ISSN:0975-9646

Detection of Vampire Attack in Wireless Sensor Networks

Deepmala Verma[#1], Gajendra Singh[*2], Kailash Patidar[#3]

[#]*PG Scholar, Dept of CSE, ShriSatyaSai Institute of Science & Technology, Sehore*
**Professor, Dept of CSE, ShriSatyaSai Institute of Science & Technology, Sehore*
**Asst. Professor, Dept of CSE, ShriSatyaSai Institute of Science & Technology, Sehore*

Abstract: Mobile ad hoc network is a kind of wireless network, in this network communication devices are known as the nodes and the connectivity between nodes are known as links. The nodes are used, these communication links for transferring information between source and target machines. For that purpose node consumes the routing strategies for path discovery and transfer of data. Due to limited connectivity the nodes are also utilizing the relay mechanism or multi-hop mechanism. Due to this network adopt the entire intermediate node in the communication path. This leads issues of internal kind of attacks in network, in this proposed work an internal attack namely vampire attack is investigated and an appropriate method is proposed for implementation and improving security with the performance of network.

1. INTRODUCTION

1.1 Wireless Sensor Network

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 [1].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.

1.2 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.

1.3 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. To make the service available to a large extent, it is not affected by any kind of faults.

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 [2] .

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 such as

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.

Authentication: Data must be accessed by authorized user.

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

1.4 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 [5].

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. Passive attacks are blocking, traffic Enquiry, and monitoring of traffic. Active attacks are jamming, impersonating, and denial of service attack.

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. Internal attacks are more severe than outsider attack since the insider knows the valuable and secret information and it is difficult to find.

Further attacks are classified on the basis of layers. There are different attacks on a different layer. Here we talk about an attack which is one of the network layers.

Routing and data forwarding is an important service for enabling communication in sensor networks. Most of the security attacks are done at the network layer. Routing protocols suffer from many of the vulnerabilities, such as an attacker might launch denial of-service attacks on the routing protocol, to disrupt network availability.

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

Here we will do a study of different kinds of attack deployment in wireless sensor networks. There are various kinds of attacks are done at the different layer wireless sensor networks are a kind of ad hoc wireless communication network. Therefore, most of the attacks are deployed at the network layer [3], [4].

Jamming attack: Jamming attack Performed at the Physical layer, which is concerned on disruption of communication. Where Jammer an attacker or entity who try to Interfere the transmission and reception of wireless communication physically. Jamming creates unnecessary interference in transmission of message, which results in the 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. This malicious node replies to route requests that it has an active route available to the destination and it also exploits the Routing Protocol by advertising itself that it has a short and valid path to a destination node as shown in fig. 1 Actually, in AODV routing for finding the path between source and sink RREQ packets are flooded and all the path replies with RREP packets if the RREP response from malicious node is arrive first then the requester node assume that the supplied information is correct and from valid node and it reply with the data packets.

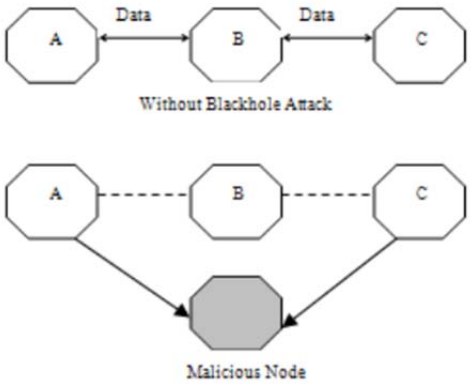

Figure 1.Black hole Attack

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. Malicious node can put down the packets at one location in the network and use recorded packets later to send them to another location through a private network shared with a colluding malicious node.

Wormhole attack can be done with one node also, but generally two or more attackers connect via a link called wormhole link. Wormhole attack is of three types: Closed Wormhole, Half Open Wormhole, and Open Wormhole as shown in fig. 2.

