VAMPIRE ATTACKS PREVENTION IN WIRELESS SENSOR NETWORK

VISHAL LOKHANDE [1], SANJAY D. DESHMUKH [2], SURENDRA T. SUTAR [3]
[1]PG Scholar, Department of Electronic & Telecommunication, Rajiv Gandhi Institute of Technology, Andheri (w), Mumbai, India.
[2]Assistant Professor, Department of Electronic & Telecommunication, Rajiv Gandhi Institute of Technology, Andheri (w), Mumbai, India.
[3]Assistant Professor, Department of Electronic & Telecommunication, Rajiv Gandhi Institute of Technology, Andheri (w), Mumbai, India.
Email:[1] lvmm21@gmail.com, [2] deshmukhsdrgit@gmail.com, [3] sforsurendra@rediffmail.com

Abstract – This paper will help in exploring the attacks on routing layers in ad-hoc network. These attacks disable the nodes from network or exhaust the battery power. Attacks which we are going to prevent are not limited to any specific protocol but depend upon the classes and their properties. From research point of view various attacks and their problems are listed in various papers. These attacks are not easy to detect and if we want to provide solutions to it then it is for limited attacks which can be one at a time. In this paper to ease these kind of attacks that are Dos, malicious node attack, directional antenna attack, Carousel attack and stretch attack a more effective protocol which is STL scheme is implemented that provably bounds the damage caused by attacks during the packet forwarding phase. This paper shows 4 to 5 nodes are connected in the network and then detection of attacks on nodes followed by their prevention. It provides more secure packet forwarding and power consumption of battery which is less than the existing one.

Index Terms - WSN, secure routing, wireless network, denial of services, packet transmission

I. INTRODUCTION

Wireless sensor network has advanced in developing and developed countries in terms of communication. WSN is divided in Ad-hoc network and MANET where MANET does not have fixed infrastructure. Every node in the network interchanges the information and forward packet to other nodes. In ad-hoc network the node are deployed in large area to monitor and collect the data of physical or environment condition and transmit it to base station for future processing. It is important to have proper way of communication in real time also a secured one. Wireless sensor network used in continuous connectivity, military application, health monitoring, structural monitoring and industries. Information is carried away from source to destination in secured manner to maintain whatever data is transmitted should be same as the one sent. In today's Wi-Fi network large number of nodes

are deployed and packets or information message is broadcasted to the nodes but it gets affected by various attack i.e nothing on beacon routing protocols, source routing, distance-vector, link-state and geographic as well as a logical ID-based sensor network routing protocol. This attack misleads the path of packet or data or sometimes will make packets to be in a loop until all the system gets crashed. To avoid such issues node verification is required when packets are forwarded in routing. To deal with these issues important steps are considered. In first case, we thoroughly calculate the existing protocols to routing layer and battery draining attacks also to ensure an authenticated and secure data transmission process. We find orthogonality relation between security methods to prevent attacks and those used to defend routing infrastructure therefore existing secure routing protocols do not protect against this attacks. Recent work on secure routing gives assurance that attacker not able to return invalid network path on basis of path detection, Also stated attacks do not affect or vary revealed paths, instead using protocol-compliant message and existing valid network paths. Wireless sensor node are exposed to various attacks like denial of attack, Carousel attack, retransmission of attack, Stretch attack, wormhole attack, sink hole, black hole, we provides way to detect, prevent and maintain packet delivery ratio, power consumption. As the sensor networks can also function in an ad-hoc manner the security goals includes both those of the traditional networks and goals matched to the unique limitations of ad-hoc sensor networks. The categorizations of security goals are as primary and secondary. The primary goals are well-known standard security goals such as Confidentiality, Integrity, Authentication (CIA) module and Availability. The secondary security goals are Self-Organization, Secure Localization, Time Synchronization and Data Freshness.

1.1 Motivation

Wireless sensor network when placed in remote location it is risk of various attacks for qualitative communication may be for wired or wireless source and destination must be secure from the undesirable interruptions. Example in mobile phones during communication noise is the interruption likewise in systems information is important that is shared between the users that can be affected by the adversary. It affects the system confidentiality, integrity and security when data is modified. Besides this it also increases the power consumption in the system leads to deplete the energy of systems. Today it is desirable to have secure packet forwarding or data transmission. The adversary tends packets to follow long root or unavailable to end users or with purposely introduced routing loops. One of the major problems of the network is consumption of energy of each and every node in the network will increase due to attack. As attacker sends packets in circle so it leads to delay in data transfer which is important parameter in any wired or wireless communication type. Here considering all this issues that caused by adversary need to be detected and prevention is required in the systems.

