ISSN No. 0976-5697

Volume 6, No. 7, September-October 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Enhanced Security Framework for Wireless Networks

Sara Ali
PhD Research Scholar, Computer Science
Mewar University Gangrar, Chittorgarh
Hyderabad, India

DR S Krishna Mohan
Principal
Siddhartha Institute of Engineering & Technology
Hyderabad, India

Abstract: Wireless Network is one of the most widely used technologies .It offers a great deal of promise by providing features like cost effectiveness, flexibility, scalability etc. As this network is wireless it dynamically changes it's topology and does 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. The Rapid advances in the technology have considerably increased the risks for security.
This research contributes to target attacks like Wormhole, Flooding while safeguarding the security and focusing on traffic related problem and suggests a solution for the same by employing a Virtual Private Network(VPN) and Observer Nodes which filters the nodes that enter into the system and a set of observer nodes which monitor the behaviour of the nodes ,the messages being exchanged and the traffic status ,using these metrics they decide the authenticity of the nodes and report the behaviour to the VPN if found malicious.

Keywords: Computer Network; Security; VPN; Wormhole; Flooding

I. INTRODUCTION

Mobile and wireless systems are concerned with two areas of communication which include Mobility and Computing.

Mobility is concerned with providing continuous accessibility to the users, while wireless communications deals with providing communication without using wires.
A Wireless Network technology like IEEE 802.11 helps in achieving a great deal of flexibility in terms of mobility and cost saving [1].

Some of the major application of Wireless Networks includes

II. WIRELESS NETWORKS & THEIR APPLICATIONS

Cellular networks: A Wireless network comprising of large number of cells where each cell has its own transmitting antenna. A base station in a cellular network comprises of transmitter, receiver, and control unit.

The cells are arranged in a fashion to have all the neighboring antennas equidistant from each other.

Cells are allocated different frequency to avoid interference or crosstalk.

E.g.: Cellular phones, PDAs, Palm Pilot

Wireless LAN: Wireless LAN or Wireless Local Area Network refers to the local area network which does not need wires to communicate with different devices; instead it uses Radio waves and IEEE 802.11 for communication. Wireless LAN comprises of an Access Point (AP) which is nothing but a wireless LAN transceiver which serves as the focal point of a standalone network or acts as the linking or connection point between a wired and wireless network [2],[3]. It has simplified the networking domain by enabling multiple computing devices to simultaneously communicate without incurring additional cost of wires
Main features of Wireless LAN include

- Flexibility of Location
- Roaming capability
- Cost Effective
-

Adhoc Networks: A Wireless Ad hoc network (WANET) is a decentralized type of network. It does not have any pre existing infrastructure. The network is built as and when the devices connect simultaneously.

It can be created for a short time where a group of people come together to share some information. It has a very limited range E.g.: Bluetooth

Wireless Sensor Networks: The WSN is an approach which performs communication using sensor nodes. A WSN is a network comprising of economical and simple processing devices (sensor nodes), which are equipped with environmental sensors for sensing temperature, humidity etc. 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 [4].The WSN gives sensors the independence to relocate at will, resulting in a dynamic network . As this network is wireless, the sensors dynamically change their topology and do not have any central point of contact which allows the nodes to join and leave the network.

The major applications of wireless sensor network are

- Seismic Monitoring
- Habitat and Ecosystem Monitoring

- Civil Structural Health Monitoring
- Monitoring Groundwater Contamination
- Rapid Emergency Response
- Industrial Process Monitoring
- Perimeter Security and Surveillance
- Automated Building Climate Control

With an increase in the usage of wireless network technology a common problem
Which is being faced with many implementers is of security. The major reason for the concern is insufficient security measures incorporated in the current system. Security plays a very important role in delivering next generation wireless multimedia applications. The current issue plays a vital role in exploring alternate avenues to enforce security mechanisms

III. WIRELESS NETWORKS SECURITY REQUIREMENTS

With an increase in the usage of wireless network technology a common problem
Which is being faced with many implementers is of security. The major reason for the concern is insufficient security measures incorporated in the current system. Security plays a very important role in delivering next generation wireless multimedia applications. The current issue plays a vital role in exploring alternate avenues to enforce security mechanisms

The security requirements [5], [6], [7] of a wireless network can be classified as follows:

A. Data Confidentiality
Data confidentiality is the most import concern in network security. In a security enabled network this is the issue which is addressed first. In wireless network confidentiality is related to keeping information secure and no leaking any information 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 which wills also encrypt a part of public data against traffic analysis attacks

B. Data Integrity
Data Integrity is required in the wireless network to certify that the message has not been altered or tampered with.

