International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 3 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

IDENTIFICATION OF VAMPIRE ASSAULT IN WIRELESS SENSOR NETWORKS

[1]Munirathana. M and [2]Prof. B. Sakthivel
munirathna1976@gmail.com and everrock17@gmail.com
[1]PG Student and [2]Professor & Head, Department of Computer Science and Engineering
P.S.V. College of Engineering & Technology, Krishnagiri

Abstract - Mobile ad hoc network is a sort of remote system, in this system specialized gadgets are known as the hubs and the network between hubs are known as connections. The hubs are utilized; this correspondence joins for exchanging data among source and target machines. For that reason hub devours the directing procedures for way revelation and exchange of information. Because of constrained network the hubs are likewise using the transfer system or multi-hop mechanism. Because of this system embrace the whole middle of the road hub in the correspondence way. This leads issues of interior sort of assaults in system, in this proposed work an inside assault in particular vampire assault is explored and a fitting technique is proposed for execution and improving security with the execution of system.

Keywords: Mobile ad hoc network, Security, multi-hop mechanism

1. INTRODUCTION

Wireless Sensor Network become more popular in today's world because of its ad hoc nature. Wireless sensor network is a self-configured network which has the capability to build the network without any infrastructure. This type of network is suitable for areas where it is not possible to set up an infrastructure such as a military area, they provide the connectivity by forwarding packets over multi-hop in the network. It is dynamically changes the topology and form a network where nodes can easily join and leave the network.WSN composed of a large number of tiny Sensor nodes that are scattered throughout the network .Each node is equipped with a sensor, processor, and radio for communication, battery for power supply and memory for data storage. Sensor node is a small, portable and lightweight device which has the ability to sense the information such as Temperature, humidity, light, pressure, sound etc.. Which sense the information then processed it and transfers it to other devices in the network. Individual sensors are not used in the network instead Of hundreds to thousands sensors are deployed in the network to monitor a system.

2. CHARACTERISTICS OF WSN

Short range, low power device equipped with battery for energy. Dense collection of nodes -wireless sensor network consists of hundreds to thousand or more nodes Manage node failure –Nodes have the ability to tolerate failure. Scalability: Easily scalable and work efficiently when add more nodes in the network. Heterogeneity of node: wireless sensor network is a heterogeneous collection of sensor node, where each sensor node having different capability.

3. ISSUES AND CHALLENGES IN DESIGNING WSN

Node Fault Tolerance: It is the biggest challenge in designing WSN to make the system available at the longer duration when some of the nodes may be faulty because performance of network depends on its availability.

Synchronization: clock synchronization is another issue in WSN. It is an important service for Wireless sensor network to synchronize all local clocks of nodes in the network to meet specific requirement.

Scalability: WSN is becoming popular because of its scalability feature. Sensor network growing increasingly because sensors are low cost devices and protocol support large network. It is challenging to deploy wireless sensor network to a large scale and work efficiently with huge amount of nodes.

Node Heterogeneity: wireless sensor network is a huge collection of heterogeneous sensor nodes. Each sensor node has a different ability, computing power and range .It is difficult to build sensor network with heterogeneous node as compare to homogenous node.

Security: Security is an important factor of wireless sensor network .It is most difficult to build WSN with security concerns.

Data confidentiality: sensor nodes do not reveal secret information to other nodes. Data integrity: It assures that data does not change by adversaries during the transmission. Data must be accessed by authorized user.

Data Freshness: It ensures that data must not contain recent or previous data.

4. ANALYSIS OF ATTACKS IN WSN

There are various attacks that have been found in WSN. These security attacks can be classified on the basis of the domain of the attackers, or the techniques used in the attacks. This security attack can be roughly classified as: passive or active, internal or external, attacks on various layers.

