International Journal of Grid and Distributed Computing
Vol. 9, No. 10 (2016), pp.273-282
http://dx.doi.org/10.14257/ijgdc.2016.9.10.24

Mobile Computing: Wireless Networking Security Issues

Javed Ahmad Shaheen, MS (CS)

Computer Science Department, Virtual University of Pakistan, Lahore–Pakistan
javedmatyana@yahoo.com

Abstract

Mobile wireless has detonated in popularity just of its simplicity, revolution in communication and Mobile computing has become very famous now days in reward of the services offered during the mobile communication and. Mobile computing has become the reality not the luxury. Mobile wireless market is increasing by leaps and bounds as Cell phones, mobile computing and communication devices have become very trendy because of their ease and portability. However, the use of such devices in this platform is accompanied by new security risks that must be recognized and addressed to protect the physical devices, the communication medium, and the information used. Security is key issue that needs to be considered. For this security protocols are proposed for different applications like Wireless Application Protocol, 802.11a etc. Most of them are based on the public and private key cryptography. The challenge for mobile network is in providing very large footprint of mobile services with high speed and security. In this paper, we have discussed security issues arising due to wireless networking of mobile computing in distributed systems. We discussed the operational model of mobile computing environment, and try to demonstrate proposed solutions. We also discuss security problems and mechanisms that can be applied one of three main components of mobile computing. The goal of paper is to point out some of the limitations, characteristics, applications and issues on security of mobile computing.

Keywords*: Mobile computing, wireless communications security, mobile computing security*

1. Introduction

Security Issues Involved in Mobile Computing is very important. It is of particular concern as it relates to the security of personal information now stored on the smart phone. More and more users and businesses use smart phones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smart phones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company. ii) All Smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smart phones that can come from means of communication likes SMS, MMS, Wi-Fi NETWORKS. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. iii) Different security counter-measures are being developed and applied to smart phones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps. [14]. With the rapid growth in the wireless mobile communication technology, and because of their benefits ,convenience, flexibility, and the ability to communicate with fixed network while in motion, small devices like laptop computers, smart cell phones, personal digital assistants

ISSN: 2005-4262 IJGDC

(PDAs), tablets, mobile data storage devices, and similar mobile computing and communication devices have become very popular at all user and application levels. As a result, a new computing platform called mobile computing is becoming widely spread The radical evolution of computers, especially in hardware (towards smaller size and weight, higher performance, lower power consumption, lower cost) and communications (wireless and 1satellite networks, cellular telephony, WANs, INTERNET), has introduced the idea of mobile computing (Imielinski and Badrinath, 1992). This means that users don't have to be tethered on expensive wired workstations in order to exchange data. All they need is mobile computers that are portable computers communicating via wireless networks. Mobile computer will be the 'communication car' for people of 21st century: the freedom to communicate in anyway, from everywhere and any time (Weiser, 1991),(Weiser, 1993). Mobile computing is tightly depending on available infrastructure of distributed systems. As a result, we can see it as an extension of distributed systems computing [2]. Mobile computing devices are capable of storing, processing, displaying, and communicating information. This information could be sensitive information, such as the identification and credit data of customers, and the mobile devices can move in and out of the boundaries of a networking environment. Mobile users have the ability to work from anywhere without being bound to any networking system. This flexibility extends the network boundary beyond a fixed point and makes security management a much more difficult task, as the users cannot be tracked down to a single location. Therefore, the implicit presumption that everything inside the company's network's firewall is secure turns out to be not true anymore [1]. Mobile communication takes place mainly through the radio signals rather than wires, so it is easier to intercept or eavesdrop to communicate on channels. Hence, traditional security technologies such as firewalls, authentication servers, biometrics, cryptography, intrusion detection, virus protection, and VPNs are not enough to tackle security issues in mobile computing. Despite the fact that every mobile computing user is concerned one way or the other about security, the defense community personnel are the most concerned "Cyber security and data protection is one of the current space races'' said David Machuga, director of identity management and business solutions at Northrop Grumman, which supplies the Defense Department with secure mobile biometric data collection technology. "There are several challenges, but the three largest are how to certify the security, how to protect the information transmitted in a wireless mode and how to protect data at rest," he said. "For DOD, this is a constant problem, whether dealing with cell phones, handheld bar code scanners used in a warehouse or mobile computers used to validate biometrics." [2]. In addition to the general security issues like confidentiality, integrity, availability, legitimacy, and accountability that needs to be individually taken care of, new security issues need to be handled properly. These new issues will be discussed in Section 3 of the paper and can be found under different areas of risks like physical risk, unauthorized access risk, application and operating environment risk, communication and network risk, and mobile data storage device risk. Although I cannot cover every security issue or problem in details, this paper provides a good discussion and a strong overall coverage and classification of the security problems and challenges arising in mobile computing environment, and it gives a good summary of the available techniques used in handling the different types of security risks and issues. The paper is organized as follows: In Section 2 is the traditional security issues found in most computing and communication systems are presented and discussed. In Section 3, the new security issues and challenge introduced by mobile computing are presented, discussed and classified. In Section 4, different techniques and requirements used in dealing with the new security challenges are presented and discussed. Finally, in Section 5, a summary and conclusion of the paper is given.

