International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
National Conference "MOMENTUM-17", 14th & 15th February 2017
Available online at www.ijrat.org

Cross Layer Design for Routing and Security Attacks in Multi-Hop Wireless Networks

Mr. Shivaji R. Lahane
Assistant Professor, Computer Engg. Department
GES, R. H. Sapat CoE, MSR, Nashik (MS)
shivajilahane@gmail.com

Abstract: The mobile ad-hoc networks (MANET) having features like self organizing, working as router and dynamic topology. OSI model initially introduced for wired networks, which not able to give good results in multi-hop wireless networks. In MANET, nodes are limited resources like bandwidth, battery power and storage space. MANET is vulnerable of different types of attack in each layer. Security is main issues in Mobile Ad-hoc Network. While studying need to give more attention on attacks within MANET, many attacks such as Blackhole attack, Flooding attack, jamming, Wormhole attack, traffic monitoring and analysis, DoS etc. and what can be done as countermeasures against them.

Keyword: DoS attacks, Mobile Ad-hoc Networks, Security, Routing Protocols

1. INTRODUCTION

MANET are multi-hop wireless network. It is dynamically formed amongst groups of mobile users having wireless network. It has different characteristics such as lack of centralized administration, distributed cooperation, changing topology and requires no existing infrastructure. Without server or base station node connect directly together. Mobile nodes are communicated with each other within the radio range through wireless links. There are many issues in MANET such as routing, power management, bandwidth management, and radio interface and security. Many more applications of mobile ad hoc networks such as tactical networks, emergency services, commercial, civilian environments, home enterprise networking, education, entertainment etc. Security services for MANET are authentication, availability, confidentiality and integrity to the mobile users. The security solution should provide complete protection to the entire protocol. Security in MANET is in different layers. MANET is suitable for applications such as military battlefield, emergency rescue etc.

2. ROUTING PROTOCOLS

Routing is a function that connects a link from source to destination in the network [1, 2]. Routing concepts involves two activities: finding optimal routing paths and send the packets through on internetwork. Three general categories of routing protocols are table driven, on demand and hybrid routing protocols.

2.1 Proactive (table-driven) Routing Protocol:

In this Mobile nodes periodically broadcast their routing information to the next node. Each node needs to maintain the records of the adjacent and reachable nodes with a number of hops. Nodes have to evaluate their neighborhood as per the network topology change. Table driven routing protocols are DSDV and OLSR protocol.

2.2 Reactive (On-demand) Routing Protocol:

These are not maintaining routing information if there is no communication. If a node wants to transmit packet to another node then the protocol finding for the route in on demand and establish the connection in order to send and receive the packet. The on demand routing is simply started when nodes desire to send data packets. On-demand routing protocols are AODV and DSR protocol.

2.3 Hybrid Routing Protocol:

The hybrid routing protocol combines the advantages of both to overcome the defects. Hybrid routing protocols are designed as a hierarchical network framework. Table driven routing is employed to completely collect the unfamiliar routing information and using the on demand routing to maintain the routing information when network topology changes. Hybrid routing protocols are ZRP and TORA.

3. SECURITY LAYER ATTACKS ON ROUTING PROTOCOLS

General attacks are threats against physical, MAC and network layers that function for the routing mechanism of the MANET [3, 4 and 5]. There are two basic types of attacks in MANET: passive and active attacks.

3.1 Passive attacks:

It does not disturbed normal activities of network. Detection of passive attacks is difficult to identify because the network operation is normal. The mechanism for solving the passive attack uses encryption of the data being sent. It is difficult for the attacker to get information from the data. Passive attacks are traffic analysis, eavesdropping, monitoring.

3.2 Active attacks:

In this type of operation, an attacker actively participates and disrupts the normal operation of the network services. A malicious node can create an active attack by altering information in the mobile ad hoc networks. It degrades the network performance. Forms of active attacks are jamming, spoofing, modification, replaying and DoS. Active attacks are classified into as internal and external attacks. Internal attack nodes are the critical part of the networks. External attacks nodes are not part of the network.

3.3 MANET physical layer Attacks

Jamming/Interception, Eavesdropping: As the approach by Jamming/Interception, Eavesdropping is to interfere the signal between two communicating authentic nodes, so the countermeasures against these attacks are oriented at the changing or "masking" the signal in some way. The first countermeasure, which can deal firmly with the eavesdropping attack and minimize the risk of interception, is the implementation of the so called FHSS technology. FHSS is a method for transmitting/receiving a signal, using different frequencies, which are changed at fix time intervals. In other words it is a way to encode the signal, and both the receiver and sender have to be synchronized, using the same "random" frequency pattern. Though the signal is sended over a single channel, it appears to be an obscure duration impulse noise for eavesdroppers, and the risk of interference is reduced because of the multi-frequency pattern [2]. The second countermeasure is the implementation of DSSS technology. The original Bit-sequence or the data input is concealed using spreading code in such way, that one original data bit equals to multiple bits in the transmitted signal [5]. (Spreading code bits XOR Data input bits = Transmitted Signal)

3.4 MANet data link layer attacks

Traffic monitoring and analysis: Traffic monitoring and analysis is not an actual attack, but an instrument to prepare such one. Via traffic monitoring and analysis an intruder can receive information about the participating users within the network e.g. who is communicating with whom, how often, for how long, as well as find out what are their communication role e.g. which applications by particular node are using bandwidth, for how long etc. Having such specific information, for an infected node is easier to choose how to attack a victim node, aiming efficiency. For all these reasons the traffic monitoring and analysis has to be considered as a massive threat.

3.5 MANet network layer attack

1. Flooding
2. Blackhole
3. Link spoofing
4. Wormhole

3.5.1 Flooding attack: In this attack, attacker selects many IP addresses which are from outside of the networks [2]. Attacker transmit RREQ message with such IP address. Nodes cannot give response RREP packets for RREQ. So reversed link is in the route table will used for longer time. Attacker can select any IP address. Attackers are continuously sending RREQ packets without waiting for RREP, thus flooding the network. The complete bandwidth is utilized and the resource of nodes is exhausted at the same time. With the increase the flooding frequency and the number of attack nodes, the network performances drop. Fig.1 shows the RREQ flooding attack, attacker node 'A' sending route request message to all nodes.

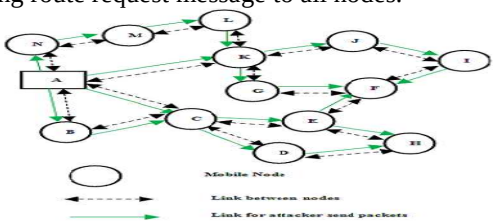

Fig.1 Flooding attack

3.5.2 Blackhole attack: It is kind of DoS attack where malicious node can attract all packets by pretending shortest route to the destination [12, 13]. It drops all traffic destined for that node when traffic is received by it. The effect of this attack completely degrades the performance of the network because the destination node never receives any information from the source. The access to the information is denied.

3.5.3 Link spoofing attack: Just in the opposite of the Blackhole attack, where the attacker try to intercept the data flow between two of its neighbors, by the link spoofing attack the attacker aims to intercept or stop the routing operations between two non-neighbor nodes. Using the OLSR protocol the infected node transmits a fake links to the two-hop neighbors of the target, and as a result the "victim" node selects it. As a countermeasure against the link spoofing attack there is a solution by which every single node within the network is driven to notify its two-hop neighbors and doing so all participants can acquire a view of the complete topology in "three-hop radius". So if a link spoofing attack is executed it will be simultaneously detected [5].

3.5.4 Wormhole attack: This is attack in MANET routing. Attacker is link by high speed off-channel link [7]. This is called wormhole link which is wired or wireless transmission link. Endpoint of wormhole link is facilitating with radio transceivers compatible with ad hoc networks to be attacked. Wormhole link attacks records the wireless data, forward this data and replays the packet through wormhole link. In the wormhole attack, nodes will not show the true picture of the network and there is effect on the decisions i.e. may be wrong. So wormhole link is unreliable. Fig.2 shows the wormhole path between two networks. X and Y are infected nodes which make wormhole path between two networks.

