INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

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, RGIT, Andheri (w), Mumbai, India.
2. Professor, Department of electronic & telecommunication, RGIT, Andheri (w), Mumbai, India.
3. Professor, Department of electronic & telecommunication, RGIT, Andheri (w), Mumbai, India.

Accepted Date: 21/06/2015; Published Date: 01/07/2015

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 secure packet and energy consumption 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.

Keywords: WSN, secure routing, wireless network, denial of services, packet transmission

Corresponding Author: MR. VISHAL LOKHANDE

Access Online On:

www.ijpret.com

How to Cite This Article:

Vishal Lokhande, IJPRET, 2015; Volume 3 (11): 92-104

PAPER-QR CODE

INTRODUCTION

With changing time may be for developing countries or developed countries communication is most important way of communication. Today it is important to have secured and real time delivery of operation on network so that proper way of communication should established. Ad-hoc network provides continuous connectivity, instantly-deployable communication for military. Many surveys have been proposed for communication so that whatever information is transmitted should be same as the one transmitted. The communication is done in two ways wired or wireless. In today's Wi-Fi network communication message is broadcasted to the nodes but it gets affected by Vampire attack i.e nothing on beacon routing protocols, link-state, distance-vector, source routing, and geographic and as well as a logical ID-based sensor network routing protocol and will remain in loop until all networks gets crashed. To avoid such problem we need intermediate verification of packet in routing. Also we can propose this in MANET which is nothing but Mobile Ad-hoc network is a wireless ad-hoc network which is used to interchange information. Each node is ready to forward data to other nodes and does not rely on fixed infrastructure.

We are considering three prime assistances. In first case, we systematically calculate the revelations of existing protocols to routing layer battery draining attacks also to ensure a secure and authenticated data transmission process. We find orthogonality relation between security measures to prevent attacks and those used to defend routing infrastructure therefore existing secure routing protocols do not protect against this attacks. Present work on secure routing challenges to ensure that attacker cannot root path detection to return an invalid network route, but mentioned attacks do not interfere or vary revealed paths, instead using protocol-compliant message and existing valid network paths. So by means of wireless network this attacks going to be resolved attacks like denial of attack, Carousel attack, Stretch attack or retransmission of packets, overhead, maintain packet delivery ratio. As the sensor networks can also operate in an ad-hoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of ad-hoc sensor networks. The security goals are categorized as primary and secondary. The primary goals are well-known standard security goals such as Confidentiality, Integrity, Authentication (CIA) and Availability. The secondary goals are Data Freshness, Secure Localization, Time Synchronization and Self-Organization.

1.1 Various Attacks on WSN

Wireless sensor network is vulnerable to several security threats. There are many papers that provide the security threats in details. Here we have briefed some of the main security threats for WSN.

1. Misdirection- Misdirection attack can cause due to varying or repeating the routing information and also advancing the message via incorrect route can cause this kind of attack. This attack is also calculated as routing layer attack.

2. Selective Forwarding- In this kind of attack, limited packets is transferred or attacker declines to advancing packets or drop them then it turn as a black hole.

3. Sinkhole Attack- In sinkhole attack, adversary appeals all the traffic from an exact area to a compromise node. This attack can also cause selective forwarding attack.

4. Sybil Attack- A malicious node represents various identities to the system which divert the attention form the intended target known as Sybil attack.

5. Wormhole Attack- In this attack an attacker or malicious node stands in between or insert two nodes in the network and advancing packets in between them the networks.

6. Hello Flood Attack-In this type of Attack, Adversary broadcast hello packets in the system to add himself as the neighbor to the further nodes network is saturated and consume the energy.

7. Denial of Services-A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to create a machine or network resource inaccessible to its proposed users. DoS aims sites or services hosted on high-profile web servers such as credit card payment gateways, banks and even root name servers. There are two forms of DoS attacks those are crash services and flood services.

8. Carousel attack- In Carousel attack, attacker constitutes packets with knowingly introduced routing loops and drives packets in circles. It objects source routing protocols by developing the restricted authentication of message headers at forwarding nodes, permitting a single packet to frequently traverse the similar set of nodes.

9. Stretch attack- An attacker builds falsely stretched paths, possibly traversing every node in the system that raises packet path length and it processes the packets through the nodes

that are autonomous of hop count across the shortest path between the attacker and packet destination.

10. Jamming attack- It interferes with the radio frequencies of the sensor nodes from which only few jamming nodes can put a significant amount of the nodes unavailable. If the adversary blocks the entire network then that set up complete DoS.

