Proceedings of the 11th INDIACom; INDIACom-2017; IEEE Conference ID: 40353
2017 4th International Conference on "Computing for Sustainable Global Development", 01st - 03rd March, 2017
Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)

Comparative study on Wireless threats and their Classification

Md. Alimul Haque
Department of Physics
V.K.S.University,Ara,
shadvksu@gmail.com

Anil Kumar Sinha
Department of MCA
V.K.S.University,Ara
sinha.anil03@gmail.com

M.U. Bokhari
Department of Computer Science
A.M.U. Aligarh, India-202002
mubhokhari@gmail.com

N.K. Singh
Department of Physics
V.K.S.University,Ara
singh_nk_phy27@yahoo.com

Abstract - The wireless network technology is growing and has greatly benefited for human being, but has helped to bring about unscrupulous, amoral and conscienceless packets. Particularly one, who has inclination to exploit others, uses the technology for one's nefarious purpose. Sniffing, spying, data blocking and stealing both information and capital are various forms of wireless threats. And these threats are increasing rapidly in all the way over the network a couple of year back. So there is a demand to complete intellect of these threats and its classification. The main motive of this study is to do a complete resolution of these threats in order to prepare alertness about the several types of attacks and their mode of action so that effective countermeasures can be invoked against them particularly concentrate on highly ambitious Wireless networks.

Keywords – Active attacks, DoS, Passive attacks, Wireless Threats

I. INTRODUCTION

Wireless network technology is one of the upcoming techniques in the digital world. These systems are used in various architecture like including dedicated networks, cellular networks, and Ad-hoc networks [1]. Especially Ad-hoc networks are facing huge amount of unauthorized access. The problems posed by the organization to each of these engineering are unparalleled especially for healthcare and defense applications. Such type of wireless network threats is adding to intricacies like disseminating misinformation, crippling the technical services, having access to valuable and highly secret information, pirating the data and influencing economic activities.[2]

With the passes of time such intricacies are spreading their wings. In spite of ever widening complication, awareness regarding the threatening issue is lacking among the people.

Ignorance about type and mode of threats is common. Defiance services is at stake. The industries are facing risk. The security of a country is at risk. Therefore proper guidelines and understanding is need of the time. It also requires such tools which may safeguard their security.

II. PURPOSE AND MOTIVATIONS OF WIRELESS NETWORK THREATS

The intention and aims of the threats need to be identified. It involves certain practices, which may be described as follow[3].

A. Blocking of Information

The hacker may block the access to information. If it happen the authorized user may feel handicapped to execute his own future plan of action.

B. Holding up Decision Making Process

Threats may hinder the emergency service affecting directly decision making process. It may result in big loss or defeat.

C. Denial in Providing Public Services

Hackers can block or disruption in domain like online transaction system, on-line ticketing or booking and share markets. Genuine user can not access the information from server.

D. Affecting the Public trust

Due to hacking of the sensitive data, users can loss their confidence in Govt. & organization. Recently Chinese hackers hacked more than lakh ATM pin of India ATM card holders.

 ISSN 0973-7529; ISBN 978-93-80544-24-3

And they did few transactions too. These threats are like terrorism.

E. Credit of the nation will be damaged

The main purpose of wireless threats is denigrating the reputation of a nation. In this digital world developing countries enhance its prestige among other country and it's bad impact will be occur due to large scale attacks across the countries networks.

F. Smashing up Legal Interest

The main motive and purpose of wireless threats is smashing up the authorized work.

III. CLASSIFICATION OF VARIOUS THREATS IN WIRELESS NETWORKS

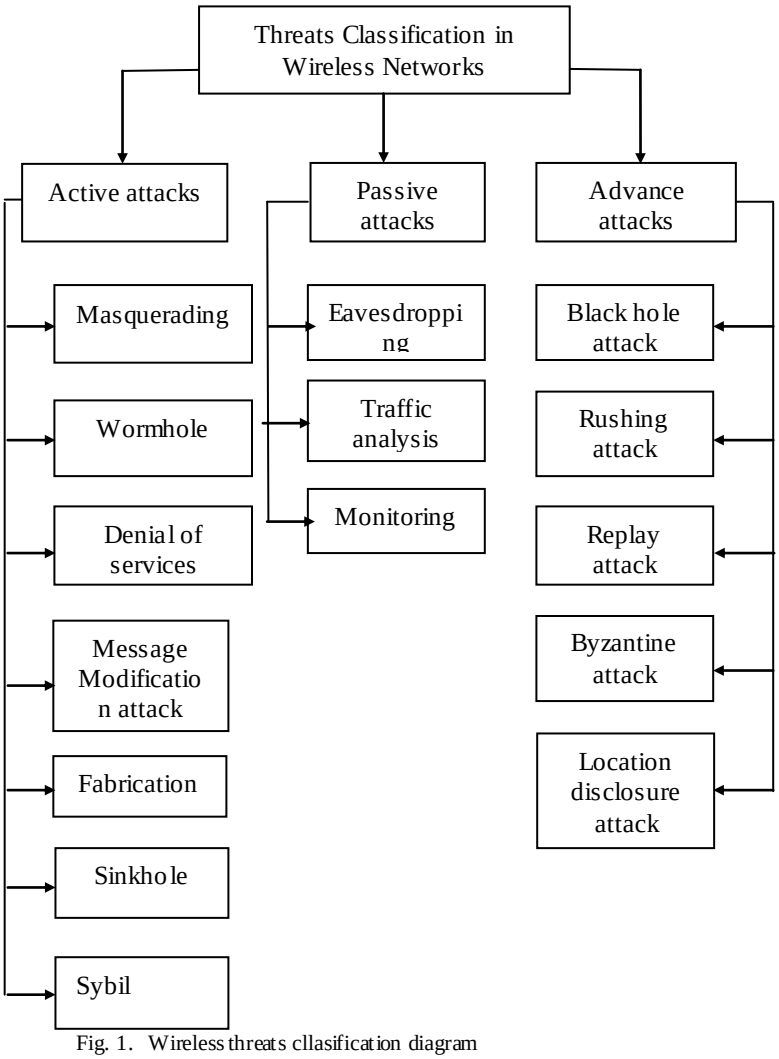

Fig. 1. Wireless threats cllasification diagram

More threats in wireless networks due to the shortage of physical infrastructural facilities. Some of the consequences of these attacks include the loss of sensitive data and network services. Wireless threats are divided into passive and active attacks[4].In passive attacks hackers monitors the traffic, but does not modify its data[5].

A. Passive attacks

(i) Eavesdropping

The attacker monitors the transmissions between a station/SS and an AP/BS[6]. These threats find out sensitive information from transmission, such information may be private or public. It also may be the key to secret and confidential planning.

(ii) Traffic analysis

Attackers can have access to the data which has been transmitted from sender to receiver but could be not edited or modified.

(iii) Monitoring

Attacker can read the secret information, but he cannot modify the message.

B. Active attack [7]

(i) Masquerading

This type of attack is actually wireless MIMA attack, where an introducer places himself between two nodes and manipulates the communication between them. In this attack a malicious node hide his identity, so that the sender change the topology

(ii) Message Modification attack

The adversarytampers the content of legitimate messages. Due to this attack delay occurred between sender and receiver transmission.

(iii) Wormhole

In a wormhole attack, an attacker creates a false out-of-band link and forwards packets and replies those packets at other node in the network through that out-of-band link. So that a beginner assumes that he found the shortest path in the network [8].

(iv) Fabrication

It generates the false routing message. This means incorrect information about the route between devices [9].

(v) Denial of services

The main motive of this attack is to be busy the network node. If a message from authenticated node, the receiver will not receive that message because receiver is busy and sender has to wait for the response.

(vi) Sinkhole

In Sinkhole a node tries to attract the data to it from his all neighboring node. This attack can manipulating, accessing or dropping of sensitive information[8].

(vii) Sybil

Malicious nodes are created in large scale resulting in enhancement of probability of threats. It someone uses multipath route, probability to select a malicious node broadens. [8, 9 and 10].

C. *Advance attacks*

(i) Black hole attack

In this attack, hacker use routing protocol. The RREQ (Route Request) and RREP (Route Reply) are generally used to interrupt data.

(ii) Rushing attack

Attacker may easily change the packet and forward to receiver. The receiver, on the other hand may think that the packets are coming from genuine sender. Thus he continuously engages himself in receiving fake packets.

(iii) Replay attack

In this attack, hackers can easily repeat and interrupted the data. It can be done by originator who detain the data and retransmit it.

(iv) Byzantine attack

In this attack a malicious node intervenes into other two nodes and execute some unethical alteration such as brining into false routing loops, sending packets through false route. Disruption may occur due to this type of attack between the two nodes and perform some unethical action such as making false routing loops, sending packet through non optimal of routing services. Due to this disruption occur.

(v) Location disclosure attack

In this attack hackers collect the data from node and monitoring the path. So it may perform more attack on the network.

IV. CONCLUSION

The major problem in wireless network is data security. Theses technologies involve almost all aspects in our day to day life. Increasing use of wireless networks also open the way of threats to hack or steal the sensitive data from govt. or private organization and that makes the country lagging behind in their further activities. During the study, we also find some dangerous threats which are directly affect life support system. This study gives proper knowledge to user about various threats, so that one can keep security measure while using wireless networks.

REFERENCES

[1] Alimul Haque, A.K. Sinha, K.M. Singh & N. K. Singh, "Security Issues of Wireless Communication Networks", *International Journal of Electronics Communication and Computer Engineering*, Volume 5, Issue 5, pp 1191-1196, 2015.

[2] Eduardo B. Fernandez, Saeed Rajput, Michael VanHilst, and María M. Larrondo-Petrie, "Some security issues of wireless systems", Journal in Computer Virology, January 2005.

[3] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification", *International Journal of Network Security*, Vol.15, No.5, pp.390-396, Sept. 2013.

[4] T. Karagiannis and L. Owens, "Recommendations of the National Institute of Standards and Technology, Wireless Network Security — 802.11, Bluetooth and Handheld Devices," NIST Special Publication 800-48, November 2002.

[5] Panagiotis Trimintzios and George Georgiou, "WiFi and WiMAX Secure Deployments", *Journal of Computer Systems, Networks and Communications*, Volume 2010.

[6] J. G. Proakis and D. G. Manolakis – *Digital Signal Processing – Principles, Algorithms and Applications*; Third Edition; Prentice Hall of India, 2003.

[7] Mohan V. Pawar and Anuradha. J, "Network Security and Types of Attacks in Network", *Procedia Computer Science* 503-506,Elsevier, 2015.

[8] Neha Khandelwal, Prabhakar.M. Kuldeep Sharma, "An Overview Of security Problems in MANET", 2015.

[9] Anupam Joshi and Wenjia Li. "Security Issues in Mobile Ad Hoc Networks- A Survey", Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County,2007.

[10] Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006.