2. LITERAURE SURVEY

Wireless sensor network undergoes various attacks due to deployment in large area or in remote location where accessing every time is not easy. So previously researcher has given various methods for detection and prevention of this attack. K.Sivakumar and P.Murugapriya[4] proposed optimal energy boost-up protocol(OEBP) defines how to abolish the attacks in the system. It analyses and validates the routing table along with verifying various attacks which affect the system to become permanently inactivate. This attack consumes energy of nodes or battery power. This method monitors the node activities and provides quality of service.

Eugene Y. Vasserman[6] and Nicholas Hopper identified a single Vampire can increase network-wide energy usage by a factor of O

(N), where N in the number of network nodes. They discussed methods to ease these types of attacks, considering a new proof-of-concept protocol that provably limits the damage caused by Vampire attacks during the packet forwarding phase.

Sureka.N and Chandra Sekaran[7] proposed to eliminate the advisory attack energy level constraint algorithm proficiently identifies the malicious nodes from the network, by removing those affected nodes we can transform to secure network with authenticated data transmission. The graphical result represents the enhanced network performance with increased throughput rate and improved packet delivery ratio.

B. Umakanth and J. Damodhar[8] proposed a EWMA method that removes the attacks in the network and to bind the damage caused by these vampire types of attacks during the packet forwarding phase also mentioned about the energy consumption while transferring packets through multi hops.

T.Sathyamoorthi, D.Vijayachakaravarthy, R.Divya and M.Nandhini[9] described about the how to detect the malicious node in WSN using a simple and effective scheme proposed as Stop Transmit and Listen (STL). Each node in a network is having the built-in time limit to stop their transmission. After few seconds every node stops their transmission and listens for malicious actions. Malicious nodes are not aware of non-transmitting time. If this node sends or forwards the data in non-transmitting time, malicious node is caught by their neighbour nodes in the network.

3. EXISTING SYSTEM

In previous cases people worked on stretch attack and carousel attack different protocol is used to detect the attacks and difficulties associate with it but no one have specified solution for both detection and prevention simultaneously. They worked on different criteria like energy, packet ratio or security issues on a single attack. They worked on stateless or stateful protocols.

Attack on Stateless protocols

Stateless do not track any sequences and are random. It is unsynchronized type and at nodes they do not maintain or store any routing information.

Source routing are targeted by some attacks that are mention below-

1) Carousel attack- In this attack attacker from source side never let nodes to forward packets to destination instead it remains in loop and repeatedly traveling through same set of nodes creating loop. It increases the power consumption in the system due to same data is forwarded through nodes.

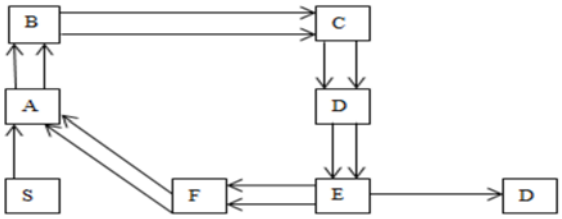

Fig.1 Dishonest route make to follow infinite loop before exiting and an honest route would exit the loop instantly from node E to destination.

2) Stretch attack- In this attack long route is followed from source to destination in forwarding phase instead mentioned this is due to adversary. Due to artificially long paths it takes more time to reach destination as well as energy consumption. Stretched path followed is S-A-B-C-D-E-D.

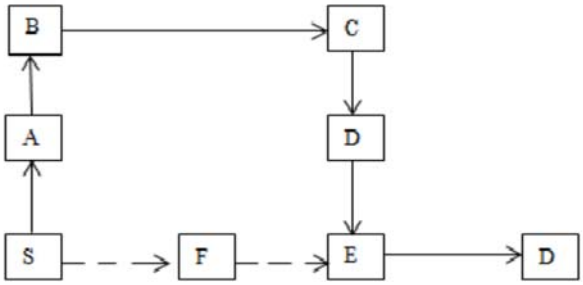

Fig.2. Malicious node is dark line while honest route is dotted. Destination is shared with the last link.

Fig.3 shows the existing system affected by the carousel and stretch attack where due to this attack packets are not reaching to destination.

