IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Survey on Preventing Vampire Attacks in Wireless Sensor Networks

Ms. S. Jayashree[1], Ms. S. Hebziba Jeba Rani[2]

PG Scholar, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, India[1, 2]

Abstract: In mobile networks the nodes tend to move as they are not stable. Packet transmission in these networks is carried out by hop to hop packet transmission. During transmission of packets in the Wireless Sensor Network, energy of nodes gets reduced as they require certain energy to receive the packets from source and send it to the proper destination. In some cases the nodes energy is highly used up by the packet when a message is transmitted. This indicates that there may be a presence of malicious nodes in the network. These malicious packets which consume more energy than the energy used up by the honest nodes are termed as "Vampire packets". The presence of these vampires in the network the energy of the nodes get drained gradually which leads to network failure. If these vampire packets can be detected and avoided, the lifetime of the nodes get increased. This paper deals with the types of vampire attacks and the mechanisms that are proposed to detect and control vampire attack.

Keywords: WSN, Vampire Attacks, Mobile Networks, Vampire packets.

I. INTRODUCTION

Mobile nodes are the nodes that configure themselves to form a network and they do not have a specific infrastructure in the case of Mobile Ad-Hoc networks. Through distributed algorithms they handle their networking tasks themselves. Wireless communication is established between the nodes through a multi hop connections. In which each node forward the packet to the other node. Wireless sensor networks (WSN) gain a much importance today in the field of research because of its wide range of usability. WSN are autonomous nodes communicating via radio signals without any additional backbone infrastructure similar to MANETs. Nodes in WSN use a broadcast communication to communicate with other nodes in the network. Network topology changes constantly due to the fact that the nodes are prone to fail. These devices have low power, low computational capabilities and limited memory. Important characteristics of WSN include power consumption for nodes using batteries or energy harvesting, resilience, heterogeneity of nodes, ease of nodes and cross layer design. The operating systems for WSN are more complex than general purpose operating systems. They are deployed for specific purpose or an application rather than the general platform. The applications of WSN includes area monitoring, Health care monitoring, Environment earth sensing, Water quality monitoring.

II. EXISTING ATTACKS IN WIRELESS SENSOR NETWORK

There are many attacks in networks including Denial of Service (DOS) attacks, Reduction of Quality (ROS) attacks, Routing infrastructure attacks and Vampire attack. Among these attacks, the Vampire attack is considered to be the most dangerous attack because it is not detected in early stage like DOS, ROS, etc. It silently resides in the network and causes a massive damage to the entire network.

III.VAMPIRE ATTACKS

Vampire attacks play a most vital role in these networks because this attack is not easily discovered unlike other attacks. Vampire attacks mainly target the depletion of nodes battery power. They enter into the network and their presence in the network is not known as they do not disturb the network immediately. The above attacks do not entirely collapse the network system but their attack will only sustain the messages. But vampire attack composes and transmits a message which causes the node to use more energy to be spent on that message. The node may be an honest node with an identical message and packet header but vampire attacks make that node to loss more energy on sending that message.

This is measured by the initial energy utilization of the node when sending a message and the energy used up by the malicious node. The consumption of energy by malicious node will be high compared to the initial message transmission by the honest nodes.

Vampire attack has two type of classification:
a) Carousel attack
b) Stretch attack.

A. Carousel Attack

In carousel attack the malicious node makes the message to be transmitted again and again to the same nodes. This continual transmission of the same message forms a loop in the network. Because of this action by the malicious node, the message will not reach the destination properly.

The main aim of this looping is to use up the battery power of the nodes by repeated message transition. Ultimately, the battery power of the nodes get drained off by unnecessary message looping.

Here node S is the sender and D is the destination. The nodes A, B, C and E acts as the intermediate nodes. E is the malicious node that makes the packet to loop inside the network.

