IJRDET

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 2, Issue 6, June 2014)

Survey of Wireless Sensor Network Vulnerabilities and its Solution

Poonam Khare [1], Sara Ali [2]

[1]M. Tech. (IS), NIT Bhopal, Madhya Pradesh, India.
[2]IEEE Member, M. Tech. (IT), IIIT Bangalore, India.

Abstract — with the advent of new emerging technologies it has been observed that there is a high increase in attacks .The latest technology which is being widely used is wireless sensor network. WSN is one of the most widely used technologies. WSN is of two types 1) Infrastructure based 2) Infrastructure less network. It offers a great deal of promise by providing features like cost effectiveness, flexibility, scalability etc. As this network is wireless they dynamically change their topology and do not have any central point of contact which allows the nodes to join and leave the network at any given time which leaves the network vulnerable and gives the attacker an opportunity to Spoof the nodes, gain sensitive information and use the same against the network.

Through this paper we have tried to target attacks like Wormhole, Spoofing while safeguarding the security. This paper even focuses on traffic related problem and suggests a solution for the same

***Keywords* — Spoofing, WSN, Attacks, Wormhole, VPN, Traffic Analysis, DOS**

I. INTRODUCTION

The WSN is an approach which performs communication using sensor nodes. A WSN is a network comprising of cheap and simple processing devices(sensor nodes) which are equipped with environmental sensor for sensing temperature, humidity etc[4].A sensor networks is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. These sensor nodes consists of data processing, messaging and communication components [16].The WSN give sensors the independence to relocate at will resulting in a dynamic network . As this network is wireless they dynamically change their topology and do not have any central point of contact which allows the nodes to join and leave the network at any given time as they are joining and leaving the network. A particular node can behave both as a sender and receiver. [17] This leaves the network vulnerable and gives the attacker an opportunity gain sensitive information and use the same against the network hence the network requires security.

By various studies we concluded that WSN suffers from three major drawbacks: 1) WSN is too vulnerable to attacks like spoofing, wormhole, black hole attacks etc. 2)WSN suffers from traffic related problems like small routes will have high traffic as a result network utilization goes down. 3) As there is no infrastructure as such for WSN so no central point is there which can mark as an authentication point for them, any node can join or leave whenever they want. Keeping all the point into consideration, this paper covers various aspects like authentication, spoofing, wormhole attacks and traffic management.

Section II deals with authentication and spoofing, Section III study about wormhole attacks and traffic problems, Section IV related work, Section V problem statement, Section VI solution, algorithm and flowchart and section VII conclusions.

II. AUTHENTICATION AND SPOOFING

Authentication is the process of actually confirming the identity. It is not a major problem in the wired networks as there is a central point which serves as an authentication point for all the nodes. Any node or device taking part in the communication is identified by a unique address [15] but since WSN is an infrastructure less network, authentication is the first and the major issue for WSN. Lack of authentication gives rise to spoofing attacks in which intruder node sends messages to a node by using the identity of some other legitimate node [17]. The intruder modifies the packet header such that it appears that the packets are coming from a trusted node [17].

III. WORMHOLE ATTACK AND TRAFFIC PROBLEM

WSN Attack classification: 1) Passive Attack 2) Active Attack. These attacks are classified as mentioned in Figure 1 [14].

Passive Attack

The Passive attacks centers around the idea of gaining information about the WSN and the sensor data it is collecting without being discovered.

It continuously monitors the target nodes and collects enough information to launch a future Active attack. They are of two types Eavesdropping and Traffic analysis

Active Attack

The attacker gains information about the network using passive attack and then launches an active attack. They are a large number of active attacks that a attacker can employ to attack a WSN. They are classified into two types Flooding Network and Routing Procedure.

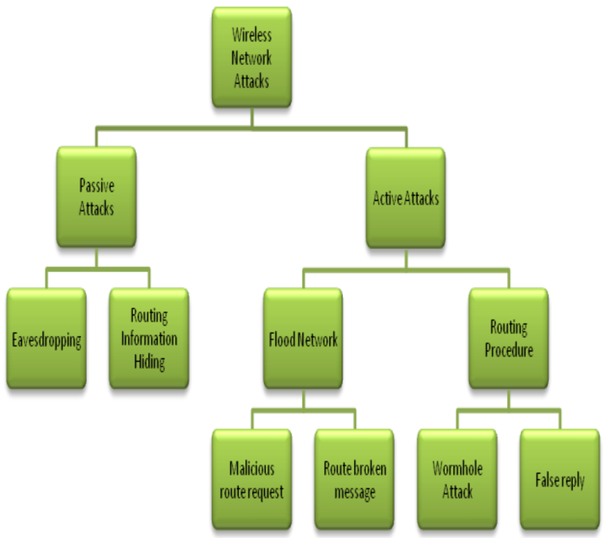


Figure 1: WSN Security Classification [14]

Our research from multiple papers concludes the most dangerous of all attacks is the wormhole attack.

