ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 8, August 2015**

# A Study on Security Issues Related to Wireless Communication

Pragati Ojha[1], Sharad Kumar Gupta[2]

PG Student, Dept. of ECE, Maharana Pratap Engineering College, Mandhana, Kanpur, India[1]

Associate Professor and HOD, Dept. of EI, Maharana Pratap Engineering College, Mandhana, Kanpur, India[2]

**ABSTRACT:** While offering many advantages, the wireless communication is associated with many security issues and threats.In wireless environment, security is a vital issue both for the providers and users of the wireless system. In wireless communication system, many common characteristics are shared with a traditional wireless networks and thus causes many security issues. While superseding the disadvantages of the wired networks by eliminating the cable cost and increased user mobility, wireless network also encounter serious security concern. This paper presents an overview of security for mobile and wireless communication.

**KEYWORDS:** Mobile, security, wired networks, Wireless.

## I.INTRODUCTION

Wireless communication provides a lot of advantages due to increased accessibility. But, at the same time, it is sensible to many security risks. If a message is not encrypted with a strong algorithm or security protocol, one can easily access it since all the communication takes place in air. In wired networks, the physical transmission medium can be secured, but the wireless networks uses air as a transmission medium. This enables easy access to transmitted data. The mobility of the wireless networks also causes problems. The transmission of signal through air and the mobility of users bring the era of wireless network. Thus, issue of privacy and security concern becomes most important with the wireless networks.

## II. WIRELESS AND SECURITY

User anonymity [1] is important in a wireless communication network .Distinct degrees of anonymity can be provided such as hiding the user identity from certain administrative authorities. Among the potential users, being available at any location at any time causes great concern about the privacy issues. Mobile users utilize the resources at many locations provided by many service providers. It is vital to understand the trust issues involved which mobile clients are allowed to access resources of different servers at distinct locations.

## III. ATTACKS IN WIRELESS COMMUNICATION

Several severe attacks are developed for countering the security protocols. If the results of these attacks are successful, it can cause severe inconvenience and threats to security. Even if the attacks are unsuccessful, they can reduce the resource available to legitimate communication. The attacks are trouble causing in the wireless communication since they are easy to execute. Some of these attacks are discussed below:

**i. Denial of service on sensing (DoSS) attack:** One can tampers the data before it is read by sensor nodes, thus resulting in false readings and leading to a wrong decision. A DoSS attack usually targets physical layer applications in an environment where sensor nodes are located.

**ii. Replay attack:** By act of replay attack, the attacker can extract and stores all the communication between the communicating parties. Later, the attacker impersonates either of the communicating parties by replaying the stored message. The replay attack can be avoided by incorporating the session variant parameter in authentication message.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 8, August 2015**

**iii. Parallel session attack:** In the attack, one can begin to communicate with either of the communicating parties and uses it as an oracle to compute the session key. It can be prevented by maintaining asymmetry in the back and forth message, since this method is not successful when the message between the communicating parties is of same structure.

**iv. Nuisance attack:** Due to nuisance attack, several unnecessary wireless responses being expended before the attacking message recognized to be deceitful or fallacious. To minimize the nuisance attack, protocol design should be incorporated.
**v. Impersonation attack:** By pretending or impersonating as a valid user, the attacker will try to mitigate either of the communicating parties from the deliberate communication, making the other communicating party to believe that he is the legitimate. To avoid the impersonation attack, protocol design must consider the mutual authentication of valid entity and the server.
**vi. Eavesdropping attack:** In Eavesdropping attack, one can secretly eavesdrops or intrude on ongoing communications between targeted nodes to collect information on connection.

**vii. Location disclosure attack –** It reveals the information about the locations of nodes or structure of the network such as which other nodes are adjacent to the target, or the physical location of a node routing.

