IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Review On Wireless Adhoc Network Security

Manoj Kumar Joshi[*1], Hardwari Lalmandoria[2]

[*1]Department of Information Technology Department, GBPUAT, Pantnagar, India

[2] Professor, Department of Information Technology Department, GBPUAT, Pantnagar, India

manojjoshi24x7@gmail.com

Abstract

Emergence of wireless networks in 21th has redefined the networks which were seen in previous century. Initially there were no system networks so they were all secure .The data kept in a standalone system was totally safe, except an attacker gets the right to access the particular system. As there was a need occurred to connect to other systems, the complexity increased and the data kept in a system got more vulnerable because to transfer it from one system there was a need of some cable medium the data got some threat from outsiders because they got some more space to do their hacking task. They can now manipulate the data passing through a medium, also they could try to remove data from the channel, or they can mislead others with wrong information. But the whole 20th century was more peaceful then of now because of comparatively less systems connected as of now. In this century, in fact, from the last decade of 20 century, the systems grew rapidly due to the popularity of internet, and growing need of the people to transfer data from one system to another, now this is the age of mobilization and every person needs information on his hands instantly. People need networking with mobility, which has given growth to wireless systems so that they can enjoy while moving and the mobility doesn't disrupt the networking benefits. This has led to the growth to wireless systems; almost half of the world's systems are now wirelessly connected to each other as our laptops, wireless enabled desktops, mobile phones, sensor nodes etc. Facilities have grown immensely but also there is an increase in threat level; now an attacker has more points to intrude our information, everything is less secure than before. So there is a need to check the security features of our networks and an enhancement to them so that they are more secure to any attack. In this paper we try to bring the attack types and some prevention to save us from any attack.

Keywords: Wireless Network, Security, Adhoc Network.

Introduction

A wireless network [2] is a network which is connects various nodes in an environment so that they are able to interchange information among them. A campus Wi-Finetwork is the most common example of a wireless network. A network can be made for permanent use or may be used for some temporary period, in the former case every node is connected to others permanently and there is no disconnection from the network, but in a temporary arrangement a network is used till a node needs to be connected in a network. The later one is called an Ad-hoc network, this is the most widely used networking system of present time, a user connects his system in a network to another system or some access point which connects it to the other systems, this is called wireless adhoc network. These networks are self-configurable, autonomous systems consisting of routers and nodes, which are capable of supporting movability and organization of their position [.Such networks are built or destructed instantly. In a small network we can be assure of security but as soon as the network grows the vulnerability increases and the data in the network becomes more unsecure.

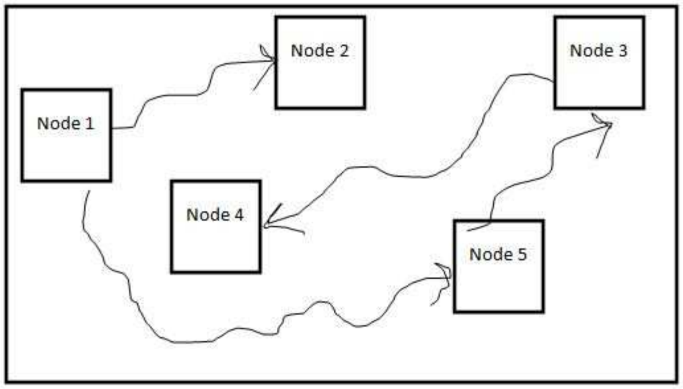


Fig 1: An Ad-hoc wireless network

Security plays the most important role in a wireless networks, because network nodes may be in a hostile location which makes them more vulnerable to physical attack by adversaries .Generally, adversaries are capable to take control of a network and extract maximum data as much as they can.

Fig.1 displays 5 nodes of an Adhoc network and every node is connected wirelessly for receiving, sending or forwarding data. They can be disconnected anytime or any other node can be connected in the range of the network. Thus more challenging than a fixed network where, there are limited number of nodes. In this article we shall discuss attacks on ad hoc networks and approaches for securing the network.

