ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Analysis of Wormhole attack Detection and their Prevention Techniques

Sara Ali, DR S Krishna Mohan

PhD Research Scholar, Computer Science, Mewar University, Mewar Rajasthan, India

Research Guide, Faculty of Computer Science, Mewar University, Mewar Rajasthan, India

ABSTRACT: Wireless Networks is one of the most widely used technologies which have grown tremendously over the last decade. Though it offers a tremendous potential and promise by providing features like features like cost, scalability effectiveness, flexibility, etc. but the dynamic nature of the network leaves it vulnerable to several attacks.
In this research we have laid special emphasis on attacks like flooding, wormhole, etc .We have tried to compare different techniques which have been implemented or are under research and have suggested a solution for the problem by employing a VPN (Virtual Private Network) along with a set of Observer nodes to monitor the behaviour of the system and its respective nodes and report any if malicious behaviour occurs to the VPN

KEYWORDS*:* Wireless Network, Attacks, Wormhole, VPN

I. INTRODUCTION

A common problem being faced by the users and implementers of wireless networks [1] is of security. The current system employs insufficient security measures. We are aware the role security plays in delivering next generation wireless multimedia applications. Hence we have tried to explore alternate avenues to enforce security mechanisms

The security requirements [2], [3], [4] of a wireless network can be classified as follows:

A. Data Confidentiality
In a wireless network confidentiality refers to keeping information secure and not letting any data leaks to the neighboring nodes. It plays a crucial role in military applications as the data stored in the network node is highly sensitive. It is therefore very important to build a highly secure network.
B. Data Integrity
Data Integrity is needed to certify that the message have not been altered or tampered with.
C. Data Authentication
Data Authentication is required to certify the reliability of the message by identifying its origin [4] .A corrupted node can not only change a single packet but might also alter the entire data stream by injecting additional packets. Authentication is needed to verify if the data is sent from the claimed sender or not.
D. Data Freshness
Data freshness is required to ensure that the data is up to date and ensure that no old messages are being replayed in the network. While dealing with encrypted network the keys needed to be changed over a period of time for this gives an opening to the attacker to use replay attack.
E. Data Availability
Availability is used to find out if the node can communicate by using the resources available in network. If a failure takes place, the issue of availability will cause a threat to the entire network. Thus for a functional network availability plays a very important role.

Attacks in a computer Network can be generally classified [1] as modification, fabrication.
Interruption and interception,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

- **Modification**: Attack to the integrity of the network .In this case the adversary not only gains access to unauthorized information but even it also modifies the information. In certain cases it might also inject service attacks like flooding the network within correct data.

- **Fabrication** :The Attacker injects false information by compromising authenticity of information transferred

- **Interruption:** The Attacker targets the network supply, for instance corrupts messages, inserting a malicious node into the network etc.

- **Interception:** The Attacker attacks the confidentiality of the network. It can be achieved by gaining unauthorized access to the network.

Wireless Network Attack Classification

Passive Attack

The Passive attacks gains information about the Network by collecting sensitive data and not being discovered. It monitors the target nodes continuously, collects enough information to organize a future Active attack. They are of two types Eavesdropping and Traffic analysis

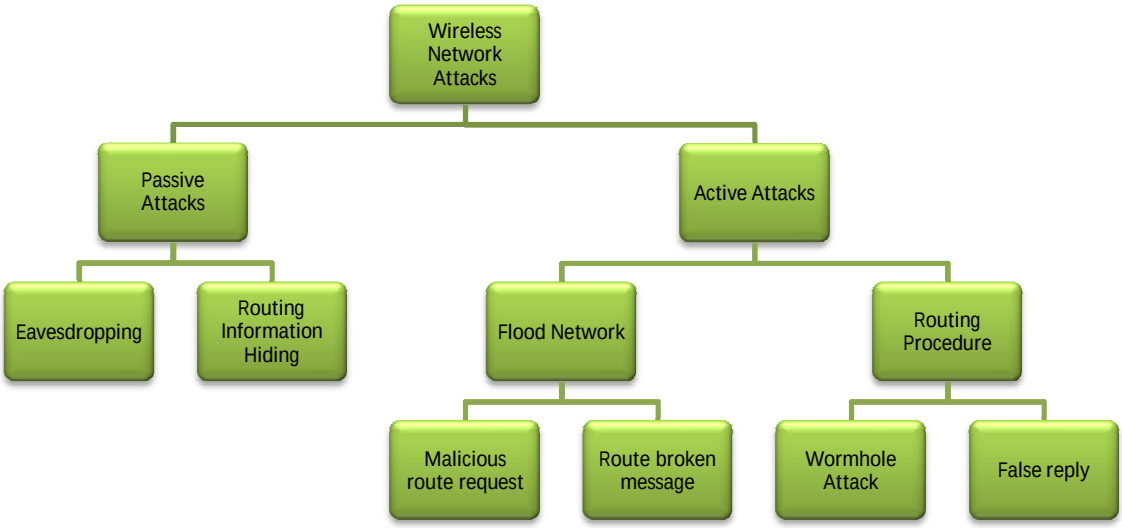
Active Attack

The attacker collects information about the network by using passive attack and then launches an active attack. It disrupts the normal flow of the network by replay of old messages or may cause denial of service attacks or injecting false data