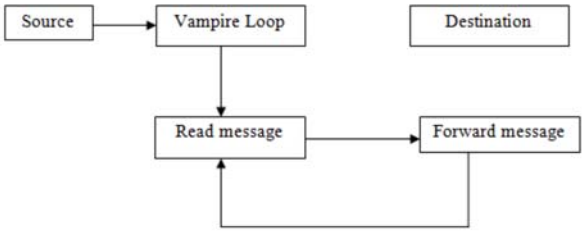

Fig.3. Existing system

Many algorithms and protocols are applied to detect and eliminate to avoid this attack. One is loop detection followed by PLGP which uses no backtracking property for advancing the data and if possible to find the shortest path. To some extend they are able to limit the parameter like packet overheads, energy consumption or throughput increased due to attacks.

3) Clean-Slate Sensor Network Routing (PLGP) –

Previous researcher used this method is with modified version of PLGP which undergoes two important steps that is topology discovery phase and packet forwarding phase.

In topology discovery phase nodes broadcast their identity certificate and public key. It forms tree like structure with groups and each node in the system identifies every nodes virtual address, public key and identity of certificate.

Packet forwarding Phase- In PFP, all decisions are made separately by each node. When a packet is received at node every forwarding event reduces the reasonable distance to target and next hope. Next hope information is calculated by means of the most significant bit of its address.

4. PROPOSED SYSTEM

This paper explores various attacks like denial of service, malicious node, Directional antenna, Carousel attack and Stretch attack are detected and then secure transmission of packet forward followed by prevention of attack is done. Due to prevention the parameters like power consumption that drains the battery also delay are reduced which is more when attack is performed and this sensor network are implemented in NS2 2.35 software to test the situation as in real time by considering all aspects eliminating the testing cost.

Proposed Architecture

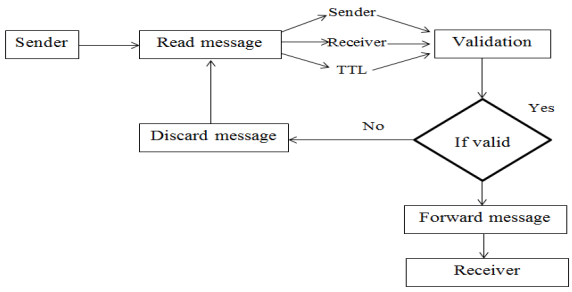

Fig.4. Proposed system

In proposed system it consists of existing and proposed system to work on detection and prevention of attack in the system. Secure packet forwarding as well as energy consumption is another important consideration. Fig.4 shows that when sensor nodes deployed in network due to nature of attack the flow of message not delivered to intended users and remains in a loop called Vampire loop. In Vampire Attack the message are routed through different node which are non-receiver nodes from where packets are advanced to next non- receiver node and as it follow same sequence in the system causing system to crash at the end.

In proposed system first sender broadcast the packets and each node will extract information like source address, TTL values and destination address. Every node validates information while forwarding that corresponding packet is arrived in routing table thus discard the packet means this packet made entry earlier. After validation the packets if it validates the condition then forward to next node until packet reached to destination other-wise the attack is performed packets are discarded this process is repeated until secure path is not formed.

The following function has been executed form source to destination during the attack in

forwarding phase. TTL value of message packet should be less than the threshold value of TTL of message packet other-wise packets are dropped.

A) Attack on Stateful Protocol

Stateful means every node will stores or maintains the records of routing tables follows the sequences and are synchronized type. It consists of two classes that is link state where it maintains information of up and down states of links in the system. Even when it is enabled or partially activated flooded by routing updates. Second is distance vector examples are Distributed Bellman-Ford or RIP also known as DSDV. In this node maintain the topology which consisting source, TTL or next hop count values to reach the destination. Stateful protocols consist of directional antenna attack and malicious node.

1) Directional antenna attack- In this attack attacker broadcast the packet randomly in any portion of the system or advancing packets to any nodes and restarting packets waste lots of energy. As packet sent decision is made independently by every node then attack on packet progress will be less. As it established a private communication channel so known as half wormhole attack. Packet leashes technique is used to prevent intermediaries.

2) Malicious discovery attack- It is similar to wormhole attack in which one malicious node in one system link to another system and draws all information to itself and make changes in the information. It affect the energy of system even they are not interested in communication.

B) DOS (Denial of service attack)- In Dos attacker perform attack on different node which may or may not be in transmission modifying them as per attacker choice and simultaneously send the data form all nodes to destination leads to jam the receiver to acknowledge which packet to accept it cannot differentiate honest one. As it is busy in acknowledge all packets it uses more energy and take more time to respond.