C. Data Authentication
Data Authentication is needed to certify the reliability of the message by identifying its origin [7] .A malicious node can not only alter a single packet but might also change the entire data stream by inducing additional packets. Authentication is required to verify whether the data is sent from the claimed sender or not.

D. Data Freshness
Data freshness is needed to ensure that the data is recent and ensure that no old messages are being replayed in the network. In case of an encrypted network the keys needed to be changed over a period of time this gives an opportunity to the attacker to use replay attack. This problem can be addressed by adding a counter to the packet to ensure data freshness.

E. Data Availability
Availability is the measure to determine whether the node can communicate by using the resources available in network. In case of failure of the base station the issue of availability will cause a threat to the entire network. Thus for a functional network availability plays a very important role.

One of the major concerns is the transmission of sensitive data between neighboring nodes in a hostile environment. A good design approach would incorporate the security measures [5], [6], [7] while considering the computing constraints in network node.

Attacks in a computer Network can be generally classified [9] as interruption, interception, modification and fabrication.

- **Interruption** is the process of attacking the network supply, for instance corruption of messages, inserting a malicious node into the network etc.

- **Interception** is the process of attacks the confidentiality of the network. This can be achieved by gaining unauthorized access to the network.

- **Modification** is the process of attacking the integrity of the networking this case the adversary not only gains access to unauthorized information but even modifies the information. In some cases it might event inject service attacks like flooding the network within correct data.

- **Fabrication** is the process of injecting false information by the adversary and compromising authenticity of information transferred

Wireless Network Attack classification
Our research from multiple papers concludes the most dangerous of all attacks [12], [13], [14] is the wormhole attack.
The classification of attacks in the WAN lies in differentiating an active attack from a passive attack

Passive Attack

The Passive attacks centers around the idea of gaining information about the Network collecting sensitive data 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

These attacks though easy to realize are very difficult to detect as the attacker does not many any changes to the network.

Examples include

- Eavesdropping message contents

- Traffic analysis-Gain knowledge of the data being transferred in the network by observing the communication characteristics

Active Attack

The attacker gains information about the network using passive attack and then launches an active attack. The attacker

gains access to the network while disrupting the normal flow of the network by injecting false data, replay of old messages or may cause denial of service attacks
They are a large number of active attacks that an attacker can employ to attack a Wireless Network. They are classified into two types Flooding Network and Routing Procedure.

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

IV. RESEARCH MOTIVATION AND RELATED WORK

This Research involves extensive study on the security breaches involved in a wireless network. This research contributes to target attacks like Wormhole, Flooding while safeguarding
The security and focusing on traffic related problem and suggests a solution for the same.

In [1] the Author discusses the security shortcomings of a wireless sensor network .The author propose using Firewall along with VPN technology. A virtual private network helps in establishing a secure path between different WSN networks while the firewall filters the incoming packets within the network. Tunneling further helps in adding additional headers facilitates virtual lease line while techniques like cryptographic, secure the private information being exchanged in the public Internet.

In [2] the author discusses the growth of WLAN in the last three decades. These networks come under the category of small scale networks which has given rise to the development of wireless technologies. Performance plays a very important role in computer networks and author concentrates on the performance evaluation of the networks. This research presents a comparison and evaluation of transmitting multimedia over the wireless LAN in three different scenarios using OPNET simulator
In [4] the author analyzes the harmful effect of wormhole attacks on shortest-path routing protocols for the wireless adhoc networks. The author through simulation results shows that the wormhole attacks can disrupt the networks total communication by 32% on an average. The author shows how to evaluate the maximum effect of the wormhole attack on the network. The author suggests a timing-based countermeasure that overcomes the deficiencies of the existing timing-based solutions which will safeguard the network against the wormhole attacks.
In [6] 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 [7] 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.