They are a various types of active attacks that an attacker can employ to attack a Wireless Network. They are classified into two types Routing Procedure and Flooding Network and

Examples include

- Spoofing – an entity impersonating to be a different entity
- Replay –Capture and retransmit the old data
- Modification (substitution, insertion, destruction) – Alter or delete messages in the network



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

II. RELATED WORK

In [1] the authors conduct a survey on the wormhole attacks .The wormhole attacks are classified based on the modes of the attacks also they talk about the current situation in terms of prevention and detection of these attacks. Also the paper talks about the various ongoing research works related to this attack.

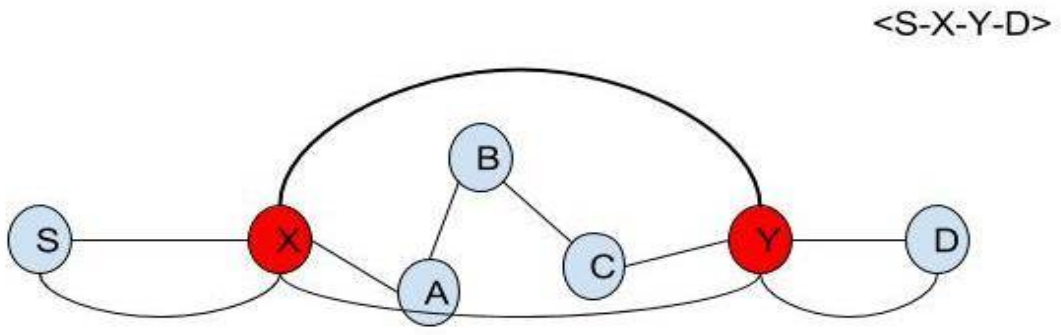
In [3] the author discusses the need for effective security mechanisms for the wireless sensor networks. The sensor networks interact with sensitive data and tend to operate in hostile environments which make them vulnerable to security attacks. The author surveys the major topics in the wireless sensor network security, and presents the obstacles and the requirements in the sensor security, while classifying the various security threats and lists their corresponding defensive measures.
In [4] the author discusses the security threats faced by the wireless sensor network. The ad-hoc nature and the limitations in terms of resources in terms of the sensor networks are discussed here. The author proposes a secure triple-key management scheme to provide resilience security against attacks in sensor networks.

III. CLASSIFICATION OF WORMHOLE ATTACKS

The Wormhole Attacks can be classifed[5] into 3 types

1. Open Wormhole attack
2. Closed Wormhole Attack
3. Half open wormhole attack.

1) Open Wormhole Attack:
In case of an Open wormhole attack the malicious nodes include themselves as a part of the RREQ packet header in the stage of route discovery. The other nodes are aware of these colluding parties to be lying in the path and think of them as direct neighbours.



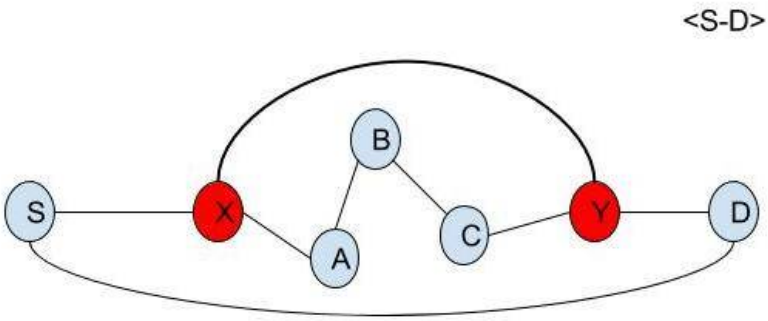
2)Closed Wormhole Attack:
The attacking malicious nodes do no alter the packets in the route discovery; they just tunnel the packet from one end of the wormhole to the other.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