1.2 Assumption and Dependencies

1. We consider the effect of attacks on geographic, link-state, source routing, beacon routing and distance vector, as well as a logical ID-based sensor network routing protocol. Above listed protocols we outlook the covered protocols as an essential subset of the routing resolution space, and stress that our attacks are probable to apply to other protocols.

2. All routing protocols works on at least one topology discovery period.

3. Our adversary's location within the network is assumed to be stable and random. Attackers have the same resources also they are malicious insiders and level of network access as honest nodes.

4. This is far from the strongest adversary model; rather this pattern represents the average expected damage from this attack. This attack would be more dangerous if intelligent adversary placement or dynamic node compromise.

5. In next case we assume that a node is completely disabled once power of battery is exhausted, now consider nodes that recharge their batteries in the field, either by continuous charging or switching between recharge and active cycles. In the constant charging case, if the attacker is able to consume power at least as fast as nodes can recharge then power-draining attacks would be effective.

6. At last we are assuming that packet processing drains at least as much energy from the targets as from the attacker, a continuously recharging attacker can keep at least one node disabled forever at the cost of its own functionality.

1.3 Motivation

For good communication may be wired or wireless source and destination must be secure from the unwanted interruptions example in mobile phones noise is the interruption likewise in systems important is the information that is shared between the user that can be affected by the attacker. It affects the system integrity and security as it is modified. Besides it increases

the power consumption in the network leads to deplete the energy of systems. Today it is needed in any wireless secure packet forwarding or data transmission. The adversary composes packets with purposely introduced routing loops. This is one of the major problems of the network where the consuming energy of each and every node in the network will increase. Since it sends packets in circle so delay in data transfer so it is again an important parameter in any communication can be wired or wireless so considering this all issues caused by adversary need of detection and elimination is required in the systems.

2. LITERAURE SURVEY

Wireless system undergoes various attacks due to deployment in large area also in remote location where access is not easy job. So to prevent this attack various implementations is done. Eugene Y. Vasserman[8] 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.

K. Sivakumar and P. Murugapriya[6] describes how to eliminate the attacks in the network it uses the proposed optimal energy boost-up protocol (OEBP) analyzes the routing table and verify the attacks which permanently disable networks by quickly draining nodes' battery power. This enhanced work increases the Quality of service in the network and it will regulates all the nodes activity.

B. Umakanth and J. Damodhar[10] 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.

Sureka.N and Chandra Sekaran[9] 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.

T. Sathyamoorthi, D. Vijayachakaravarthy, R. Divya and M. Nandhini[11] described about the how to detect the malicious node in WSN using a simple and effective scheme proposed as Stop Transmit and Listen (STL) to find the malicious node. 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 neighbor nodes in the network.

3. EXISTING SYSTEM

Attack on Stateless protocols

Stateless are not synchronized and do not follow any sequences. They even do not store or maintain any routing information at nodes. In previous study people worked on carousel attack, stretch attack different protocol is used to eliminate attacks and problems associate with it but no one have given solution for both detection and elimination simultaneously. They worked on different criteria like energy or packet ratio or security on single attack. Some attacks that targets source routing are mention below-

1) Carousel attack- In this attack attacker tends to forward packets in loop means that packet will not reach to destination from source side and repeatedly traveling through same nodes forming loop. It increases the route length to limit it with number of allowed nodes.

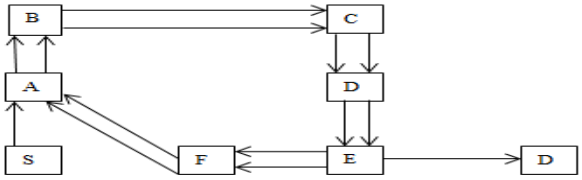

Fig.1. An honest route would exit the loop immediately from node E to destination, but a malicious packet makes its way around the loop twice more before exiting.

2) Stretch attack- In this attack adversary makes artificially long route to follow while sending packets leads to more time delay as well as energy consumption. It makes the packet not to follow larger than optimum number of node.

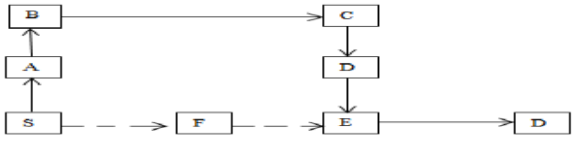

Fig.2. Honest route is dotted while malicious route is dark line. The last link to the destination is shared.

Below shown is the existing system affected by the both the above mentioned attacks where packets not reach to destination and affected by the vampire.