In [8] the author discusses the various methods of enabling security in the wireless sensor networks. It investigates the security challenges and reviews the existing security mechanisms .These comparisons helps in arriving at a holistic approach to incorporate layered security which will result in a robust network.

V. ASSUMPTIONS,FLOWCHART AND ALGORITHM

VPN
A Virtual Private Network [10], [11] is a technology used to secure the network which creates an encrypted network over a less secure network, when the underlying network fails to do so.

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

Assumptions

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 also 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 detected as malicious node and set malicious threshold flag to zero.

5. Once the node enters the network the information is shared with the observer nodes.

6. The observer nodes constantly monitor the network at random time *t*.

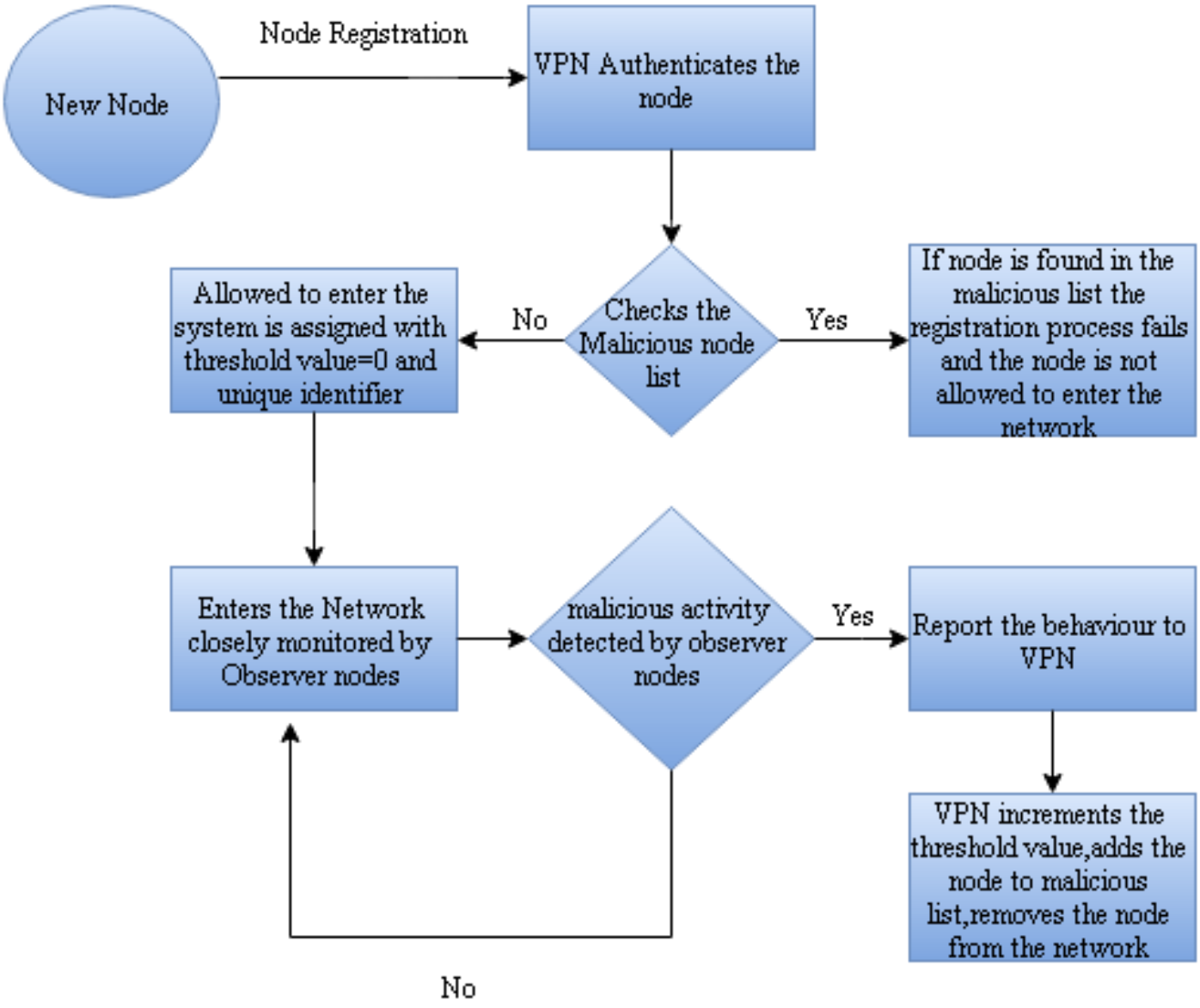
7. Once the node is detected as malicious it is reported to the VPN which assigns a malicious threshold flag