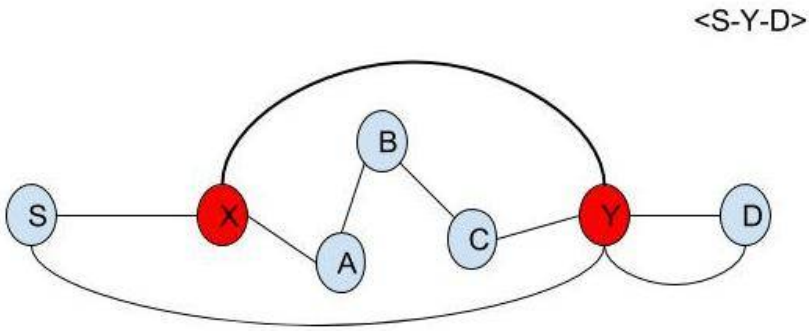
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016



3)Half Open Wormhole Attack:
One end of the wormhole does not modify the packet and while the other half modifies the packet following the packet route discovery process



IV. A BRIEF SUMMARY OF WORMHOLE DETECTION TECHNIQUES

The table below indicates the various techniques which have been either implemented or are under research for detecting and preventing the wormhole attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Techniques	Advantages	Disadvantages
Distance and location based approach to detect wormhole geographical and temporal in	Both the techniques are employed where strict clock synchronization and global positioning system coordinate all nodes	Restrict the transmission distance of packet and need the nodes to be tightly synchronized
Directional Antenna	Requires less synchronization.	Each nodes needs to be equipped with a special hardware and may result in directional errors and requires encryption
LITEWORP	Guard node or Observer nodes are used to detect the wormhole if one of its neighbor is behaving maliciously	Utilizes large memory space.
Techniques	**Advantages**	**Disadvantages**
Graph Theoretical	Approach Uses encryption techniques	Guard node uses local broadcast keys which are available only in one hop neighbors.
Cluster based detection techniques	1. Guard nodes are used to inform cluster heads about the attack. 2. No special hardwires are used.	It is only applicable for layered architecture of the network.

V. PROPOSED ALGORITHM

VPN

A Virtual Private Network is a technology used to secure the network which creates an encrypted network over an less secure network, when the underlying network fails to do so.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Observer Nodes

Network Nodes which are concerned with monitoring the network performance and detecting any security breaches

1. VPN build on top of it which maintains a record of all nodes present in the network and maintains a malicious list. The system contains observer nodes which constantly monitor the network at random interval of time.
2. VPN maintains a record of all the malicious and threshold reaching nodes. It maintains the status of malicious threshold flag.
3. All Nodes need to get authenticated by the VPN to enter the network
4. VPN assigns a unique identifier to the node and during the registration phase checks if the node was previously
5. Detected as malicious node and set malicious threshold flag to zero.
6. Once the node enters the network the information is shared with the observer nodes.
7. The observer nodes constantly monitor the network at random time *t*.
8. Once the node is detected as malicious it is reported to the VPN which assigns a malicious threshold flag
9. This gets incremented whenever the observer nodes report the node to be malicious.
10. When malicious threshold flag is greater than or equal to 1 it is removed from the network and the node
11. With its unique identifier number and IP address gets added to the malicious node list

VI. CONCLUSION

The Major contribution of this paper lies in 2-Phase monitoring of the network .The first phase filters the nodes being added to the network and the second phase is involved in strictly monitoring the behavior of the nodes after they enter the network .This two level check 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. This research also gives a solution for traffic management by giving a threshold factor, taking the malicious behavior of nodes into consideration. The use of VPN improves the authenticity of the network, as all the nodes have to pass it before making their entry in the network. As a whole, our paper focuses on prevention and detection of wormhole attacks along with a solution for traffic.

REFERENCES

1. Ali, Sara, and S. Krishna Mohan. "Enhanced Security Framework for Wireless Networks." *International Journal of Advanced Research in Computer Science* 6.7 (2015).
2. Zheng, Jun, and Abbas Jamalipour. *Wireless sensor networks: a networking perspective*. John Wiley & Sons, 2009.
3. Jangra, Dr Banta Singh, and Vijeta Kumavat. "A Survey on Security Mechanisms and Attacks in Wireless Sensor Network." *International Journal of Engineering and Innovative Technology (IJEIT)* 2.3 (2012): 291-296.
4. Zia, Tanveer, and Albert Zomaya. "A secure triple-key management scheme for wireless sensor networks." *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*. IEEE, 2006.
5. Sharma, Priyanka, H. P. Sinha, and Abhay Bindal. "Detection and Prevention against Wormhole Attack in AODV for Mobile Ad-Hoc Networks." *International Journal of Computer Applications* 95.13 (2014).

BIOGRAPHY

Sara Ali is a Research Scholar in the Computer Science, Mewar University GANGRAR, CHITTORGARH. She received Master In IT from IIIT Bangalore .She is currently working as an Associate Professor at Shadan College of Engineering and Technology