2. Mobile System Infrastructure (2G and 3G Technology)

This provides the necessary services demanded for the proper functioning of the entities involved in a mobile system and architecture. The widely deployed cellular infrastructures are GSM also known as 2G. Its designs had several goals. It has better quality for voice, higher speeds for data, international roaming, and protection against fraud charge. The UMTS or 3G promised advanced services such as mobile internet, multimedia messaging, video conferencing etc. UMTS standards have defined by an international consortium called 3GPP (3rd generation partnership project) [20].

2.1. Fundamentals of a Cellular System for Mobile Computing

Block diagram of a cellular system is shown in the Figure 2.1, below. A user may gain services of other networks which we say a foreign network and there have an agreement for roaming with user's/subscriber's home network. Each cellular network has a database called as Visitor Location register (VLR) of users currently visiting that network with the list of services the subscriber entitled to.2G technology. It introduced Subscriber Identity Module (SIM) card which stores three secrets used for cryptographic operations these are:
1. IMSI (International Mobile Subscriber Identity) it is unique 15 digit subscriber identification number used to identify each registered users. It has following parts.
a. Mobile Country Code (MCC): It has 3 decimal places.
b. Mobile Network Code (MNC): It has 2 decimal places. These two fields uniquely identify a country and the operator.
c. Mobile Subscriber Identification Number (MSIN): It has a maximum of 10 decimal places and identifies the user in the home network.
2. A 128 bit subscriber authentication key known only to the SIM and HLR of the subscriber's home network.
3. A PIN known to the phones owner and used to unlock the SIM.

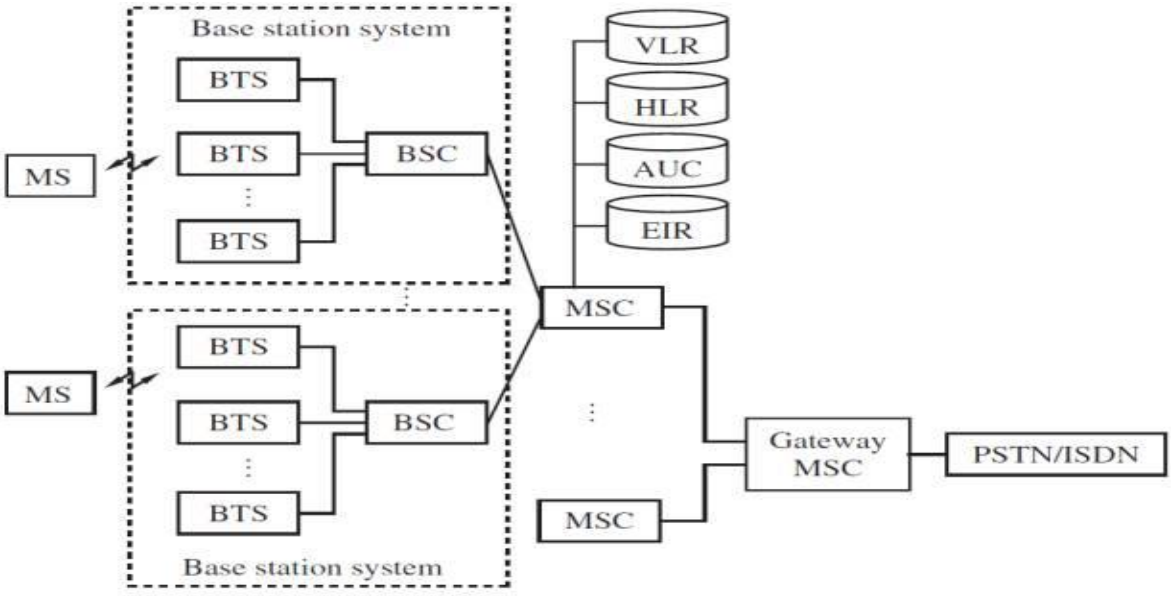

Diagram 2.1

2.2. Security Issues

Classifications of security issues in communication networks have been presented by many authors [15]. The fundamental goals of security in information system are five *i.e.*,

- ✓ *Confidentiality*: it is preventing unauthorized users from gaining access to critical information of any particular user.
- ✓ *Integrity*: it ensures unauthorized modification; destruction or creation of information cannot take place.
- ✓ *Availability*: it is ensuring authorized users getting the access they require.
- ✓ *Legitimate*: it is ensuring that only authorized user have access to services.
- ✓ *Accountability*: it is ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked if and when necessary.

The way through which following goals are achieved depends on the security policy as adopted by the service providers.

2.3. The Technology Infrastructure

Wireless information systems are computing systems that provide the ability to compute and communicate anywhere and anytime. A number of terms have been used in the literature to describe such systems, including wireless computing, ubiquitous computing, and nomadic computing and decoupled computing. Wireless networks communicate by modulating radio waves or pulsing infrared light. Wireless communication is linked to the wired network infrastructure by stationary transceivers. The area covered by an individual transceiver's signal is known as a cell. Cell sizes vary widely: for example, an infrared transceiver has a range of a few meters, and a satellite beam can cover an area more than 400 miles in diameter.