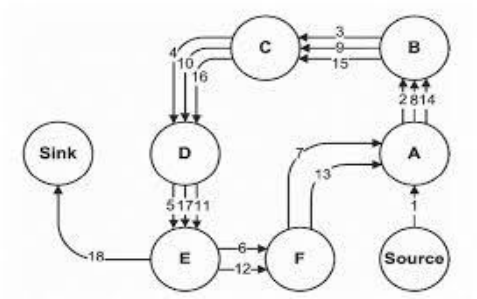

Fig. 4.1 Analysis of Attacks

Passive and Active attack: Passive attack involves disclosure of information or data files to an attacker without any interruption in Network Activity. Active attack includes attempts to break security features, to introduce malicious code, and to steal or modify information. It involves disruption of its normal activity of the network.

Internal and External Attack: External attacks are those attacks which are carried out by the outsider nodes that are actually not present in the network. Internal attacks are carried out by nodes, which are actually present within the domain of the network

Jamming attack: Jamming attack Performed at the Physical layer, which is concerned on disruption of communication.

Black hole attack: A Black hole attack was formed at the time of poor routing infrastructure. When a malicious node joins the network this problem arises.

Black hole Attack Wormhole attacks: In a wormhole attack more than one malicious node are joining the network and according to the nodes they are connected through high speed data buses by which their promises to send data from source to sink.

Eavesdropping: Eavesdropping is a serious kind of attack on the privacy of data that usually happens in the Wireless Ad hoc Networks.

Session hijacking: Session Hijacking is done on the transport layer. Before any communication TCP establish a connection after that start a session.

Denial of service attack: DOS is a multilayer attack. This attack could be performed at the different layer in different for.

Hello Flood attack: In this attack, attacker broadcast Hello packets to all the nodes to show their existence in the network.

Sybil attack: In which malicious node legitimately joins the network with multiple copies of itself at the different locations .This will create the confusion in the network.

Impersonation attack: In this attack an illegal Entity assumes the identity of legal entity and takes the privileges without restrictions and without any indication visible to the recipients. It is the first step for launching any attack.

Rushing attack: When a neighbor of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further requests from this Route Discovery.

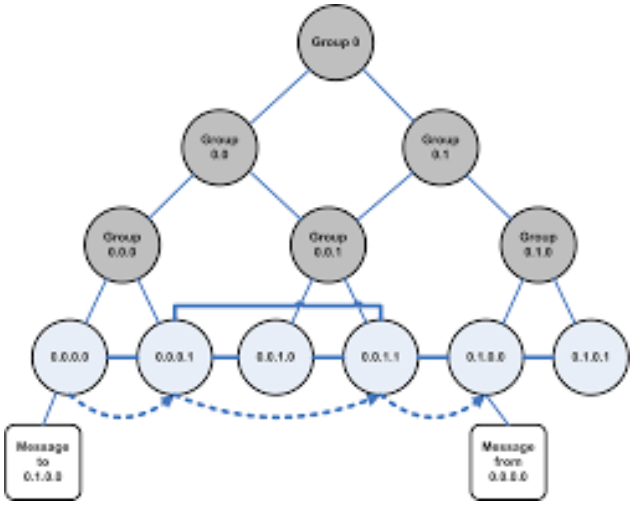

Fig. 4.2 Rushing Attach

5. SECURITY ISSUES IN WSN:

Security has become the most important factor in building a network and its implementation. Security in a sensor network is very challenging as the performance of WSN is depending on its security.

Data Integrity: Data Integrity is an important factor for secure communication. Lack of integrity means inaccurate information. This may lead to a serious consequence in integrity of information in some applications such as healthcare monitoring and traffic analysis etc.

Authentication of data: Authentication of data verifies the identity of the persons or entities who are involved in a communication.

Data Freshness: One of the Network layer attack is replay attack in which adversary seizes the packet and send them later to create confusion in the network. So when designing WSN preserve data freshness must be necessary means recent data not send again by nodes or in other words prevent data from resend in the network.

Data Availability: It Ensure that availability of network services at all time, even in the presence of Denial of service attack.

6. SECURITY THREATS IN WSN

In Wireless Sensor Network one of the Denial-Of-Service attacks on routing protocol is resource depletion attack known as a vampire attack. Battery power is an important resource, each sensor node have depended on the battery power for their work, but vampire attack deplete the node's battery and slowly disable the network availability.

Vampire attack: Vampire attack is a kind of DOS attack. In which formation and sending of message done by the malicious node which causes more energy to be consumed. It causes resource depletion (energy) at each sensor nodes, by destroying battery power of every node. They do not disrupt the network availability immediately, instead it compose a message with little amount of data and larger energy drain. These work slowly over a long period of time and destroy the network services by draining the battery power of nodes. It transmits a small complaint messages to disable a whole network, hence it is very difficult to diagnose and prevent.

7. PROBLEM DEFINITION

Basically vampire attack is a variant of DDOS attacks, which performs resource consumption on neighbor nodes. Therefore, during the vampire attack targeted packets are modified for preparing long routes or misguiding the packets.

In addition of that the malicious nodes are making frequent connectivity of the entire neighbor nodes in the network using false control message exchange. Due to these neighbor nodes replies the false request for connectivity and draining energy rapidly.

Therefore, in order to detect and prevent the malicious nodes in the network a new kind of scheme is required which monitor the network node's activity and provide the decision for malicious behaving nodes. On the other hand the malicious host only changes a few information of the packets thus; it is difficult to locate on the network.

Additionally, during such kind of attack deployment the other network performance parameters like PDR (packet delivery ratio) and the Routing overhead not much effected thus when an attacker node penetrate the security is not identifiable.

Thus detecting such kind of malicious host is a complex issue. In order to overcome the effect of the malicious attacker a new strategy is required to develop which is described in detail in next section.

8. PROPOSED WORK

In order to provide solution during route discovery phases the threshold concept is utilized for trusted nodes estimation. Additionally the nodes are mobile in network scenarios. The vampire attack usage the packet flooding and RREQ flooding to establish the malicious connection during. Due to this target node flood the packets further and drain their energy and performance in network. Thus when the attack is deployed than the first the number of broadcast in network is counted and a threshold value is determined. This threshold value is used to mark the node

suspicious. Thus now a sampling is performed on network by which the nodes broadcast values are compared to the estimated threshold value. Thus algorithm performs the following step.

For each node in network.

If node.Broadcast > threshold than

Label node as suspicious

Else Legitimate

End if End for

After classifying the nodes in two groups the suspicious nodes are removed from the active communication and the normal network is communicating. During this the average packet delivery ratio of each node is estimated.

If suspicious nodes PDR < normal nodes PDR

Remove node Else Label normal End if

9. CONCLUSION AND FUTURE WORK

Wireless sensor network is a kind of ad-hoc network. There is a new kind of internal attacks called vampire attack drain the energy of each Sensor in the network, in this proposed work a vampire attack is investigated and an appropriate method is proposed for implementation for improving security and performance in network by identifying and removing suspicious node from the network. Based on the recently developed techniques a new security technique is designed and implemented for simulating the effect of attack deployment and the performance improvement after security scheme implementation. Additionally, for justifying the solution and their enhanced performance traditional routing protocol is required to compare with the developed routing protocol. In terms of throughput, end to end delay, remain energy and packet delivery ratio. In future we implement our proposed Technique in NS2 and detect malicious node which causes vampire attacks and remove the vampire node from the network. We also compare our proposed work with Existing work.

REFERENCES

[1] VasileParvan, Timisoara "Main Types of Attacks in Wireless Sensor Networks" Department of Computer and Software Engineering.

[2] Sunil Gupta, Harsh K Verma, A L Sangal"Security Attacks & Prerequisite for Wireless Sensor Networks" Volume-2, June 2013.

[3] Manju.V.C. "A Survey on Wireless Sensor Network Attacks" Volume 2, Issue 2, August 2012.

[4] 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, February 2013.

[5] P.DivyaPrabha, R.Sundaram"Exhausting Verve by Vampire's in wireless Ad Hoc Sensor networks", Vol. 3, February 2014.

[6] P.Rajipriyadharshini, V.Venkatakrishnan, S.Suganya, A.Masanam"Vampire Attacks Deploying Resources in Wireless Sensor Networks".

[7] Chahana B. Thakur, V.B. Vaghela"Detection and Elimination of Vampire Attack in Mobile Ad hoc Network" Volume - 5 | Issue - 1 | Jan– 2015.