# Study of Security and Fraud Detection in Mobile and Wireless Network Technology

Deepak & Ranbeer Singh

(Assistant Prof. Dept. of Computer Science)
I.E.T. Group Of Institution, Alwar

**Abstract:** The fusion of computer and telecommunication technologies has heralded the age of in- formation superhighway over wire line and wireless networks. Mobile cellular communication systems and wireless networking technologies are growing at an ever faster rate, and this is likely to continue in the foreseeable future. Wireless technology is presently being used to link portable computer equipment to corporate distributed computing and other sources of necessary information. Wide-area cellular systems and wireless LANs promise to make integrated networks a reality and provide fully distributed and ubiquitous mobile communications, thus bringing an end to the tyranny of geography. Higher reliability, better coverage and services, higher capacity, mobility management, power and complexity for channel acquisition, handover decisions, security management, and wireless multimedia are all parts of the potpourri.
[Deepak & Ranbeer Singh. **Study of Security and Fraud Detection in Mobile and Wireless Network Technology.** Academia Arena, 2012;4(3):55-58] (ISSN 1553-992X). http://www.sciencepub.net. 9

**Keyword:** Security; Fraud Detection; Mobile, Wireless ;Network Technology.

## Introduction:

Wireless technology is presently being used to link portable computer equipment to corporate distributed computing and other sources of necessary information. Wide-area cellular systems and wireless LANs promise to make integrated networks a reality and provide fully distributed and ubiquitous mobile communications, thus bringing an end to the tyranny of geography. Higher reliability, better coverage and services, higher capacity, mobility management, power and complexity for channel acquisition, handover decisions, security management.

Further increases in network security are necessary before the promise of mobile telecommunication can be fulfilled. Safety and security management against fraud, intrusions, and cloned mobile phones, just to mention a few, will be one of the major issues in the next wireless and mobile generations. A "safe" system provides protection against errors of trusted users, whereas a "secure" system protects against errors introduced by D. S. Alexander, W. A. Arbaugh, etc. [1]. Therefore, rather than ignoring the security concerns of potential users, merchants, and telecommunication companies need to acknowledge these concerns and deal with them in a straightforward manner. Indeed, in order to convince the public to use mobile and wireless technology in the next and future generations of wireless systems, telecom companies and all organizations will need to explain how they have addressed the security of their mobile/wireless systems. Manufacturers, M-business, service providers, and entrepreneurs who can visualize this monumental change and effectively leverage their experiences on both wireless and Internet will stand to benefit from it.

Concerns about network security in general (mobile and wired) are growing, and so is research to match these growing concerns. Indeed, since the seminal work by D. Denning [2] , many intrusion-detection prototypes, for instance, have been created. Intrusion-detection systems aim at detecting attacks against computer systems and wired networks, or against information systems in general. However, intrusion detection in mobile telecommunication networks has received very little attention. It is our belief that this issue will play a major role in future generations of wireless systems. Several telecom carriers are already complaining about the loss due to impostors and malicious intruders. Mobile network security, V. Gupta and G. Montenegro [3] in this work we will discuss the intrusion detection systems and describe several aspects of wireless and wired and wireless networks and identify the new challenges and opportunities posed by the ad hoc network, a new wireless paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, they rely on each other to keep the network connected. Next, we will examine the authentication problem of mobile users. Further we shall discuss the problems of cloning and fraud detection in mobile phone operations.

## WIRELESS SECURITY PROBLEMS

Security is an essential part of wired and wireless network communications. Interestingly enough, these systems are designed to provide open