C) Secure TTL Scheme

We will use this scheme for all attacks for detection and prevention of various attack followed by secure packet transmission. In stretch attack adversary creates packet to forward via long loop leads to increase packet delay and energy like-wise carousel attack tends to follow infinite loop, Direct antenna attack broadcast packet to all nodes to overcome this we propose a routing table (TTL values) containing information of nodes. This helps in monitoring the previously arrived packets to node if arrived same discarded that leads to packet drop. So after validation if same packet is arrived new acknowledgment is sent for new packets to have secure packet transfer to destination removing that routing loop and choosing shortest path example carousel attack. Likewise other attacks are prevented and detected using this scheme and parameter energy consumption is reduced.

5. ALGORITHM

s- extract_source_address(p);
a- extract_attestation(p);
if(source sig is not verified(p)) or (empty(a) and not is neighbour(s))
then drop(p);
For each node in a do
Prevnode – node;
If(not are neighbours(node,prevnode))or
(not making_progress(prevnode,node)) then drop(p);
C - nearest next node(s);
P' – add(p);
If is_neighbour(c) then send(p',c);
Else forward(p', next hop to non neighbour(c));

AODV

1) When the source node has data packets in its routing cache table which route to the destination node, then source node directly sends data packets. Else the source node broadcasts a RREQ. Then, jump to 2).

2) When intermediate node receives a RREQ, it does the following operations. 1) If node is not the destination node, then jump to 3. Otherwise, jump to 2.

2) When first time RREQ is receive to the destination node, the node will put the value of RREQ's request for source address field and the value of RREQ's request for broadcast ID field into cache table, then establish the reverse route with its last hop count. Then, jump to 7. Otherwise, the destination node discards the RREQ. Then, jump to 8.
3) It looks for its broadcast ID cache table based on the values in the source address field and broadcast ID field of the RREQ. If there is entry which has the same values of request source address field and request broadcast ID field as those of the RREQ, jump to 6. Otherwise, jump to 4.
4) Since RREQ is the first time to receive for node, it will put the value of RREQ's request for source address field and the value of RREQ's request for broadcast ID field into cache table, then establish the reverse route with its last hop count.
5) If the node has a route to the destination node, then jump to 7. Otherwise, the node will randomly generate a delay and after the delay has arrived, the node broadcasts RREQ. Then, jump to 2).
6) Since the node received a RREQ already. The node discards the received RREQ which receive from its last hop node, establish no the reverse route with its last hop node. Then, jump to 8.
7) The node sends RREP to source node. The establishment of the route is completed.
8) The node does nothing.

6. SIMULATION RESULTS

In NS2 software we deployed sensor nodes allowed them to communicate with each other during that process attack is performed on nodes. So important tasks after attack is to detect and prevent. During the detection phase lots of packets are drop or delay occurs. To deal with that in prevention we provide secure packet transmission. Fig.5 shows the graphical representation of energy consumption versus number of nodes which shows that Carousel and Streach attack uses extra energy when attacker attacks the node and during prevention to most extent energy is saved. While directional antenna attack, Dos attack and malicious node attack consumes comparatively less energy compared with the Dos and carousel attack. During prevention phase using scheme consumption of energy is reduced to great amount which is main concern in any sensor node.

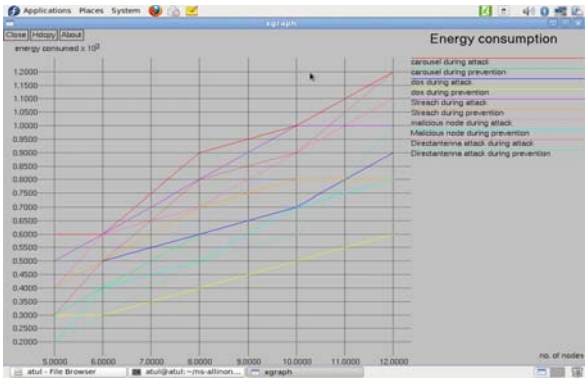

Fig.5. attack vs energy consumption based on number of node

Fig.6 & Fig.7 shows delay and packet delivery ratio when affected by attacker based on number of nodes. Carosuel and streach attack has large delay as it makes packets to remains in loop and to follow long path for long time. And same is case with packet delivery ratio for carousel and streach attack has lesser PDR. Dos, directional and malicious node has comparatively less delay comapred to other attack in detection phase as makes it unavaliable packet at destination or broadcast packets to all the node which are not in communication also tunnes the packet in another network. Directioanl, malicious node and Dos attack has relative less PDR during attack and during prevention we reduced the delay occurred in detction phase and has higher PDR in all attack using STL scheme.