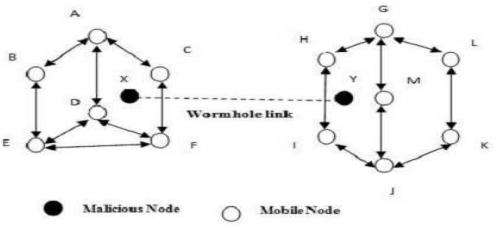

Fig.2 Wormhole attack

3.6 MANET transport layer attack

SYN Flooding: In this attack, an infected node sends a huge amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYN-ACK packets are transmit out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the reply of ACK packet. Without any reply of ACK packets, the half-open data structure remains in the victim node. If the victim node saves these half-opened connections in a fixed-size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer and the victim node would not be able to accept any other invalid attempts to open a connection. Normally there is a time-out associated with a pending connection, so the half-open connections will eventually expire and the victim node will recover. However, malicious nodes can simply continue transmits packets that request new connections faster than the expiration of pending connections.

3.7 Multi-layer attack

The attacks cannot strictly be associated with any specific layer in the network protocol stack. Multi-layer attacks are those that could occur in any layer of the network protocol stack. Denial of service and impersonation are some of the common multi-layer attacks. Here we will discuss some of the multi-layer attacks in ad hoc wireless networks.

3.7.1 Denial of Service attack:

In this, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. A DoS attack can be carried out in many ways. The classic way is to flood packets to any centralized resource present in the network so that the resource is no more available to nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of ad hoc wireless networks, there exist many ways to launch a DoS attack in such a network, which would not be possible in wired networks. DoS attacks can be launched against any layer in the protocol stack [1, 3]. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network

Some example of DoS attack:

Jamming: In this, the attacker initially keeps monitoring the wireless medium in order to find the frequency at which the destination node is receiving signals from the sender. It then sends signals on that frequency so that error-free reception at the receiver is hindered. FHSS and DSSS are two commonly used techniques that overcome jamming attacks.

Distributed DoS: DDoS attack is more severe form of Dos attack because, in this attack several adversaries that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network.

Resource Consumption/Vampire: In this, an attacker tries to consume or waste away resources of other nodes present in the network. The resources that are targeted are bandwidth, power battery and computational power, which are only limitedly available in ad hoc wireless networks. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes. Using up the battery power of another node by keeping that node always busy by continuously pumping packets to that node is known as a sleep deprivation attack.

4. IMPLEMENTATIONS AND RESULTS

4.1 Blackhole attack:

This attack has been launched using Network Simulator. Presently four nodes are considered 0, 1, 2 & 3 through which data goes from one node to another using AODV routing protocol. Node 0 is a malicious node and Node 1, 2 & 3 is honest nodes. Node 0 received all the data packets from other nodes, dumped that packet and dropped it for distraction of valid communication between honest users. Following Fig.3 & Fig.4 shows these results.

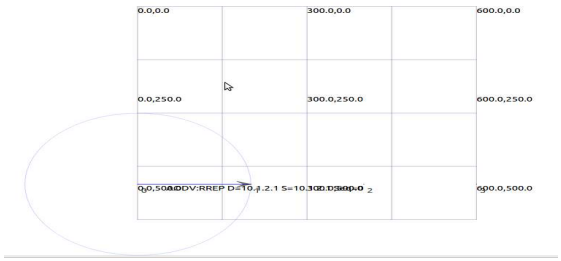

Fig.3 Topology of node

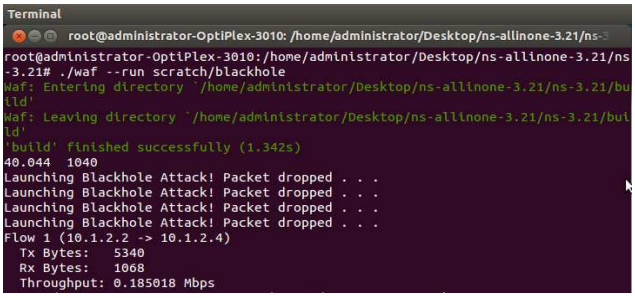

Fig.4 Launching Blackhole attack

Fig.4 shows Transmitted data is 5340 Bytes, Received data is 1068 Bytes and Throughput is 0.185018 Mbps which is very less.

4.2 Vampire attack:

In this system detection of vampire attack has been done by using simulation results. For detection of vampire attack we present simulation result in which number of nodes are considered through which data goes from one node to another. For authentication purpose login has been specified which is one part of identifying the user is honest or malicious. Following figure shows these results. In Simulation, 6 nodes have been considered for forwarding node from one to another. In Fig.5 data
forward from Node B to Node F.

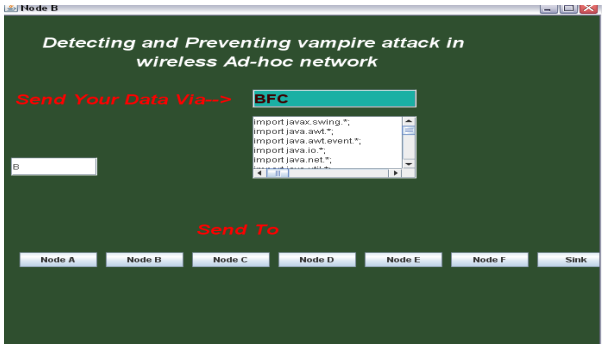

Fig.5 Node B to Node F

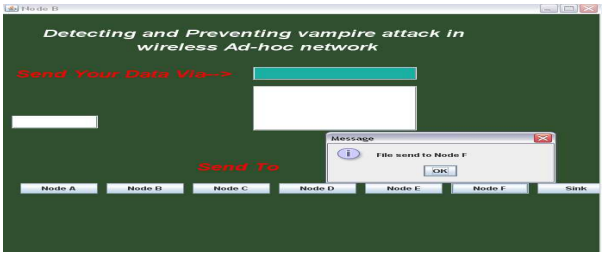

Fig.6 Node F to C

In Fig.6 data forwarded from Node F to Node C.

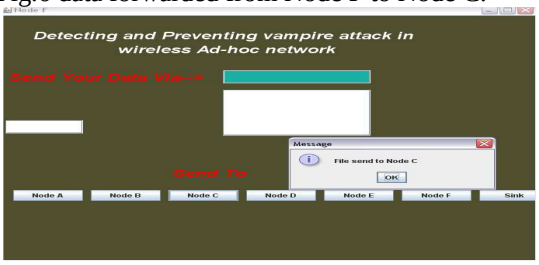

Fig.7 Node C to Sink

For detecting the vampire attack the data has been forwarded to sink which has been shown in Fig.7

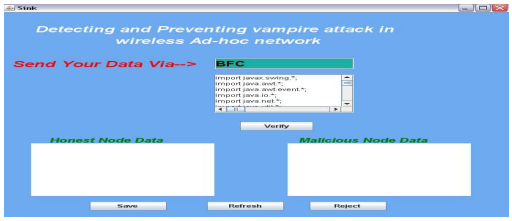

Fig.8 Verification

For detection the vampire attack the data has been verified which has been shown in Fig.8

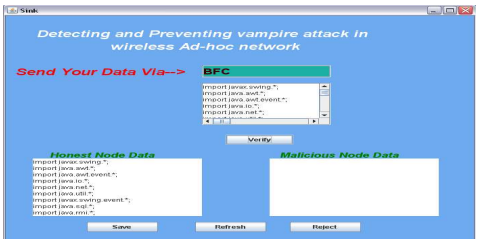

Fig.9 Detecting Honest Node Data

In Fig.9 The verification result has been shown in which the traverse data is honest node data.

In the above figures vampire attack has been detected, if the user is a valid user the path specified is traversing through three nodes. when the user is a malicious one who is trying to forward malicious data the path excedded upto six node in which the malicious data drain the energy of all the nodes in the network making the node lifeless.

5. CONCLUSION

We have discussed security issues related to integrated MANET, Internet and stand alone network. The proposed mechanisms until now have solved many security issues related to integrate MANET but they have not solved them completely. So, we can design a security mechanism by which we can minimize or completely remove many of those attacks.

Future Scope:

In future, system proposes to design a robust framework that uses minimal public key cryptography to avoid overload on the network and uses shared key cryptography extensively to provide security.

REFERENCES

[1] Rashid Hafeez Khokhar, Satria Mandala. *A Review of Current Routing Attacks in Mobile Ad Hoc Networks*. *International Journal of Computer Science and Security*, 12, 2008.

[2] Verizon Federal Network Systems, Wesley M. Eddy. *Defenses against TCP SYN Flooding Attacks*. *The Internet Protocol Journal*, 9(4), December 2006.

[3] Bounpadith Kannhavong, Hindehisa Nakayama, Yoshiaki Nemota and Abbas Jamalipura, "A survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications, October 2007.

[4] Panagiotis Papadimitratos and Zygmunt J.Has, "Secure Routing for Mobile Ad hoc Networks", In Procedings of the SCS Communication Networks and Distributed Systems modeling and Simulations Conferences, Computer Standards & Interfaces 31 (2009) 931-41.

[5] Kemal Bicakci, Bulent Talavi, "Denial-of-Service attacks and countermeasures in IEEE wireless networks", Computer Standards & Interfaces 31 (2009) 931-941

[6] Ejiro E. Igbesoko, Mona Ghassemian, "Simulation-based Security Analysis of a Reactive Ad hoc Routing Protocol under Black Hole Attack", 1st International Conference on communications Engineering, 22-24 December 2010, University of Sision Boluchesian.

[7] Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 48-2008.

[8] Hamieh A., Ben-Othman J., "Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution", Communications, 2009, ICC'09 IEEE International Conference.

[9] Yi-Chun Hu, Adrian Perrig, David B.Jhonson, "Rushing Attacks and Defence in Wireless Ad Hoc Networks," 2003, ACM 1-58113-769-9/03/0009.

[10] Satoshi Kurosawa,Hidehisa Nakayama,Nei Kato, Abbas Jamalipura, and Yoshiaki Nemoto ,"Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning method,"International Journal of Network Security ,Vol.5,No.3,P.P338-346,Nov.2007.

[11] Tamilselvan L, Sankaranarayanan V (2007), "Prevention of Black Hole Attack in MANET," 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydeney, Australia, 27-30, August 2007.

[12] Jaishankar N, Saravanan R, Swamy K D, "A Novel Security Approch for Detecting Black Hole Attack in MANET", International Conference on Recent Trends in Business Administration and Information Processing, Thiruvanthapuram, India, 26-27,March,2010.

[13] Mistry N, Jinwala D C, ZAVERI M,

"Improving AODV Protocol Against Blackhole Attacks", International Multi Conference of Engineers and Computer Scientists, Hong Kong,17-19 March 2010.

[14] Zho Min, Zho Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", 2009 International Symposium on Information Engineering and Electronic Commerce.

[15] Tsou P. C, Chang J. M, Lib Y. H, Lin Y.H, Chao H.C, Chen J. L, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", 13th International Conference on Advanced Communication Technology, Phonix Park, Korea, 13-16 Feb 2011.

[16] Nishu Garg, R. P. Mahapatra, "MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, Volume 9, No.8,2009.

[17] Vaidya B., Jae. Young Pyun, Sungbum Pan, Nak. Yong Ko, "Secure Framework for Integrated Multipath MANET with Internet**"**. International Symposium on Applications and the Internet, Pages 83– 88, Aug. 2008.