Wormhole Attack

The wormhole attack is one of the most dangerous attacks in the wireless network. Two or more Malicious nodes can collaborate together to forms a low latency tunnel link and it re transmits them in different parts of the network. The Architecture of the wireless network allows the malicious nodes to create a wormhole link even for the packets which are not addressed to them by overhearing them and can transmit the same to the other malicious node present at the other end of the network, thereby creating an illusion that these two nodes are physically very close each other.

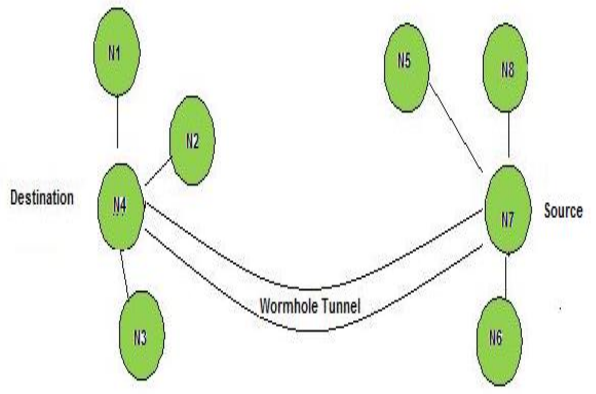


Figure 2: Wormhole Attack [14]

This disrupts the routing as nodes get an impression of a low cost link consisting of 1 or 2 hops as opposed to multiple hops .This attacks are very dangerous and are difficult to detect as these tunnels are private and out of bound and won't be visible to the WSN. These attacks are particularly very dangerous and hard to detect when routing protocols are employed where information like hop count is advertised by the nodes[14].The above Figure 2 [14] illustrates this behavior.

Wormhole and black hole attacks gives the impression to the legitimate nodes that the path/route they are providing is the shortest as a result all the traffic is diverted to the is route leading to lot of traffic on one route resulting into Denial-of-Service attacks .

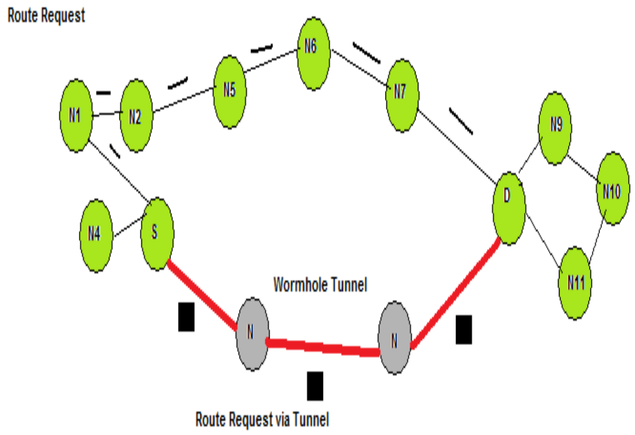


Figure 3: Route Request from Source Node of Destination in presence of wormhole Tunnel [14]

IV. Related Work

Lot of research has been done in the field of WSN, and nowadays with all kinds of survey made it was found that WSN is becoming too prone to attacks. Here is the list of related works which has been earlier done.

The author of the paper [11] proposed solution for digital investigation of wormhole attacks in WSN.[14]. In [12] authors address serious problem of wormhole and gave solution. Nouri, et al. [13] gave a one-hop vicinity method as a solution to wormhole attacks. In paper [4] authors gave a detail study of wormhole attacks and the related work done in that area. With all the studies done, this paper concludes that up till now very less work is done in detection, prevention, traffic monitoring and authentication of WSN [14].

V. Problem Statement

a) Detection and Prevention of Wormhole attacks. b) Traffic monitoring and authentication in WSN

Our research from multiple papers conclude the most dangerous of all attacks is the wormhole attack. Our paper prevents and detects wormhole attack by creating a VPN(virtual private network) which plays an important role in providing authentic registry into the network.

With the help of threshold mechanism we are able to provide traffic management. With the flag monitoring system this paper can handle and monitor the suspicious activities going on in the network. With all these parameters taking into account our paper presents an algorithm and a flowchart which provides a solution to the problem of wormhole attack.