2.4. General Architecture of Wireless Networks

The vision of mobile wireless computing requires ubiquitous wireless network connectivity, adequate wireless bandwidth and a small, portable computing platform with sufficient functionality. The necessary networking infrastructure (called PCN, for personal communication network) is still very much under debate, although it will most likely be based on the cellular networking architecture. The cellular (in future, microcellular and picocellular) architecture is capable of providing voice and data services to users with hand-held devices. Continuous coverage of cellular service is restricted to metropolitan regions. Wide-area moves require the user to inform the network of his new location. The available bandwidth is very low for most data intensive applications. CDPD stands for Cellular Digital Packet Data, is another emerging technology. It transmits packet based data over existing analog networks for voice communications, using frequency hopping. The CDPD device listens to a channel. When it finds an adequate idle time in a call, it transmits the packets using the full bandwidth. If the channel is full, it hops to another channel and repeats the same process. The main advantage with CDPD is that it has low cost, while billing is based on amount of data rather than time. Finally, the so-called PCS (Personal Communication Services) technology can provide local area services such as voice, fax and data communication. The advantage of PCS over cellular networks is that it will offer a wider bandwidth. Wireless LAN is a traditional LAN architecture extended with a wireless interface to service small low-powered portable terminals capable of wireless access. The wireless LAN is further connected to a more extensive fixed network such as LAN or WAN. Wireless LANs have limited range and are designed to be used only in local environments. There are two types of wireless LAN architectures: ad-hoc networks and infrastructure networks. The Wide-Area Wireless Networks are special mobile radio networks that provide wide coverage for low bandwidth data services. In paging networks the service is usually receive-only and has very low bandwidth. The initial applications for satellite systems are voice and paging. Additional services planned include messaging and fax transmission.

2.4. Operational Problems

The essential properties of mobile computing are wireless communication, mobility and portability (Forman and Zahorian, 1994). Each one of these properties introduces, however, a number of problems. Some of the problems that wireless communication introduces are: Disconnection. Wireless communications suffer from frequent disconnections due to a higher degree of noise and interference as well as the process of inter-cell hand-offs. Disconnections can be hidden by asynchronous operation.

2.4.1. Bandwidth and Interface Variability: Bandwidth can shift one to four orders of magnitude, depending on whether the system is plugged in or using wireless access or switching interfaces, *e.g.*, from infrared to radio when the user moves from indoors to outdoors. Mobile applications have to adapt their behavior properly (Katz, 1994).

2.4.2. Heterogeneous Network: To achieve wireless communication a mobile host must get connected to different and heterogeneous networks. The general problem of heterogeneity can be addressed by exploiting emerging distributed systems standards such as the Object.

3. Traditional Security Issues

Security policies and domains Security policy refers to the set of rules, laws and practices that regulate how an organization manages, protects, and distributes sensitive information. A security policy must specify the security goals the system must meet and the threats it must resist. This implies that a security policy should determine the type of secure communication required for various transactions, the type of authentication, auditing procedures, recovering techniques and access control. One important part of security policy is access control. In general, the access control policy specifies who can access particular resources and what operations the accessor can perform on those resources (Yialelis, 1996). The crossing of administrative (security) domains is of special interest, as the mobile unit moves, and appropriate functions needed. A security domain means a set of network entities on which a single security policy is employed by a single administrative authority (Vasquez Gomez, 1994).

Let we discuss briefly the most addressed general security issues that are common to most wireless network system.

3.1. Authentication

This enforces the verification and validation of the identities and credentials exchanged between mobile systems or a mobile device and a service provider. It ensures that the user accessing the information is the right person. The initiating service requester must be authenticated to prove its identity with reliable credentials to prevent masquerading attacks (when a user is deceiving about its real identity which may lead to impersonation).

3.1.1. Authorization: This ensures that the service requester has the right to access the information on different network or mobile resources. It defines the policies associated with the required access control to the resources.

3.1.2. Non-Repudiation: This ensures that the different communicating parties cannot deny the exchange of information or the acceptance of a committed transaction at a later time. It ensures accountability.

3.1.3. Availability: This ensures that the mobile computing environment or the services of the information systems are all the time available for users. This could be threatened by a well known type of attacks.

3.1.4. Denial of Service (DoS): Whenever an unauthorized user or a hacker tries to disrupt a service or a device by flooding it with useless traffic then DOS consumes server/device resources and forces them to be unavailable.

4. Mobile Computing Security Issues

Mobile computing is a broad area that describes a computing environment where the devices are not restricted to a single place. It is the ability of computing and communicating while on the move. Wireless networks help in transfer of information between a computing device and a data source without a physical connection between them. These networks include wireless LAN, wireless access point, and cellular networks [3]. So some of the new security issues introduced in mobile computing are originated from the security issues of wireless networks and distributed computing systems. In addition, poorly managed mobile devices introduce new security issues involving information exposure and compromise especially when these devices like laptops, PDAs, iPhones, