Verifier
System begins to transmit packet data
No
yes
If exceeds discovery hop limit
No
Malicious node alarmed list
Malicious node detected list
Broadcast alarm to other nodes
Yes
Yes
Packet Rejecter

Fig2. Proposed system data flow diagram

4. FUTURE SCOPE

The networking opportunities for MANETs are intriguing and the engineering trade-offs are many and challenging. This paper presented a description of ongoing work and there can be a lot done to this area. There is a need for standardized, secure and interoperable routing for manets. This paper provides only node security. Data security should also be included so that the network works properly. The future holds the possibility for deploying inexpensive, IP internetworking compatible solutions to form wireless routing fabrics. A single variation in throughput and end to end delay is observed in case of CBDS which re-mains the area of further improvement.

5. CONCLUSION

In this paper, we have analyzed the security threats an ad hoc network faces. On one hand, the security sensitive applications of an ad hoc network requires high degree of security. Ad hoc networks are very vulnerable to threats. Therefore there is a need to make them more secure and robust. ECBDS is a costly prevention technique used to prevent wireless system from attacks like black hole at-tack. Due to its cost it is mandatory to check that it is effective for other attacks too. End to end delay has reduced as data reaches to receive without communication with malicious node.

6. REFERENCES

[1] Chin-Feng Lai, HanChieh Chao, Jian-Ming Chang, Isaac Woungang, and Po-Chun Tsou, Member, IEEE. Defending against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach.

[2] Babak Hossein Khala, Hamidreza Bagheri, Marcos Katz, Mohammad Javad Salehi, Mohammad Noor mohammadpour, and Seyed Mohammad Asghari Pari ”A Self Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks”.

[3] Nicklas Hedman and Tony Larsoon “Routing protocols in wireless ad-hoc networks”.

[4] Durgesh Kumar Mishra (Acropolis Institute of Technology and Research, Indore, India). Mahakal Singh Chandel (Arjun Institute of Advaced Studies and Research Centre, Indore, India), Rashid Sheikh IEEE 2010. Security Issues in MANET: A Review.

[5] Bing Wu, Jie Wu, Jainmen Chen, Mihaela Cardie “A survey on attacks and countermeasures in Mo-bile Ad Hoc Networks”.

[6] Prof Ravindra Rathod, Prof. M D Ingle, Prof R M Kawale “Detecting of routing misbehaving links in MANET by 2ACK scheme”.