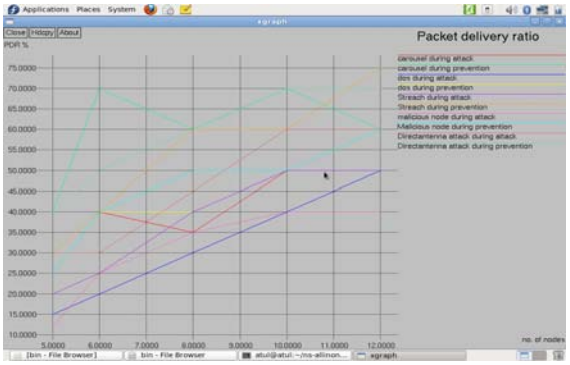

Fig.6. PDR vs attack

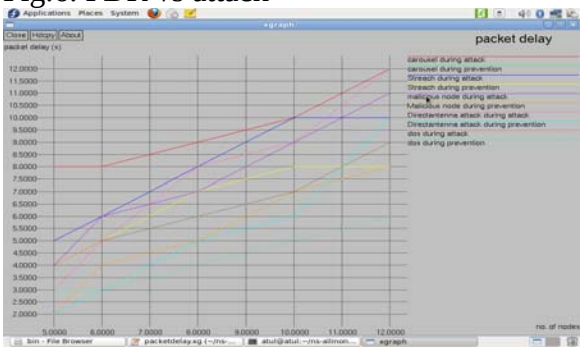

Fig.7. Delay vs attack

CONCLUSION AND FUTURE SCOPE

Due to distributed nature of wireless sensor network and deployment in hostile condition or remote location it is needed to provide efficient transferring of packets. But the network functioning gets affected by various attack which we considered in the system. Also we can classify this attack as energy draining attack where it depletes the node. we proposed a system which not only provide less energy consumption i.e. For Carousel attack to 45% and on an average to all attack 38-50%, less delay for Dos, carousel attack and other attacks on an average 30-45% respectively. We also maintain the PDR to provide secure packet forwarding in the system that is almost to 40% more which is less during attack as refer to Fig.6. Same graphs are plotted in ns2 using xgraph for delay, energy consumption. Hence we have implemented all 5 attacks random & manually. Future work advances by adding more attacks and their performance on different parameters like transmission range, increasing the traffic packets can be analyzed.

REFERENCES

[1] Lina R. Deshmukh and Amol D. Potgantwar "Prevention of Vampire Attacks in WSN Using Routing Loop", proc. IRF International Conference, February 2014.

[2] Shyamala Ramachandran and Valli Shanmugam "Detecting and preventing vampire attack in wireless sensor network" proc. Sensor & Ubiquitous Computing International journal of ad-hoc, Vol.3, No.4, August 2012.

[3] Babli Kumari and Jyoti Shukla "Secure Routing in Wireless Sensor Network" International journal in Computer Science and Software Engineering advance research, Vol.3, pp. 746-751 August 2013.

[4] K. Sivakumar and P.Murugapriya "Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks" proc. International Conference On Global Innovations In Computing Technology, Vol. 2, Issue 1, 2014.

[5] Thanmanam. P and Suguna. M "Detection of Vampire Attacks using Optimal Energy Boost-up Protocol in WSN's" IJETCSE, Vol. 8,issue 1, 2014.

[6] Eugene Y. Vasserman and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE Transactions on Mobile Computing**,** Vol. 12, No-2, 2013.

[7] Prof. S. Chandra Sekaran and Sureka.N "Securable Routing And Elimination Of Adversary Attack From Manet" proc. ICGICT**,** Vol. 2, Issue 1, 2014.

[8] B. Umakanth and J. Damodhar "Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks"proc. IJETT, vol. 4, Issue 8, 2013.

[9] T.Sathyamorthi, D.Vijayachakaravarthy, R.Divya, M.Nandhini "A Simple and Effective Scheme to find Malicious node in Wireless Sensor Network" International Journal of Research in Engg. And Tech.,Vol. 3, Issue 2, 2014.