International Journal of Computational and Electronics Aspects in Engineering
Vol. 1, Issue. 2, March 2015, Revised in June 2020, pp 75-80
https://doi.org/10.26706/ijceae.1.2.20150106

Review on Security Threats of Wireless Networks

Leena L. Nikhare[1]
leenanikhare44@gmail.com

Neha M. Nandagawali[2]
nehanandagawali@gmail.com

DMIETR Sawangi (Meghe),
Wardha-442001,
Maharashtra,India.

***Abstract*: Wireless networks are gaining popularity to get its highest and strongest level today, as the users want connectivity in terms of wireless medium irrespective of their geographic position. On the Wireless Network, there is an increasing threats, viruses and various attacks. The main goal of this paper, is to provide a survey of the wireless network and attacks that occur on the wireless network. The Design of wireless Network uses NS2, which is based on Security evaluation, and it also describes the proposed model of the system as well as complete description of the Simulations and software program needed for implementing the Wireless Network. NS2 is a very widely used tool of networks. This paper also provides an overview of routing protocols being used in wireless networks. Ad-hoc network must have a secure way for transmission and communication which is quite challenging and phrasing most issues regarding to the wireless networks. Ad-hoc network are rapidly gaining popularity because they do not depends on a pre-infrastructure and can be deployed quickly. Ad-hoc network is used from offices to modern battlefields this is the application of it. It has open secure functionality hence it uses most on private places and also for mobile communication purposes.**

Keywords: Wireless Network, AODV, NS2, Security, Trace File format Routing Protocol.

I. INTRODUCTION

Now a day, communication being a mode of sending and receiving information is gaining more popularity. There are different modes of communication one of them is wireless mode; in which communication takes place through an open medium. There are various types of wireless networks such as cellular networks, satellite networks and ad hoc mobile networks. Amongst the wireless networks 802.11 networks are the most popular. Wireless 802.11 networks can be categorized into two types: Infrastructure and Ad-hoc mode. Infrastructure based 802.11 networks have a fix backbone. An ad-hoc network is a collection of nodes which can communicate with each other without any infrastructure. Wireless medium can be accessed by both legitimate users and attackers. End users and corporations are interested in taking the advantage of this wireless medium, but this also comes with some security issues.

In this project we will be studying the routing protocols in ad-hoc wireless network using the ns2 simulation tool. Another aim is to implement attacks on access points and also attacks on network layer in ad-hoc wireless network. These attacks are carried out using backtrack cd and also by implementing tcl files in ns2 simulation tool. The last module includes the detection of attack by analysing trace file generated by ns2 simulation tool.

Technical Article
First Online on – 30 March 2015, Revised on – 30 June 2020

Cite this article – Leena L. Nikhare and Neha M. Nandagawali, "Review on Security Threats of Wireless Networks", *International Journal of Computational and Electronics Aspects in Engineering*, RAME Publishers, vol. 1, issue 2, pp. 75-80, 2015, Revised in 2020.
https://doi.org/10.26706/ijceae.1.2.20150106

II. WIRELESS NETWORK

Network is described as a network of devices which communicate by using wireless technologies [7]. Wireless communication is used as a term for transmission of information or data from one place to another. This may be one-way communication as in broadcasting systems (such as radio and TV), or two-way communication (e.g. telephone). In telecommunications, wireless Network communication is the transfer of information and without the use of wires [5].Wireless Network communication refers to any type of computer network or devices network that is commonly associated with communications wireless network to interconnections nodes.

III. AD HOC NETWORK

A. Introduction

Wireless LANs can be classified based on their mode of operation such as infrastructure and ad-hoc. Infrastructure mode has a fixed wired backbone for communicating with each other; whereas the ad-hoc mode doesn't rely on a backbone. An example of formation of ad-hoc network can be of sensor nodes present in an open atmosphere. In this network each sensor node has the capability of processing the information available to it from the atmosphere and capable of sharing this information with other nodes. Application of the ad-hoc wireless sensor network is sharing climate information such as humidity, temperature, etc. at high altitude pilgrimage place.