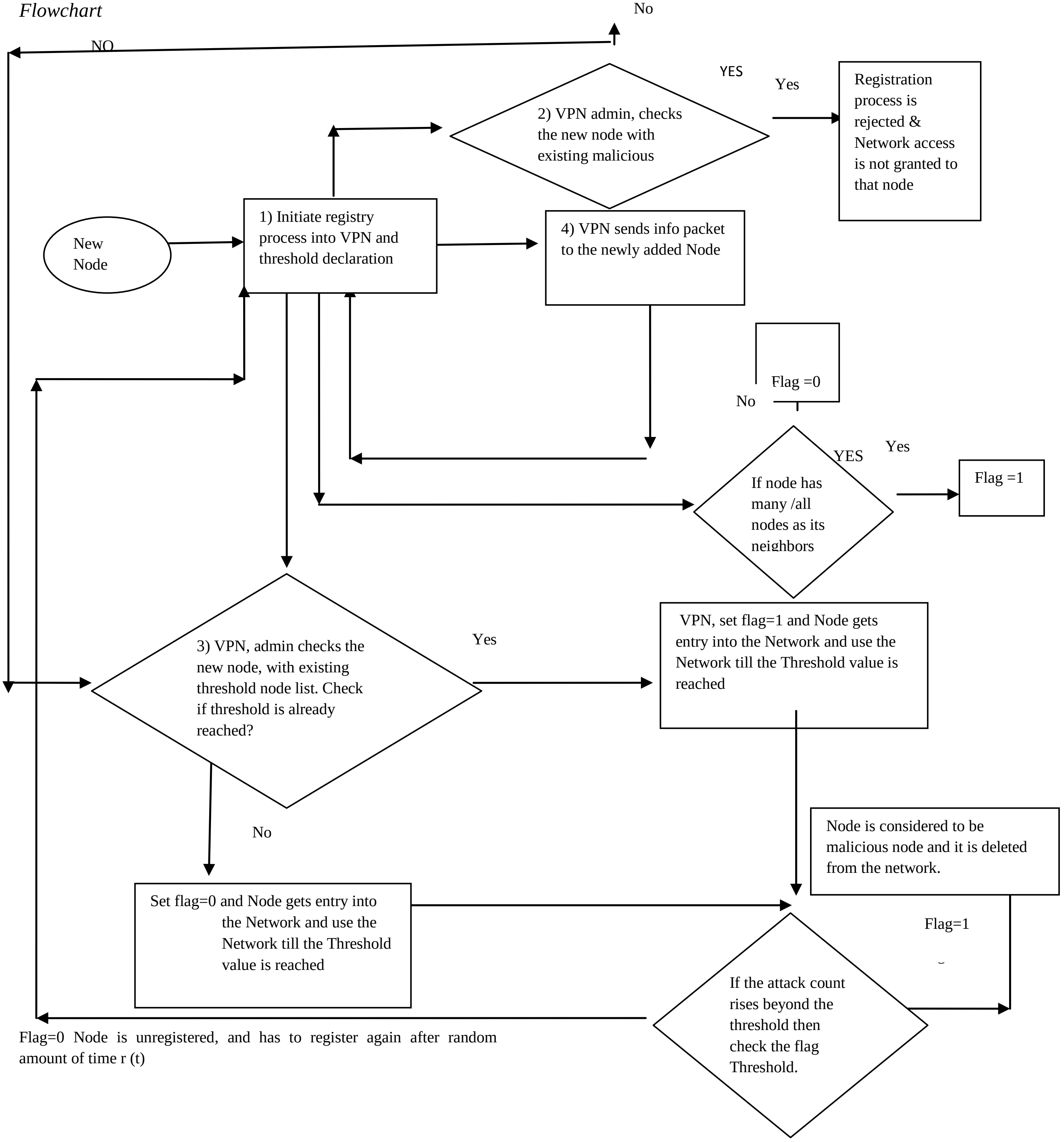
VI. Assumptions, Flowchart And Algorithm

Assumptions

VPN maintains a record of all the malicious and threshold reaching nodes. It also maintains the status of flags.

- All nodes have to pass through VPN and get them registered.
- VPN at the time of registry will give them the threshold value (which is no of times a particular node can be used for routing purpose) and checks whether the node was earlier rejected because of the threshold status, if so set the flag to one, it not so set it as o.
- If threshold of a node increases and check Flag is o then that node is unregistered by the VPN and the node again had to register after random amount of time say r (t).
- If threshold of a node increases and check Flag is 1 then that node is considered to be malicious node and it is deleted from the network.
- After every registry, an info packet is circulated in the network and sent to that node and the node specifies its no of neighbours within the hop count one, when the node fills this information then info packet is sent back to the VPN.
- A strict monitoring is done to that nodes which has many or almost all nodes in the hop count of one, set flag to 1 and if any suspicious behaviour is found then we can directly unregistered them, before the value of threshold reaches.