DOI 10.17148/IJARCCE.2016.5255

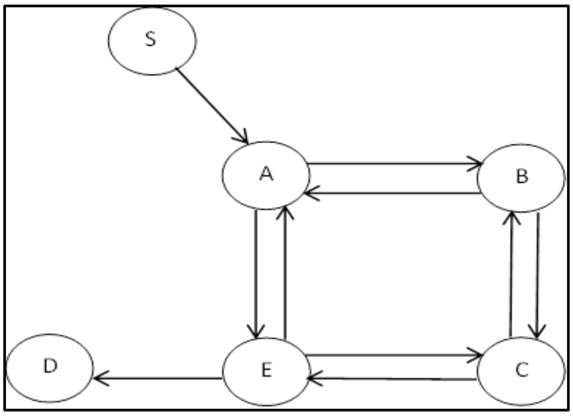

Fig 1.Representation of carousel attacks

B. Stretch Attack
In stretch attack, the route between the sender and receiver nodes will be extended. In other words, there exists a stretch in the route between the source and the destination. The original route gets stretched due to the malicious node activity. The stretching of route is mainly to increase the path of the message or the route in which the packet transmission takes place. The stretched routes can be referred to as the artificial routes. The artificial routes lie along honest nodes and increase the path of the route unnecessarily. This causes nodes to lose their energy without any reason.

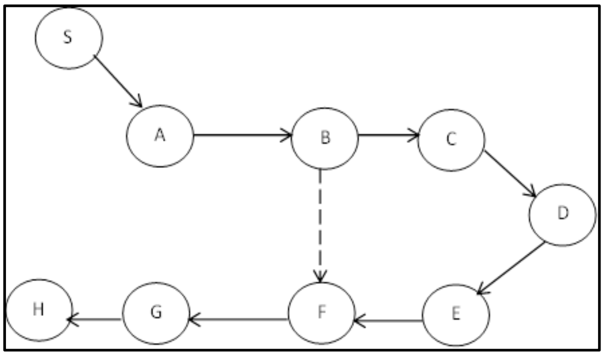

Fig 2: Representation of stretch attack

Here, dashed line from B to F represents the original path for packet transmission by minimum distance routing. But, B node acts as a malicious node and diverts the packet to the other node C where form C, the packet gets diverted away from the original source.

IV. PROPOSED ALGORITHMS TO RESIST VAMPIRE ATTACKS

A. Ad Hoc On-Demand Distance Vector
The AODV belongs to the distance vector routing protocols (DV). Every node has its own routing table which contains information about nodes in the network, neighbour node's distance and next hops. The AODV is an "On demand routing protocol" which establishes a route only when needed for transaction. It supports unicast, broadcast and multicast. AODV has the integrated multicast routing which is one of the greatest advantages of AODV. A multicast routing table contains IP Address, sequence number of group, sequence number of group leaders IP address, hop count to the leader, next hop in multicasting tree and lifetime of the hop.

To join a multi hop group a node sends a route request RREQ to the group address. A node in the group receives the request RREQ and replies with a RREP. The requesting node can have several RREP from many number of nodes in the multi hop network. The requesting node selects the RREP which have a minimum number of hops which is considered to be the shortest distance to the group. The node activation is done by sending the MACT (Multicast Activation) message to activate the branch.

Advantages
The main advantage of AODV is that the route is established only on demand and destination sequence numbers are applied to find the latest route to destination. Connection setup delay is low.

Disadvantages
One of the disadvantages is that when the intermediate nodes have old sequence number which can lead to inconsistent routes. The route reply packet to the single route request is multiple and can lead to overloading of the network. Unnecessary bandwidth consumption is also a drawback in AODV.

B. Destination Sequenced Distance Vector
In DSDV, a routing table is used to maintain the availability of the destinations and the number of hops between each node. This is updated periodically when there is a transition between the nodes. When the new information is available then the routing table will be updated. Each station in the network maintains a routing table which is updated periodically in the presence of new nodes or information. The route table entry is tagged with a sequence number which is originated by the destination station.

Disadvantages
Regular updating of routing table is required which consumes battery and bandwidth. The topology changes may introduce a new sequence number before network re-coverage's. Thus it is not suitable for highly dynamic networks.

C. Parno, Luk, Gustad And Perrig (Plgp)
The traditional sensor routing protocols such as SAODV, SEAD checks whether the packets consistently make progress towards the destination. They concentrate only on the network layer not on the application layer where malicious packet originally originates.

In PLGP method, we are considering both network layer and application layer. The network layers help in checking the vampires from the network whereas the application layer finds out the vampire inside the running process. Vampire packets when detected in the network are discarded and are not forwarded.

