International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Solution to Vampire Attacks: Techniques to Make Network Live

Vikas Juneja[1], D.V. Gupta[2]

[1] *Assistant Professor, Department of Information Technology, JMIT, Radaur, Haryana, India*
[2] *Professor, Department of Mathematics, College of Engineering Roorkee (COER), Roorkee, Uttarakhand, India*

Abstract - *Wireless sensor network (WSN) is a network of low cost, low energy sensor nodes which collects the information around physical surroundings. Sensing and pervasive computing features of WSN opened up various applications which in turn lead to research work. In various areas such as in military, forest, health, inventory etc., WSN has been implemented. In WSN, Energy is an important factor for sensor node. There is one new type of attack called vampire attack has been exposed which disables network by overwhelming battery life of sensor nodes in a network. The proposed work introduces new methodologies focused on energy based intrusion detection system, path tracking techniques, on energy threshold and packet broadcast threshold of sensor node of network. Earlier it was limited to packet forwarding phase only but not work with topology change. The projected solution is simple and also works with topology change in network.*

Key Words: **Vampire attack, Wireless sensor network, Intrusion detection, Routing,Security.**

1.INTRODUCTION

A Wireless Sensor Network (WSN) constructed of large number of sensor nodes may be in hundreds or thousands. These sensor nodes can transfer information to each other inside network or directly to an outer base-station node. The more sensor nodes make network to sense over more physical areas with higher degree of accuracy. Sensor nodes communicate sensed data to each other and form high-quality useful information about the surroundings [1]. Each sensor node bases its decisions on its goal, currently gathered information, and its proficiency of its computation, transmission, and energy assets. These distributed sensor nodes have the ability to route data either to other sensors or to an external network nodes. This node may be a stationary node or a mobile node proficient of connecting the sensor network to the available communication infrastructure or to the web where a user has access to the sensed information. Attractive features [2] of Vampire attacks that make them the most prominent attack are:

- Vampire Attacks are not protocol-specific i.e. they do not target particular protocol.
- Vampires use Protocol-Compliant messages.
- Transmission of trivial information with largest energy drain is achieved.
- They do not interrupt or alter discovered paths.

In this paper, the solutions or techniques of the vampire attacks in the wireless ad hoc networks are discussed. These types of attacks not directly link with the protocols; it links with the properties of the routing protocols in the communication networks. This attack affects the properties such as relation state between the nodes, remoteness vectors between the nodes, resource and location based routing. The vampire attack in the WSN is not easy to discover and to predict. Due to the solitary vampire attack in the networks, total force goes down and leads to the complete system to the collapse. In order to overcome the above attacks in the wireless ad hoc networks we proposed techniques for secured transmission in the networks. In order to overcome the above attacks, various techniques such that an efficient intrusion detection system based on energy of nodes, path tracking approach and on energy threshold and packet broadcast threshold of sensor node of network are discussed.

The remainder of this paper is organized in three sections. The first section will discuss the related work which familiarizes the earlier security measures on wireless sensor network. Second section will discuss the proposed techniques to overcome the vampire attacks. After that paper is concluded.

1.1 Related Work study

Routing Protocols in WSN can be categorized into three categories based on network structure flat-based routing, hierarchical routing and location based routing [3].In Flat-based routing all network nodes poses similar functionalities and equal roles while in hierarchical –based routing node plays different roles assigned to them. In case of location-based routing positions of sensor nodes are exploited for routing data in the network. A routing protocol is self adaptive because they can change the network parameters in order to adjust with the present network state and energy capacity of network nodes. Moreover, these protocols can also be classified on the basis of protocol operation namely query oriented, Multipath-oriented, negotiation-based, QoS-based routing techniques. Protocols can also be classified on the basis of route discovery process from source to destination which are named reactive, proactive and hybrid routing. In reactive protocol on demand route discovery method is used i.e. route is derived just before sending of message, while in proactive routing route are pre-discovered irrespective to time of sending message[4]. Hybrid protocols consist of these two strategies. In case of static nodes, it is preferable to have table driven routing protocols rather than using reactive protocols. In case of reactive protocols, process of route discovery and path setup consumes some amount of energy. One more type of routing protocol has been noticed namely cooperative routing protocol. In cooperative routing, there is one central node where all the data is aggregated from all other network nodes and then that data is further processed, and reduces route cost in terms of energy usage. Many other protocols depend on position and timing information.

2. Proposed Techniques

In this paper, three techniques have been discussed to detect and eliminate resource consumption attack called vampire attack which drains the battery power of nodes in the network abnormally. Three techniques [5] are:

1. Energy based Intrusion detection system.
2. Packet broadcast threshold of sensor nodes of network.
3. Path tracking technique.

Energy based intrusion detection system

Initially almost all nodes have same energy. The energy or power of nodes is used in packet transmission or forwarding of data packets. Thus there will be a small variation in energy level of nodes. Vampire attack causes more energy to be consumed than a network with normal node does for the same processing and forwarding. It makes the energy of whole network very much low. Energy based intrusion detection is the concept of energy level. It works on the fact that the malicious nodes will have abnormally high energy than legitimate nodes. Thus in this energy of all nodes are measured, node with abnormally high energy is detected as malicious node. The network authority will eliminate the detected node by informing all other nodes about this high energy detection. The nodes will eliminate the malicious node from its list and stop to forward packet to that detected nodes.

Packet broadcast threshold of sensor nodes of network

The threshold concept [6] is utilized during route discovery phases for trusted nodes estimation to overcome the vampire attacks. Nodes are mobile in networks. The vampire attack initiate packet flooding to establish the malicious connection. Due to this, target node floods the packets further and drains their energy and performance in network. Thus when the attack is deployed then the first number of broadcast in network is counted and a threshold value is determined. This threshold value is used to mark the node suspicious.

Path tracking technique

The vampire attack drains energy by introducing routing loops and stretching the normal route. Routing loops occurs because nodes are not aware of whether they are processing the same packet that it processed previously. To avoid this, in the proposed technique, a log-file is maintained for each node. The log- file contains the source, destination and packet id.

Whenever a packet arrives each node check the log file for the source- destination pair of packet. If present it verifies that it is not processing the same packet by comparing the packet id. The energy spent for this checking is less compared to the energy drained during infinite looping of a single packet. Stretching of route happens because nodes are not aware of whether they are forwarding the packet towards destination or making a path that takes packet away from destination. This stretching occurs when source itself become malicious and intermediate node forward the packet according to source route without any further checking. This can be avoided by tracking the path. In this, a path history is maintained along with packet. Each node makes an attestation to each packet by adding its id to the end of packet. On receiving, the node checks the path history to verify that the packet is actually moving forward to the destination and not backtracking. Thus stretching of routes can be avoided.

4. CONCLUSIONS

This paper includes study of major techniques to deal with vampire attack. Dynamic detection and removal of vampire attack solutions in WSN are based on threshold energy level, path tracking and energy based intrusion detection system. These mentioned techniques provide provable security but still there are some limitation in topology phase and this makes it susceptible to Vampire attacks. So the further modification is required in the topology phase to secure the protocol entirely from Vampire attacks.

REFERENCES

[1] Eugene Y. Vasserman, Nicholas Hopper, "Vampire Attacks: Draining life from Wireless Ad-hoc Sensor Networks," IEEE transactions on mobile computing, vol.12 no.2, 2014.

[2] Virjot k, Priyanka R., "Vampire attacks: exploration & consequences", International Journal of Scientific & Engineering Research, Volume 7, Issue 4, April-2016.

[3] Jamal N. Al-Karaki Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey".

[4] Manish S., Bharat P.,"Detection and Removal of Vampire Attack in Wireless Sensor Network", International Journal of Computer Applications, Volume 126, No.7, September 2015.

[5] Ambili M.,Biju B.,"Vampire Attack : Detection and Elimination in WSN" in International Journal of Scientific Research, Vol. 3,April 2014.

[6] Deepmala V,Gajender S., "Detection of Vampire Attack in Wireless Sensor Networks" , International Journal of Computer Science and Information Technologies, Vol. 6 , 2015.