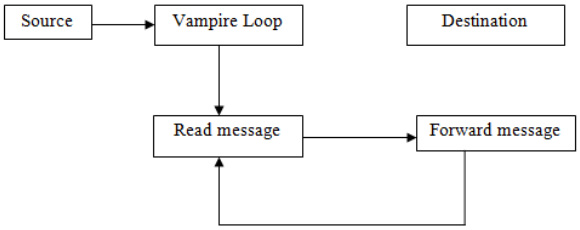

Fig. 3. Existing system

Many algorithms and protocols used to detect and eliminate one is loop detection followed by PLGP which used no backtracking property for forwarding the data and finding out the shortest path if possible but it adds more overheads, delays and energy consumption to a extend they able to limit it.

4) PROPOSED SYSTEM

In this project we will implement five objectives i.e Prevent the Vampire attack. Showing simulation results measuring the performance of several illustrative protocols in the presence of attack. During packet forwarding phase it alter an existing routing protocol to provably bind the damage from attacks. Decrease drainage of battery. Less delay i.e. less time complexity and this is implemented in NS2 software that reduces the cost.

PROPOSED ARCHITECURE

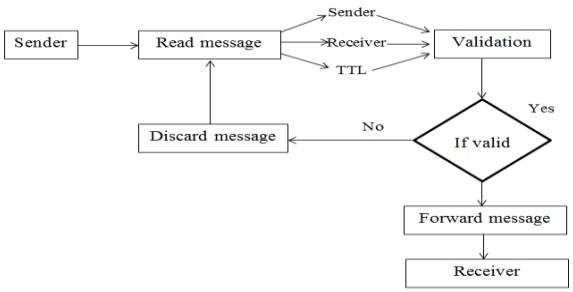

Fig. 5. Proposed system

In this system we are going to implement both the systems existing and proposed system to work on secure packet forwarding as well as energy consumption. From the above figure it

shows that when Vampire attack has been deployed in network the flow of message packet is such that it doesn't gets delivered at receivers end and flows in a loop called Vampire loop. In this Vampire Attack the message is routed to non-receiver node from where it is again forwarded to next non receiver node and this continues in the network causing system to crash.

For the proposed system design implementation will be first sender sends message and each node will extract information like TTL values, sender's address, and destination address. Validation will be done like if there is an entry already made in routing table of corresponding message packets which means the packet has already been transmitted thus that particular packet will be discarded from forwarding queue. After validation the packets which are not discarded will be sent to other node and same procedure will repeat until the message packet reaches the destination. The following function ensures secured forwarding of packets from source to destination when Vampire Attack has been executed. If TTL value of message packet should be less the threshold value of TTL of message packet for proper communication or else it will be discarded.

A) Attack on Stateful Protocol

Stateful means it maintains the records of routing tables at nodes follows the sequences and are synchronized. it consist of two classes that is link state and distance vector. In link-state protocols nodes retain information of the up and down state of links in the organization and flood routing updates of up and down link when it is enabled or not every time. Distributed Bellman-Ford or RIP also known as DSDV is example of distance vector where every node has the routing table record which is simultaneously sent to all neighbors to maintain topology this tables contains all available destination, next hope information to reach the destination. Carousel and Stretch attacks are not affected by these two protocols.

1) Directional antenna attack- In this attack attacker sends the packet randomly in any portion of the system or advancing packets locally and waste lots of energy while by restarting the packet forwarding in a network and also attack on packet progress will be less as packet forward verdict are made individually by every node. It is also known as half wormhole attack because it established a private communication channel. Packet leashes are made to prevent intermediaries but they are not protecting malicious message sources.

2) Malicious discovery attack- It is also known as spurious rote discovery. In most protocols, every single node will forward route discovery packets meaning here a single message can initiate a flood. Both AODV and DSR are susceptible to this attack since nodes may start detection at any interval, not just for the period of the topology change. This attack becomes

more serious when nodes claim that long distance route has altered. This attack is insignificant in open networks. Packet leashes cannot avoid this attack.

Another attack which we are considering is Dos which affects the packet security and power consumption.

B) DOS (Denial of service attack)- In Dos attack adversary makes nodes in a sensor network affected and sending false information to the receiver. It first attacks the nodes making them to relies on the adversary as per his choice of action it send requests to receivers about availability form all nodes that make receiver busy in sending information or acknowledge of availability hence it not able to receive intended message form source or communicate. Here we proposed systems that not only detect this attack also eliminated from the network. Below in figure A is attacker or adversary and R is receiver.

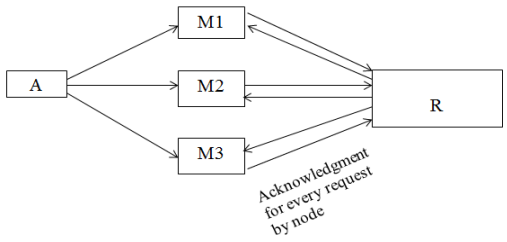

Fig.3. Adversary make node to continuously send request to receivers so every request it send acknowledgment leads to Dos attack.