Wireless ADHOC Network Architecture

In a typical wireless adhoc network we see following network components -

Nodes- nodes is every computing or non-computing device which uses network resources.

Gateway-A Gateway is used for communication between various nodes.

Network Manager-The person responsible for designing network for communication. Security Manager- the person who is responsible for securing the communication.

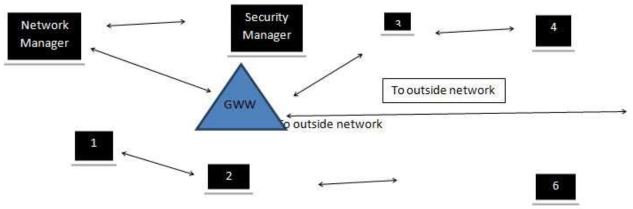


Fig 2. Wireless adhoc network architecture

Security Goals in ADHOC Wireless Networks

Wireless adhoc networks are susceptible to many attacks either active or passive. We have to save our network from those both kinds of attacks. Main goals of a network security are

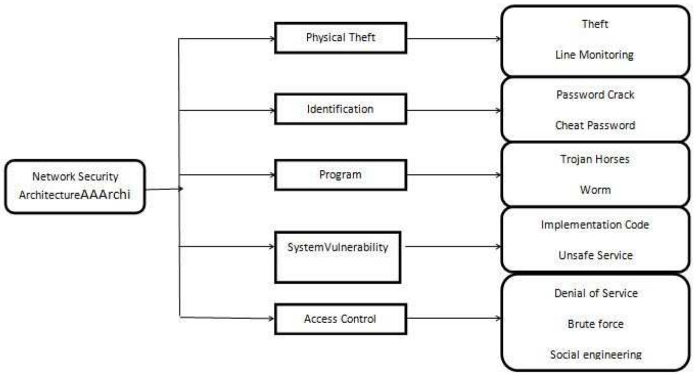
1. CONFIDENTIALITY- protecting secret information only with authorized users.
2. INTEGRITY- ensuring of full message delivery.
3. AUTHENTICATION- the message is from authenticated source.
4. ACCESS CONTROL- restricting access to only authorized users.
5. AVAILABILITY- all the resources must be available whenever required.
6. NON-REPUDIATION- ensuring that sender can't deny from what he has sent.
7. NON-IMPERSONATION – no one else must be able to pretend to be another authorized user.

Wireless ADHOC Networks Attack Types

Various researchers on their papers have mentioned many kind of attacks here some important kind of attacks are described so that we have some idea about the major categories of attacks

1. Denial of Service- any event which eliminates or diminishes a network to perform its usual functionality.
2. Sybil –It is defined as multiple identities taking of a malicious device.
3. Wormhole – An attack in which an adversary routes the information by giving false routing information to other nodes.
4. Sinkhole – In this a node is shown attractive enough to route all information through that node.
5. Manipulation of Routing Information-false information is sent in the network about node position.
6. Cloning- making a false impression of other node.
7. Traffic Analysis-By traffic analysis the real approximation of data.
8. Insider attacks- an insider attacker gains access by using an authorized access to an network and try to jam the network or any other work in which he is interested.
9. Spoofing- A malicious node uses IP address of other node(s) and receives the packets in a network.
10. Selfish Behavior – This refers to a node from where no cooperation is given in any routing activity. It may show that it is sleeping to save energy.

Classification: Network Security Threats



Routing Protocols in ADHOC Wireless Networks

In comparison to general networks ad hoc networks face additional problems. Thereare manywell-known protocols at are developed specially for adhoc networking environment.

Table driven protocols, also known as proactive allow every node to have a clear and consistent view of network structure, to send information from one node to another. Any change in structure causes the updation of table hence another protocol is **on-demand routing** is used which updates the routing table information whenever a change occurs in the structure.