Flowchart


No
NO
YES
Yes
2) VPN admin, checks the new node with existing malicious
Registration process is rejected & Network access is not granted to that node
New Node
1) Initiate registry process into VPN and threshold declaration
4) VPN sends info packet to the newly added Node
Flag =0
No
YES
Yes
If node has many /all nodes as its neighbors
Flag =1
3) VPN, admin checks the new node, with existing threshold node list. Check if threshold is already reached?
Yes
VPN, set flag=1 and Node gets entry into the Network and use the Network till the Threshold value is reached
No
Node is considered to be malicious node and it is deleted from the network.
Set flag=0 and Node gets entry into the Network and use the Network till the Threshold value is reached
Flag=1
If the attack count rises beyond the threshold then check the flag Threshold.
Flag=0 Node is unregistered, and has to register again after random amount of time r (t)

Algorithm

- Create a VPN (virtual private network).
- Registry of all nodes.
- Circulation of the packet by the VPN to the newly registered node, filling of info packet by registered node.
- When info packet reaches VPN, if many neighbours are their of that particular node, set flag 1 and continuously monitor them, if some suspicious behaviour is found and automatically unregistered that node.
- VPN continuously monitors the threshold and any node meets that threshold, then check below
- If threshold of a node increases and also check its flag if it is set to 0, then that node is unregistered by the VPN and the node again had to register after random amount of time say r(t) and if Flag is 1 then that node is considered to be malicious node and it is deleted from the network.
- Threshold value = no of times a particular node can be used for routing purpose
- Flag is set either to 1 or 0
- Set Flag = 1 for suspicious nodes, else Flag = 0 for normal nodes.

Info packet = $\boxed{\text{No of neighboring nodes}}$

VII. Conclusion

Importance of this paper lies in algorithm which not only prevents the system from harmful attacks, it also detects malicious nodes and it also corrects the system by deleting the malicious nodes from the network. Our paper also gives a solution for traffic management by giving a threshold factor taking into account .The use of VPN improves the authenticity of the network, as all the nodes had to pass it before making their entry in the network. As a whole, our paper focus on prevention and detection of wormhole attacks along with a solution for traffic.

REFERENCES

[1] An Introduction to Wireless Sensor Networks Bhaskar Krishnamachari

[2] Wireless sensor network survey By Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal

[3] MANET(Mobile ad hoc network)- Characterics and Features

[4] Wormhole Attacks in Wireless Networks By Yih-Chun Hu, , Adrian Perrig, and David B. Johnson

[5] Wormhole Attack in Wireless Ad Hoc Networks:Analysis and Countermeasure ByMajid Khabbazian, Hugues Mercier and Vijay K. Bhargava

[6] The Wormhole Routing Attack in Wireless Sensor Networks (WSN) By Lukman Sharif* and Munir Ahmed

[7] Alzaid, Hani and Abanmi, Suhail and Kanhere, Salil and Chou, Chun Tung (2006) Detecting Wormhole Attacks in Wireless Sensor Networks. Technical Report, Computer Science and Engineering School - UNSW, The Network Research Laboratory - UNSW

[8] A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks Radha Poovendran, Loukas Lazos

[9] Network Security Using Cryptographic Techniques Sumedha Kaushik and Ankur Singhal

[10] International journal of innovative research in computer and communication engineering.

[11] Bayrem Triki, Slim Rekhis and Noureddine Boudriga, ―Digital Investigation of Wormhole Attacks in Wireless Sensor Networks‖, IEEE 2010, pp 179-186.

[12] Thanassis Giannetsos, Tassos Dimitriou and Neeli R. Prasad, ―State of the Art on Defenses against Wormhole Attacks in Wireless Sensor Networks‖, IEEE 2009, pp 313-318.

[13] Mahdi Nouri, Somayeh Abazari Aghdam and Sajjad Abazari Aghdam, ―Collaborative Techniques for Detecting Wormhole Attack in WSNs‖, IEEE 2011, pp 1-6.

[14] An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach Saurabh Ughade, R.K. Kapoor and Ankur Pandey

[15] Adhoc networks :filter based addressing protocol, Tanaya Mehendale,Y.D.Chincholkar

[16] A novel deterministic key pre distribution schemes for wireless sensor networks, Mahesh , Sachin, Snehal, Rajkumar and Suryakant

[17] Comparative review study of security of ARAN and AODV routing protocols in manets, Er Ruby Goel and Er M eenakshi Mittal.