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

The modified version of PLGP is able to prevent the attacks than the original one. It consists of Topology Discovery Phase and Packet Forwarding phase. In discovery phase it forms node as tree and same is shared through neighboring nodes like leafs but before broadcasting node knows itself and entirely leaf nodes are physical and having virtual address.

TDP- In this phase, every node starts as cluster size one with virtual address zero and clusters are combined with smallest neighbors choose cluster as 0 or 1. At the end each node identifies every nodes virtual address, certificate and public key. It broadcast its certificate of identity along with public key.

Here it follows no-backtracking property towards the attacks. It indicates that for each packet in the protocol execution trace and honest node crossed between source and destination is self-

determining action of malicious node also PLGPa never floods and its packet sending overhead is Satisfactory.

Packet forwarding Phase- In PFP, all verdicts are made individually by each node. Every forwarding event reduces the reasonable distance to target and next hope is determined by verdict the most significant bit of its address when a packet is received at node.

D) SECURE PACKET SCHEME

We will use this scheme for all attacks for secure packet forwarding. In Carousel attack where adversary makes packet to forward in infinite loop. When packet is forwarded to destination that time due to attack first thing packet goes in infinite loop second to overcome this we propose a table containing information (TTL values) of nodes so when a packet passed from one node to another it maintain a record there that this packet is arrived on this node. If again visited to same node it gets discarded but due to this packet get lost at that node also delay occurs due to same rotation of packets in nodes that is routing loop. So to have secure packet transfer also less delay we send acknowledgment again after the packet found in same node to retransmission of packet to destination eliminating that routing loop path and selecting shortest path example carousel attack.

E) ENERGY CONSUMPTION SCHEME

When packet are found in loop by means of attack it means it uses lots of energy for sending same data to destination address also when the path gets stretch i.e in stretch attack where adversary makes the packet to take longer route to follow to destination that not increase the delay but also more energy consumption towards packet forwarding. So this scheme will decrease the delay time as well as energy consumption with the help of routing table that holds the TTL value, source and destination address.

Also in case of Dos it leads to energy consumption due to making receivers side busy in handing the request form the adversary of being available for packet forwarding so when we apply this proposed method it not only decreased the delay also secure packet forwarding.

F) ALGORITHM

Function secure_forward_packet(p)

s ⟵extract_source_address(p);

a ⟵extract_attestation(p);

if (not verify_source_sig(p)) or

(empty(a) and not is_neighbor(s)) or

(not saowf_verify(a)) then

return ; /* drop(p) */

foreach node in a do

prevnode ← node;

if (not are_neighbors(node, prevnode)) or

(not making_progress(prevnode, node)) then

return ; /* drop(p) */

c ← closest_next_node (s);

p' ← saowf_append (p);

if is_neighbor(c) then forward(p', c);

else forward(p', next_hop_to_non_neighbor(c));

G) BE-CO SCHEME

It is nothing but beacon and co-ordinate protocol that works to find out malicious node in network by selecting one fixed node with set value for that node to determines our packet send are sequential or not. This node holds information of neighbour nodes their address their energy consumption and bandwidth. Examples of beacon and coordinate are BVR and GPSR. For routing they uses physical beacon or coordinate distances. In GPSR packet is sent if obstacle comes in between it can be end node it travels along large path length until target is available without considering obstructions. In BVR this attacks can be limited if each node is making independent packet forwarding decision. In this packets are directed towards a node close to the target.

CONCLUSION AND FUTURE SCOPE

In wireless secure data transfer or packet forwarding is main concern due to distributed nature of these networks and their distribution in remote areas, These networks are prone to several

security threats that can adversely affect their appropriate functioning. Also we can classify this as energy draining attack where it deplete the node in the system here we proposed a system uses the protocols which not only provide less energy consumption, less delay but also secure packet forwarding in the system. In future work more attacks can be added and their performance on different parameters 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. Priti Lale and Dr. G.R. Bamnote "Detecting and preventing vampire attack in wireless sensor network" proc. Scientific & Engineering Research International conference, Volume 4, Issue 12, December 2013.

3. 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.

4. 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.

5. Dr. S. Palaniswami and A.Rajaram "Malicious Node Detection System for Mobile Ad hoc Networks" IJCSIT, Vol.1 (2), pp. 77-85, 2010.

6. 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.

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

8. 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.

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

10. 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.

11. 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.