PARAMETER	NETWORK	PROTOCOLS	EXAMPLES
RESPONSE TIME AND BANDWIDTH	ADHOC	PROACTIVE PROTOCOLS	OPTIMIZED LINK-STATE ROUTING(OLSR)
			DESTINATION-SEQUENCED DISTANCE VECTOR(DSDV)
		REACTIVE PROTOCOLS	AD-HOC ON-DEMAND DISTANCE VECTOR(AODV)
			DYNAMIC SOURCE ROUTING
			GEOGRAPHY BASED ROUTING
			CLUSTER BASED ROUTING
ENERGY	SENSOR	NETWORK STRUCTURE	FLAT NETWORKROUTING
			HIERARCHIAL NETWORK ROUTING
			LOCATION BASED ROUTING
		PROTOCOL OPERATIONS	NEGOTIATION BASED ROUTING
			MULTI-PATH BASED ROUTING
			QoS BASED ROUTING
			COHERENT BASED ROUTING

References

[1] Karan Singh, Rama Shankar Yadav and Ranvijay,"A review paper on adhoc network security". International journal of computer science and security, volume (1): issue (1), 2007.

[2] Zhijun Li and Guang Gong, "A survey on security in wireless sensor networks". Department of electrical and computer engineering, university of waterloo, Ontario, Canada, 2008.

[3] Hemanta Kumar Kalita and Avijitkar., "Wireless sensor network security analysis".International journal of next – generation networks, vol.1, December 2009.

[4] Mona Sharifnejad, Mohsen Shari, MansourehGhiasabadi and SarehBehesht. "A survey on wireless sensor network security",SETIT 2007

[5] Jonny Karlson,Laurence S. Dooley and GoranPulkkis.Routing, "security in mobile ad-hoc networks".Issues in informing science and information technology.volume 9,2012

[6] Pushpendra Kr. Verma and Preety,"Security for wireless network and intrusion prevention",VSRD-IJCSIT,Vol 1(1),2011,9-21.

[7] Bharat Singh et al., "Sensor data encryption protocol for wireless network security",Global journal of computer science and technology,Vol 12 issue 9 version 1.0 April 2012.

[8] Virendra Pal singh et al., "Flood attack and its countermeasures in wireless sensor networks",IJCSI,Vol 7,No 11,May 2010.

[9] Min-KyuChoi et al., "Wireless network security: Vulnerabilities,Threats and Countermeasures", International journal of multimedia and ubiquitous engineering,Vol 3,No. 3,july 2008

[10] D.V.ChandraShekhar et al., "Wireless security: A comparative analysis for the next generation networks".Journal of theoretical and applied information technology.

[11] Vishal Kumar et al., "Vulnerabilities of wireless security protocols". International journal of

advanced research in computer engineering &technology,Vol 1,issue 2,apr 2012.

[12] Minho shin et al., “Wireless network security and interworking”. Proceedings of the IEEE,Vol94, No.2, Feb 2006.

[13] Rodrigo Roman et al. “On the security of wireless sensor networks”.Institute for information research,Singapore.2005.

[14] Vikas Solomon Abel “Survey of current and future trends in security in wireless networks”.International journal of scientific & engineering research,Volume 2,Issue 4,Appril 2011.

[15] JinatRehana “Security of wireless sensor network”Helsinki University of technology,TKK T-110.5190 Seminar on Internetworking.

[16] HassenRedwan and ki-Hyung Kim. “Survey of security requirements,attacks and network integration in wireless mesh networks”.Japan-China joint workshop on frontier of computer science and technology,2008.

[17] Qazi Ahmad Faraz et al., “An overview of security of wireless networks”.International journal of multidisciplinary sciences and engineering ,Vol. 3,No. 3,March 2012.

[18] KshitizSaxena and C. Rama Krishna “Multidmensional analyses of 802.11 wireless network security protocols” Department of computer science NITTR ,chandigarh.2009.

[19] PallaviAgarwal et al. “ wireless network security for corporates”. International journal of research and practices in engineering sciences,Vol. 1,Issue 1,Mar-May 2012,pp.87-93.