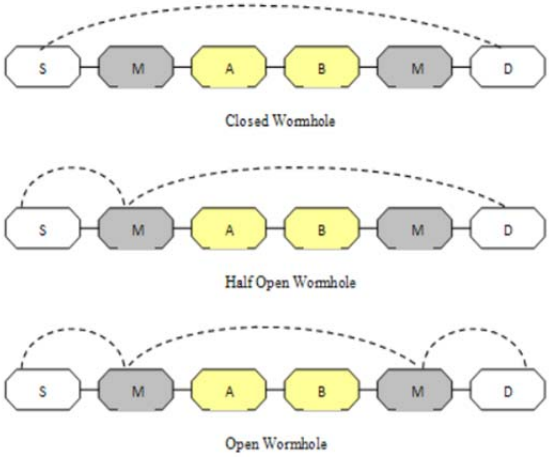

Figure 2. Wormhole attack

Eavesdropping: Eavesdropping is a serious kind of attack on the privacy of data that usually happens in the Wireless Ad hoc Networks. The intention of eavesdropping is to gain access of private information that should be kept confidential during the communication. This private information may include the location of data, public key and private key of the sender and receiver because it is an essential parameter for communication. Such data are very important for the security purpose of nodes; it should be kept secret from unauthorized access.

Session hijacking: Session Hijacking is done on the transport layer. Before any communication TCP establish a connection after that start a session .During this period attacker theft the valid session ID and hijack the session .The attacker use this session id to get the information about data.

Denial of service attack: DOS is a multilayer attack. This attack could be performed at the different layer in different form .The aim of this attack is to prevent the access of network services by the authorized user. In Denial-of-Service (DOS) attack, an attacker trying to prevent authenticate users from accessing information or network services. By attacking on the client computer and its network connection, or the computers and network of the sites client is trying to use, an attacker may be able to prevent the client from accessing email, websites, online accounts, or other services that rely on the affected computer.

Generally Denial of service attack occurs when an attacker overloads the server with a large number of false requests and prevent accessing information by legal authority ,at that time the server can only process A certain number of requests , so if an attacker overloads the server with requests, it can't process the legitimate request.

Hello Flood attack: In this attack, attacker broadcast Hello packets to all the nodes to show their existence in the network .When every node in the network receiving a hello message assumes that it is in the range of the sender and reply with packets. An adversary continuously floods the network with false REQ packets .This will lead to the consumption of battery power of sensor nodes. Deployment of this attack is done at the network layer [4].

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. Sybil attacks harm the network in a different way, such as unfair share of resources; consume data storage and multiple path with the same node id.

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. When non-attacking REQUESTs arrive later at these nodes, they will discard this legitimate REQUEST.

2. BACKGROUND STUDY

2.1 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 .Following are the basic security parameters are needed to build secure Wireless sensor network [4].

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. In sensor networks, it is a necessary task for each sensor node and the base station to verify that the data received was really sent by its original sender and not by an illegal authority that agree the normal nodes into accepting false data. The Security of information from unauthorized parties is important in sensor networks to protect unauthorized access of information. Otherwise, it may result in eavesdropping on the 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.

2.2 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 depend 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 [6].

Vampire attacks are a network layer attack. They are not protocol-specific, in that they do not depend on the design properties or implementation details of specific routing protocols, but rather utilize common properties of protocol classes such as link-state, source routing, geographic, distance vector, and beacon routing. Neither do these attacks depend on

Flooding the network with huge amounts of data, but somewhat try to transmit as little data as possible to attain the biggest energy drain, preventing a rate limiting solution.

There are two types of vampire attack:

Carousel Attack: In this attack, the adversary, compose a packet that could travel through a path repeatedly .Packet repeat the same path in a loop mean same node appear many times in a path shown in fig. 3. In which malicious node purposely sends packets in a loop to drain the energy of honest node [7].

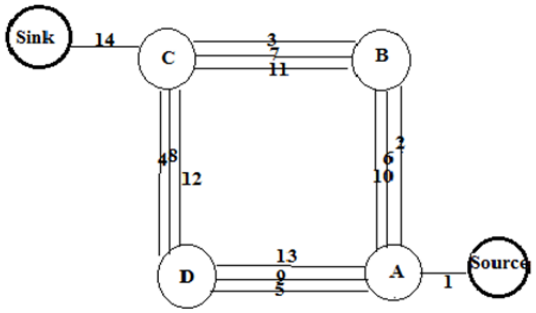

Figure 3. Carousel Attack

Stretch Attack: In this attack, attacker artificially constructs the long route that traverses every node in the network as shown in Fig. 4. Since it increases packet path lengths, causing packets to be traversed through a number of nodes that Unnecessary Increased the Path length between the adversary and packet destination [7].