access across vast networked environments. Today's technologies are usually network-operation-intrusive, i.e., they often limit the connectivity and inhibit easier access to data and services. With the increasing popularity of wireless networks, the security issue for mobile users could be even more serious than we expect. The traditional analogue cellular phones are very insecure. The 32-bit serial number, the 34-bit phone number, and the conversation in a cell can be scanned easily by an all-band receiver. The widely used advanced mobile phone system (AMPS) is an analogue phone system. Therefore, sending a password or a host name through this system can be a serious security issue. Other security issues in wireless networks that have been studied extensively are anonymity and location privacy in mobile networks; these have received a great deal of interest recently S. P. Shieh, C. T. Lin, and J. T. Hsueh, [4]. A typical situation is one in which a mobile user registered in a certain home domain requests services while visiting a foreign do-main. Concerned about security and privacy, the user would prefer to remain anonymous with respect to the foreign domain. That is, only the home domain authority should be in- formed as to the mobile user's real identity, itinerary, whereabouts, etc. Another important issue, namely cloning phones, raises a number of concerns to many telecom carriers. In- deed, many telecommunication companies are losing money due to the use of clones or genuine mobile phones by impostors. One might argue that although it is rather easy to clone an AMPS phone, it is much trickier to clone a D-AMPS, a GSM, or an IS-95 phone. However, the security issue remains, and needs to be resolved in the next wireless network generation. Consequently, there has been a great deal of interest recently in designing mo- bile phones using new technologies, such as Boot Block flash technology used by Intel Corporation, that will make it much more difficult to clone cellular phones. However, to the best of our knowledge there is very little work being done at the software level. To combat cloning, cellular operators analyze usage to check for unusual patterns. Most obviously, they know that genuine phone cannot be in two places at once. If a phone is making more than one call at a time, it has definitely been cloned. Furthermore, to verify if a call is out of the client patterns, current software (i) does not have an efficient automatic process to warn clients about the impostors using their mobile phones; in most of these systems, human staff are used to do that (only lists of large bills are reviewed to identify cloned phones); (ii) has no efficient ways to control/identify impostors; and (iii) uses an "experimental satisfaction" to prove the correctness of the security framework. Some systems provide the billing process via the Web. However, the identification of a cloned phone is done only at the end of the month. This, unfortunately, is not quite efficient and may lead to a big loss of revenue for the carrier.

The wireless Web opens up many new business opportunities, the most important of which use location-based technology. Ever since the mobile Internet was first suggested, antivirus companies have warned that viruses could attack cellular phones and PDSs. Timofonica was among the first viruses that attacked cell phones. Timofonica was an ordinary virus programmed to send abusive messages to random users of Spanish Telefonica mo bile systems. Viruses are a threat to any computing platform and may be a threat to wire- less terminals that include processing and memory akin to those of modern computers.

## WIRELESS SECURITY MANAGEMENT PLAN

An adequate security system management policy has long been an important issue. A comprehensive network security plan must also consider losses of privacy when we define authentication and authorization as well as losses of performance when we define key management and security protocols. Therefore, a security plan must encompass all of the elements that make up the wireless and/or wired network, and provide important services such as:

1. Access control, i.e., authorization by capability list, wrappers, and firewalls (access control matrix)
2. Confidentiality, i.e., we must ensure that information and transmitted messages are accessible only for reading by authorized parties
3. Authentication, i.e., the receiver must be able to confirm that the message is indeed from the right sender
4. Nonrepudiation, i.e., the sender cannot deny that the message was indeed sent by him/her
5. Integrity, i.e., the message has not been modified in transit
6. Availability, i.e., making sure that the system is available to authorized parties when needed
7. Security administration, i.e., checking audit trails, encryption and password management, maintenance of security equipment and services, and informing users of their responsibilities.

## INTRUSION DETECTION SYSTEMS (IDS)

Intrusion is most probably one of the key issues that wireless and mobile systems will have to deal with. The nature of wireless ad hoc networks makes them very vulnerable to an adversary's malicious

attacks. Generally speaking, an intrusion can be defined as an act of a person or proxy attempting to break into or misuse your system in violation of an established policy. Very little research work dealing with the intrusion problem has been done for wireless networks.

In our work, we shall describe the intrusion problem in general. We hope that re- searchers will pick up what has been done in related areas, and find efficient approaches on how to deal with this problem in an ad hoc network environment. There are many different intrusion systems available in the marketplace. Expert systems are based on knowledge-based intrusion detection techniques. Each attack is identified by a set of rules. Rule-based languages N. Habra et al., Asax: [5] are used for modeling the knowledge that experts have accumulated about attacks/frauds. Information regarding some intruders has also been added to these systems. A major drawback of knowledge-based intrusion systems is the difficulty of gathering the information on the known attacks (which should be updated regularly) and developing a comprehensive set of rules that can be used to identify intrusive behaviors. Some systems use a combination of several approaches to cover both the normal and proper behavior schemes T. Lunt, Automated audit trail analysis intrusion: and detection [6].