B. Ad hoc network characteristics

An ad hoc wireless network can be created when a group of mobile devices communicate with each other without depending on any fixed infrastructure [11]. In such cases, neighbouring nodes communicate with each other while communication between non-adjacent nodes is performed via the intermediate nodes that can act as routers. The network topology also frequently changes in ad-hoc network. Ad-hoc wireless networks are not good to route breaks that can result due to various sources such as node mobility, signal interference, high error rate and packet collision [11].

C. Routing in Ad hoc network

Routing in an ad hoc wireless network is the most important task that needs to be performed with carefully. Since nodes in ad hoc wireless network depend on intermediate or neighbouring nodes in carrying of the data so there are various routing protocols used in this process in wireless network. The main goal of routing protocols in an ad hoc network is to find shortest path between source and destination with minimum overhead and bandwidth [6]. Depending on the routing infrastructure being used they are classified as follows: proactive, reactive and hybrid.

Proactive Protocols: In proactive protocol each node present has information of complete topology [6] in the wireless network. The table is updated constantly so that they contain fresh enough information for routing process.

Reactive Protocols: In reactive protocol nodes create path on an on-demand basis process. Information about the network topology is collected only when it is needed. This avoids the overhead associated with frequent updating of routing table in each node in the wireless network [6].

Hybrid Protocols: In hybrid protocols group of nodes are formed and then the nodes are assigned different functionalities and outside the group in network. Grouping is done based on position of nodes in network[6].

D. Reactive Routing Protocols

In the type of routing protocols; reactive routing protocols are the most widely used because of their lower overhead in sharing of routing information. The main reactive routing protocols used is AODV.

IV. ATTACKS IN WIRELESS NETWORKS

Wireless networks are more influenced to various attacks because of their shared physical medium, open transmission of radio on tcp/ip protocols.. The attacks on wireless networks can be shown in diagrammatic manner in figure as bellows: frequencies [5]. 1. The release of massage content: This means that if user A transmit the some confidential email to B but the email content are released to user C against the width of user A. 2.Traffic analysis. If the encoded massage is transmitted from user A to user B. Only user A and user B can decade the massage because they know the code language. 3. Active Attack: The active attacks are those attacks in which the attacker modifies the data or performs some harmful activity that disrupts the network.

AODV is a reactive routing protocol which creates a path source to destination when needed. Routes are not creating until certain nodes send route discovery message as an intention to communicate or transmit data with each other [3]. This routing protocol uses two phases. First phase is route discovery. Second

1. Masquerade attack: A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. It trying to pose another entity evaluates a masquerade attack. In masquerading attack may involve capturing authentication sequence which later can be replaced to gain illegal access to the computer system.

Where,

G1:- Global

Inspector

B1:- Unauthorized

Unauthorized node

Sender Receiver

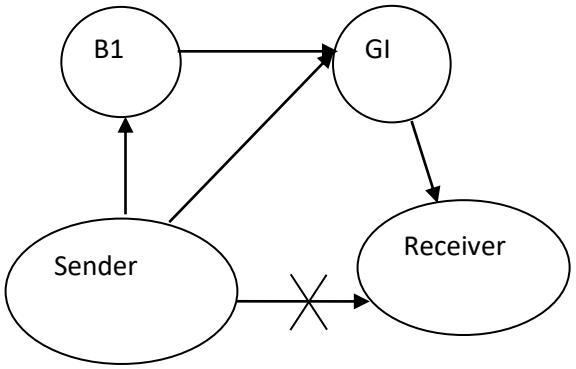

Figure 1. Network Topology

This attacker is further categories as reply attack and alternation.

i. In this attack a user captures a sequence of events or some data and resend them.

ii. Alternation of message: This involve some change to the original massage.