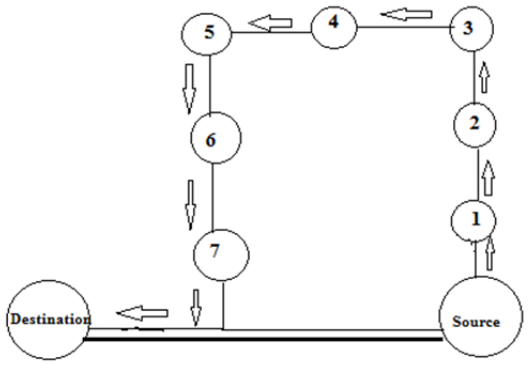

Figure 4. Stretch Attack

3. LITERATURE SURVEY

Eugene Y. Vasserman et al [6] find that all examined protocols are susceptible to Vampire attacks, which are destructive, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of network nodes. Author discusses methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

P. Rajipriyadharshini et al [8] provides a solution for vampire attacks and described as Wireless sensor network is a communication network across the sensors nodes. Energy is the one most important factor while considering sensor nodes. Wireless sensor networks require solution for conserving energy level. Hence there is a large of energy loss. New protocol called PLGP, a valuable and secure protocol is proposed along with the key management protocol called Elliptic Diffie-Hellman key exchange protocol to avoid this vampire attack.

In this paper discuss two types of vampire attack. In which proposed System added a Flag _Field as a security Mechanism to the packet header in order to avoid packets loops or stretch attack. This Flag Field is8 bit in size therefore does not occupy much space in the header. The Flag _Field is 0 in the begging. Only when a node receives repeated packet or a packet which contains its own ID then its forwards repeated packet to the Source node and identify the new route. The proposed system detects and eliminate vampire node in mobile ad hoc network which causing vampire attack [9].

Vampre Attacks are dangerous kind of attacks as in worst case a single Vampire can cause a network wide energy by a factor of O (N) where N is the number of nodes in the network. In an Ad hoc wireless network during the attacks in packet forwarding the energy usage is increased in network. In this paper the main highlight of the implementation is to prevent adversary influence on the nodes battery power and to establish the secured transmission with less energy consumption [10].

In ths paper a detection and control method is introduced for the vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad-hoc wireless networks by depleting nodes' battery power. The proposed methodology can be implemented as four phases, network layer vampire detection, Application layer vampire detection, Vampire handling and entropy and port scan details. By using all these concepts the system is made more secure against the vampire attacks. Methods are there to detect the vampires from the network and inside the node. Once a vampire is detected then, they are handled according to their type [11].

4. 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.

5. 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

$$threshold = \sum_{i=1}^{N} \frac{number\ of\ broad\ cast}{N}$$

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.

$$PDR_t = \sum_{i=1}^{N} \frac{PDR}{N}$$

If suspicious nodes PDR < normal nodes PDR
Remove node
Else
Label normal
End if

Assumption

According to the proposed solution of vampire attack when the vampire attacks deployed on the network the performance of the network in terms of the packet delivery ratio is decreasing and number of broad cast is increasing in network.

In order to provide a solution during route discovery phases the thresholding 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 broadcasts in the network is counted and a threshold value is determined. This threshold value is used to mark the node suspicious.

6. 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.

REFERENCE

[1] P.PreethiMonolin**,** Dr.J. Amutharaj" **Cache Consistency and IDS for Handling Attacks in Routing Ad-hoc networks"**April 2014.

[2] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar "**Issues in Wireless Sensor Networks"** July 2 - 4, 2008, London, U.K.

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

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

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

[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, February 2013.

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

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

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

[10] Kavya.H.B, Manjunath R Raikar" **Prevention of VampireAttacks to Control Routing Behavior in Wireless AD Hoc Networks".**

[11] Anoopa S, Sudha S K, *Vol. 4, April 2014*, "Detection **and Control of Vampire Attacks in Ad-Hoc Wireless Networks".**