## IV. SECURITY ISSUES IN WIRELESS COMMUNICATION

Some areas of wireless system security are discussed below:
**i. Anonymity:** It is the state of being not identifiable within a set of principles [2]. The information about a particular person or an organization is private and is restricted only to the owner or the person who has rights to access it. Retaining anonymity [1] is of high concern in wireless communication system for various reasons. Wireless system is more sensible to interfering and taping as compared to a wired network. Now a day's user stores a number of information in mobiles that are related to user itself. This leads the user information more widespread and highly available. It is also uncertain that whether the data stored is safe or not.
There are some factors that should be considered to solve the problem of anonymity. A basic solution to this problem in current system has been adopted. By means of alias or temporary identity, anonymity can be restricted. Aliases or nicknames allow a user to be referenced without revealing his identity. Another way to provide user anonymity is to encrypt the real identity [3].

**ii. Authentication:** The main objective of authentication scheme is to prevent unauthorized users from accessing to a protected system [4].The authentication process is necessary for verifying both an entities' identity and authority. Authentication protects the service provider from unauthorized intrusions. By mutual authentication [5] mobile station also authenticates the server. Authentication is important for two reasons first, it prevents a malicious station from pretending to be a base station and then it permits the mobile station to choose the service of a particular base station in the presence of collocated networks.
**iii. Availability:** When denial of service (DoS) attack takes place, the availability ensures the survivability of network services. In DoS, all the nodes in the network can be targeted and some selfish nodes make some of the network services unavailable. A DoS attack can be done at any layer of the network [6].

**iv. Integrity:** It ensures that a message being transferred will never corrupt. It can be described in the following ways [7]:

i) Malicious altering - In Malicious altering, the attacker alters an account number in a bank transaction.
ii) Accidental altering –In Accidental altering, transmission error may occur.

In Malicious altering, a message could be replayed, removed, or revised by an adversary with malicious attack goals on the network. In Accidental altering, the message is lost or if its content is changed due to some failures, which may be transmission errors in communication.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 8, August 2015**

**v. Confidentiality: S**ome information is only accessible to the person who owes it. Confidentiality ensures that certain information is never disclosed to unauthorized entities. It must be keep secret from all entities that do not have the validity to access them, in order to maintain the confidentiality of some classified information.

## V. SECURING WIRELESS NETWORKS

**i. Encryption:** It is the most effective way to secure the wireless network from eavesdroppers. In encryption, encryption or scrambling of the message is done for communication over the network. The encryption is done by certain secret codes to prevent the message from getting intruded.

**ii. Anti-virus and firewall:** Install anti-virus and anti-spyware software, and keep them up-to-date for securing the wireless communication. Firewall systems prevent unauthorized access to or from a private network. Basically, a firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks.

**iii. Turning off the wireless network:** Attackers cannot access a wireless router when it is shut down. If one turns the router off when it is not in use, one can limit the amount of time that it is susceptible to a hack.

## VI. CONCLUSION

Wireless communication Lots of opportunities to gain high productivity and reduced costs. It is impossible to totally mitigate all the risks associated with wireless communication, but it is possible to achieve a reliable level of overall security by adopting a systematic approach to assessing and managing. In this paper, several security threats to the wireless communication are discussed. The threats can cause many severe issues to the wireless communication. By adopting the safety protocols, one can ensure a safe wireless communication and prevents the personal information from being trapped.

## REFERNCES

[1] Samfat, D., R. Molve, and N. Asokan, "Untreacibility in Mobile Networks," *Proc. of ACM Int. Conf. on Mobile Computing and Networking*, Berkeley, CA, November 1995.
[2] Pitzmann, A., and M. Köhntopp, "Anonymity, Unobservability, and Pseudonymity—A Proposal for Terminology," *Designing Privacy Enhancing Technologies, LNCS 2009*, Springer-Verlag, pp. 1–9, 2001.
[3] Park, C. S., "Authentication Protocol Providing User Anonymity and Untreacibility in Wireless Mobile Communications Systems," http://www.misecurity.com/ko/forum/ forum_06.pdf.
[4] Morris, R., and K. Thompson, "Password Security: A Case History," *Communications of the ACM*, Vol. 22, No. 11, pp. 594–5971997.
[5] Joos, R. R., and A. R. Tripathi, *Mutual Authentication in Wireless Networks*, Technical Report, Computer Science Department, University of Minnesota, 1997.
[6] X. Gu and R. Hunt, "Wireless LAN Attacks and Vulnerabilities" In the Proceeding of IASTED Networks and Communication Systems, April 2005
[7] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity (Accessed on May 24, 2010)