The original version of PLGP protocol designed for security purpose is vulnerable to vampire attacks. The initial phase of PLGP will be a topology discovery phase

DOI 10.17148/IJARCCE.2016.5255

and the next will be the packet forwarding phase. The no backtracking property of the PLGP is defined as only when the packet consistently makes progress towards the destination in the network.

This backtracking property is preserved by adding a verifiable path history to every PLGP packet. This packet history address will be useful for securely verifying the progress of the packet, preventing any significant adversarial influence on the path in which a single traversal may be viewed by monitoring the history of the packet. A repayable attestation or signature is attached to a packet when it is forwarded by a node. The forwarding node identifies the path of the node by verifying the signature, thus ensuring that the packet has never traversed away from the address space.

The packet are verified for the presence of vampire by two categories 1) the signature in the packet which indicates the authorisation of the packet in the network and 2) the packets logically closer to the destination than previous hop. The detection is done by the use of TCP header checking and grouping of packets into two groups namely infected and non-infected packets. Handling of infected packets includes the checking of packets IP address, flags and by the use of anomalies.

Here, the packet is not deleted immediately when it is found to be a vampire because the packet may contain some important information about the previous node or the sender node. But when a vampire is detected within the node, it will be deleted immediately.

Advantages
This method can be implemented as four stages or phases network layer vampire detection, application layer vampire detection, vampire handling and scan details. It provides a high level of security against vampires.

D. Enhanced Ad Hoc On Demand Vector

The Enhanced Ad-Hoc on Demand Vector proposes the alternative path selection at the break of link. This path is selected on the basis of least energy consumption of the node to forward a packet in a secure manner. The path is considered to be the best since it is also capable of repairing the link break at distant node with the shortest path. The intermediate nodes will be nearer to the source and destination hence it can quickly find the nearest path to the broken link. Thus the repairing of link is also an easy task. The intermediate nodes will En-route to repair the broken link to the destination. This En-routing will be carried out for finding the shortest distance. The packets that are used for communication includes RREQ (Route Request), RREP (Route Reply) and RERR (Route error).

In ENAODV three new packets were introduced along with the above packets. R-R (Route Repair), RR-OK (Route Repair-OK), RR-F (Route Repair Failure).

Advantages
In this method, energy depletion detection and attacks on energy depletion is blocked. The Adaptive power aware Multicasting algorithm is used to save the power.

E. Enhanced Adaptive Acknowledgment

The watchdog scheme is capable of detecting malicious nodes in the network. But it fails in many cases like transmission power, false misbehaviour report, etc.

In EEACK scheme, a digital signature is used to prevent the attacker from forging acknowledgement packets. It consists of acknowledgement (ACK), Secure-Acknowledgement (S-ACK) and Misbehaviour Report Authentication (MRA). The entire acknowledgement in this scheme should be verified by the receiver for the sender's digital signature.

Advantages
The security of the packets will be a maximum because this work prevents the attackers to initiate the forged data work. This is suitable for the limited power transmission protocols.

V. CONCLUSION

Vampire attack may be detected using the above discussed protocols.

REFERENCES

[1] E Y Vassermann, N Hopper, Vampire Attacks: Draining life from wireless Ad hoc sensor networks, IEEE Transactions on Mobile Computing, volume 12, issue 2, published on 2013.
[2] M Mohana, P Kaviya, A Survey on Secure Packet Transmission against Vampire Attack in Wireless Ad-hoc Sensor Networks, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 11, November 2014.
[3] Anoopa S et al, Detection and Control of Vampire Attacks in Ad-Hoc Wireless Networks, Int. Journal of Engineering Research and Applications, Vol. 4, Issue 4 (Version 6), April 2014, pp.01-07.
[4] G. Vijayanand et al, Overcome Vampire attacks problem in wireless ad-hoc sensor network by using distance vector protocols, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January- 2014, pg. 115-120.
[5] Anand Kaushik, Bikram Pratap Singh, to secure attacks in MANET using IDs based EAACK scheme, International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 3 Issue 2, May 2014.
[6] V. Sharmila et al, Energy Depletion Attacks: Detecting and Blocking in Wireless Sensor Network, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.8, August-2014.

DOI 10.17148/IJARCCE.2016.5255