**SECUREING DATA TRANSFER IN DIGITAL MOBILE SYSTEMS AND AD- HOC NETWORK**

All digital mobile systems provide security through some kind of encryption. Data can be encrypted in many ways, but algorithms used for secure data transfer fall into two categories: symmetric and asymmetric. Both rely on performing mathematical operations using a secret number known as a key. The difficulty with symmetric algorithms is that both parties need to have a copy of the key. On the other hand, asymmetric techniques use two separate keys for encryption and decryption. Usually, the encryption key can be publicly distributed, whereas the decryption key is held securely by the recipient.

The most widely used symmetric algorithm in DES (data encryption standard), developed by IBM in 1977. It uses a 56-bit key, which seemed unbreakable at that time. In 1997, a group of Internet users managed to read a DES-coded message. Most organization now use triple-DES, which uses 112 bits. Many WLANs in use today need an infrastructure network. Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control, etc. In these infrastructure-based wireless networks, communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes. Ad hoc wireless networks, however, do not need any infrastructure to work. Each node can communicate with another node; no access point controlling medium access is necessary. Mobile nodes within each other's radio range communicate directly via wireless links, whereas those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology.

**AUTHENTICATION AND FRAUD DETECTION FOR MOBILE SYSTEM**

Some wireless communications systems protocols such as GSM S. P. Shieh, C. T. Lin, and J. T. Hsueh, S. P. Shieh, C. T. Lin, and J. T. Hsueh, [8] and IS-41 S. Mohan [7] use the secret key crypto-system for authentication. Although the authentication of these systems is only unilateral, and the user's identity and location are not anonymous, the protocols provide more security functions, such as identity, confidentiality, and mutual authentication. The drawback of the above schemes is that they all need a third party, i.e., a third trusted server such as the home location register (HLR) and old visitor location register (VLR). Although HLR creates a record that contains the mobile station's (MS) directory number, profile information, current location, and validation period, etc., whenever the MS subscribes to the service of a mobile system, VLR records the temporal information for the MS when it visits a mobile system other than the home system. HLR acts as the CA; VLR is responsible for authenticating the MS.

With the increasing popularity of wireless networks, the security issue for mobile users could be even more serious than we expect. Before the mobile phones became widely popular, the greatest threat to the network security in most organizations was dial- up lines. While dial-up lines still merit attention, the risks they pose are minor when com-pared to wireless and mobile connections. To break the system, one need only buy a piece of portable radio equipment, such as a scanner, to program a mobile cloned to debit calls from genuine mobile phone, and register the frequencies at which mobile phones operate in surrounding areas. Then the person committing the fraud may, for example, park his car in a shopping mall, jot down various frequencies, transfer the data to clones, and then pass them to whoever may be interested in these cloned mobiles.

**Conclusion:**

In this paper we studied about the fraud detection of wireless application when any unwanted person entered in this application. We can capture the fraud person who entered without person. Because in this theory we can implemented the wireless application.

**Reference:**


1. D. S. Alexander, W. A. Arbaugh, A. D. Keromytis, and J. M. Smith, Safety and security of pro-gram able networks infrastructures, *IEEE* Communications *Magazine, 36,* 10, 84–92.
2. D. Denning, An intrusion-detection model, *IEEE Transactions on Software Eng.,*
3. V. Gupta and G. Montenegro, Secure and mobile networking, ACM*/Baltzer MONET, 3,381*–390, 1999.
4. 14. S. P. Shieh, C. T. Lin, and J. T. Hsueh, Secure communication in global systems for mobile telecommunication, in *Proceedings of the First IEEE Workshop on Mobile Computing*, 1994
5. 15. N. Habra et al., Asax: Software architecture and rule-based language for universal audit trail analysis, in *Proceedings 2nd European Symposium on Research in Computer Security*, LNCS, vol. 648, 1992.
6. 16. T. Lunt, Automated audit trail analysis and intrusion : detectionA survey, in *Proceedings 11th* International Computer Security Conference, 1988
7. 17. S. Mohan, Privacy and authentication protocol for PCS, *IEEE Personnel Communication*, 1996,
8. 18. S. P. Shieh, C. T. Lin, and J. T. Hsueh, Secure communication in global systems for mobile telecommunication, in *Proceedings of the First IEEE Workshop on Mobile Computing*, 1994.


2/5/12