8. This gets incremented when ever the observer nodes report the node to be malicious.

9. When malicious threshold flag is greater than or equal to 1 it is removed from the network and the node

10. With its unique identifier number and IP address gets added to the malicious node list

Flowchart



Algorithm

- Create a VPN (virtual private network).
- Create Observer Nodes
- Register the nodes and assign a Unique Identifier and Threshold value

  Uniq_id=0

  Threshold_val=0
- Initialize the Observer nodes at random time *t*
- VPN monitors the threshold and any node meets that threshold, then check below
- If node is detected as malicious by the observer node it reports to the VPN
- Threshold value > 1 node is treated as malicious node removed from the network and added to the malicious node list
- Increment Flag for suspicious nodes, else Flag = 0 for normal nodes.

VI. ACKNOWLEDGMENT

I would like to thank Dr.S Krishna Mohan Rao for his constant guidance and support. I would also like to thank all the authors whose work has helped me immensely in my current research.

The Major contribution 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.

VII. REFERENCES

[1] Malik, Aruna, Harsh K. Verma, and Raju Pal. "Impact of Firewall and VPN for securing WLAN." *International Journal* 2.5 (2012).

[2] M. M.A. Ghazala, M. F. Zaghloul, and M.Zahra, “PerformanceEvaluation of Multimedia Streams over Wireless Computer Networks (WLANs) ”,International Journal of Advanced Science and Technology Volume 13, December, 2009

[3] Malladi, Rajeswari, and Dharma P. Agrawal. "Current and future applications of mobile and wireless networks." *Communications of the ACM* 45.10 (2002): 144-146.

[4] Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava, “Severity Analysis and

Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks”, IEEE Transactions on Wireless Communications, vol. 8, no. 2, February 2009

[5] Zheng, Jun, and Abbas Jamalipour. *Wireless sensor networks: a networking perspective*. John Wiley & Sons, 2009.

[6] 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.

[7] T.A Zia and A.Y. Zomaya, “*A security framework for wireless sensor networks, in the proceedings of IEEE Sensor Applications Symposium (SAS06)*, February 7-9 2006, Hoston, Texas, USA.

[8] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, “Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey” Journal of Theoretical and Applied Information Technology, 2010, PP. 14-27.

[9] Messai, Mohamed-Lamine. "Classification of Attacks in Wireless Sensor Networks." *arXiv preprint arXiv:1406.4516* (2014).

[10] Liu, Alex X., and Fei Chen. "Privacy preserving collaborative enforcement of firewall policies in virtual private networks." *Parallel and Distributed Systems, IEEE Transactions on* 22.5 (2011): 887-895.

[11] Jayarekha, P., Sunil Kalaburgi, and M. Dakshayini. "SECURITY AND COLLABORATIVE ENFORCEMENT OF FIREWALL POLICIES IN VPNS."

[12] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks." *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. Vol. 3. IEEE, 2003.

[13] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Wormhole attacks in wireless networks." *Selected Areas in Communications, IEEE Journal on* 24.2 (2006): 370-380.

[14] Stallings, W., (2000) Cryptography and Network Security Principles and Practice, Cryptography Book, 2nd Edition, Prentice -Hall, 0 -13-869017-0