4. DOS (Denial of services): DOS Attacks

Denial of Service (Hard to Prevent, But These Draw Immediate Attention To The Attacker)

Example: Flooding Attacks, Disassociation Attacks

A. Attacks on Routing Protocols

Routing protocols are used by both the source nodes and the intermediate nodes in ad-hoc wireless network. The two most commonly used routing protocols are AODV and DSDV. Attacker can launch a single attack in which many fields of

AODV are modified or an aggregate attack consisting of multiple attack messages [1]. The examples of single attacks are those in which a single field of AODV is being modified to perform.

Forging Sequence number: The sequence number field in AODV messages indicates the freshness of the route to the specific node. A packet with large sequence number is generally accepted because it indicates fresh route in AODV. An attacker can exploit this vulnerability. Attacker sends a reply message with large sequence number and it causes the victim node to pass through its own node.

Sleep Deprivation: Every node in ad-hoc wireless network requires a battery to send and receive signals from it. The devices transmit signals only when there is a need to do so. An attacker can send large number of route request messages so that these devices process it and thereby reduce the battery of the devices in network.

Flooding Attack: In this attack the attacker sends large number of route request packets. Generally, there is a limit on number of route request packets to be sent in a network. But the attacker surpasses this number and floods the network with large packets, thereby disrupting the services in the network.

Denial of Service: The ad-hoc network contains nodes in the network. Some of the nodes can be malicious nodes. The malicious nodes are those nodes that drop packets completely or selectively. It causes denying of the service to the legitimate nodes. The denial of service attack is a serious attack on the ad-hoc network because the legitimate nodes are deprived of the services in the network.

V. SECURITY GOALS

All security system must provide a pack of security services that can confirm the secrecy of the system. These services are usually referred to as the goals of the security system. These goals can be listed under the following three main categories in this paper as follows:

a. Confidentiality

b. Integrity

c. Availability.

VI. APPROACH METHODOLOGY

The main aim is to study the routing protocols in ad-hoc wireless network using the ns2 simulation tool. There are three modules in the project namely: Routing Protocol module, Attack module and security module. In this section first of all ns2 simulation tool will be explained followed by the modules in the system along with the diagram.

.

A. NS2 tool

The simulation tool most widely used for the wireless network is the ns2. NS2 is the second version of a popular network simulator intended for wireless networks. It was developed and created by the Virtual Internetwork Test based project (or VINT). This second version is extended by the possibility to simulate ad hoc wireless networks. NS2 is an event based simulator, which means that simulation is following a timeline with several pre-defined events on it.Tcl was created by John Ouster hoot. The characteristics of these languages are:

a. It allows a fast development.

b. It provides a graphic interface.

c. It is compatible with many platforms.

d. It is flexible for integration.

e. It is a scripting language.

B. Routing Protocol Module

The routing protocol module is used to study and analyse the routing protocols used in ad-hoc wireless network. The simulation is done using the ns2. The block diagram for this module can be shown as bellows:

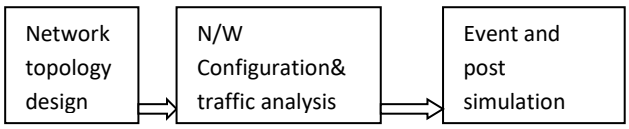

Figure 2. Network topology

In general, a simulation scenario consists of three main components:

A network topology

Connections, traffic and agents (protocols)

Events and failures

*Network topology design***:** A network topology defines many nodes and their connectivity, and can either be created manually. Connections and traffic are set up by traffic generators and agents (protocols) at a node.

*Configuring and running simulation***:** This step implements the design specified in the first step. In first step network configuration is done such as which protocols to be used i.e. tcp or udp. This step maintains the simulation clock and generates a trace

*Event and post simulation***:** The main tasks in this step include verifying the integrity of all programs and evaluating the performance of the simulated network. In this step the trace file generated by the ns2 is also analysed to understand the packet formats and types. The next module can be defined as Attack module. In this module the various attacks such sniffing and obtaining user credentials, denial of service, packet injection are being performed in network.. The attacks are implemented using the backtrack cd and also by writing scripts in ns2. The ns2 tcl script coding is used to perform some attacks and these are simulated using the ns2.

C. Security module

The third module can be defined as security module. In this module the procedures to prevent attacks done against the access point will be described. It also contains the analysis of the ns2 trace file to detect attack in the network. Ns2 trace file format: Whenever a ns2 tcl script is run a trace file is generated that describes the packet formats and types being used in simulation. Understanding of this trace file is very important in identifying the attack happening on the wireless network.

Event	Time	From Node	To Node	Pkt type	Pkt Size	Flag	FId	Source Addr	Dest i. addr	Seq no.	Pkt Id

Figure 3. Ns2 Trace file Format

The file format can be explained as bellows:

1. **Event**-The event type is first field. It contains the four possible symbols r, +, -, d which correspond respectively to receive, enquired, desuetude and dropped.
2. **Time**-time at which the packet tracing string is created.
3. **From node**-The from node field gives the input node of the link at which the event occurs.
4. **To node**- This to node field gives the output node of the link at which the event occurs.
5. **Packet type**- This field specifies the packet type such as CBR or TCP. This name depends on the type of stream packet specified in the scripting file.
6. **Packet size**- It gives in bytes.
7. **Flags**- It specifies the flags being used in the packet format in trace file.
8. **Fid**- It specifies the flow id of the IPv6 that a user can set for each flow at the input OTcl script in trace file.
9. **Source address**- This gives the source address in the form of "node. Port"
10. **Destination address**- This gives the destination address in the form of "node. Port"
11. **Sequence number**- This is the network layer protocols packet sequence number in trace file format.
12. **Packet id**- This field identifies the unique id of the packet in trace file.

VII. CONCLUSION

Wireless network is a computer network which are wireless, and they are commonly associated with a telecommunication network whose interconnections between nodes are implemented without the use of wires. Wireless networks are gaining more and more popularity in today's world because of their many benefits. Because wireless communication use open medium for sending and receiving data they are more susceptible to attack. Wireless ad-hoc networks have more security threats as they solely rely on the nodes present in the network. Routing is an important issue that needs to be handled with care in ad hoc network.

In this paper we have discussed some attacks and vulnerabilities in wireless and ad hoc network. This paper provides us with an insight of attacks done on wireless ad hoc networks. This paper can act as a basis for understanding of wireless ad hoc network and also attacks occurring on them.

REFERENCES

[1] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko," A Specification-based Intrusion Detection System for AODV", Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks, pp.125-134, 2003

[2] Sreedhar. C, Dr. S. MadhusudhanaVerma and Dr. N. Kasiviswanath,"Potential Security Attacks On Wireless networks and Their Countermeasure", International Journal of Computer Science & Information Technology (IJCSIT), Vol.2, No.5, pp. 76-89, October 2010.

[3] NitalMistry and Devesh C Jinwala," Improving AODV Protocol against Black hole attacks", Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol II, March 2010.

[4] Dr.M.S.Aswal, ParamjeetRawat, Tarun Kumar", Threats and Vulnerabilities in Wireless Mesh Networks", International Journal of RecentTrends in Engineering, Vol 2, No. 4, pp. 155-158, November 2009.

[5] Shalini Jain and Dr.Satbir Jain," Detection and Prevention of Wormhole attack in mobile Ad hoc networks", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, pp.78-86, February, 2010.

[6] Amol A. Bhosle, Tushar P. Thosar and SnehalMehatre, " Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA, Vol.2, No.1, pp. 45-54, February 2012.

[7] Richard kissel ,kevin Stine ,and Matthew "Information Security" NIST Special publication 800-64 Revision 2,October 2008 .

[8] Wireless Communication, link http://www.atis.org/, Archived from the original on 2008-01-02.

[9] Andrea Goldsmith, Wireless Communications, Cambridge University Press, September 2005, ISBN13: 9780521837163.

[10] William Stallings, Wireless communications and networking, William Stallings books on computer and data communications technology, Publisher Prentice Hall, 2002, ISBN10 0130408646.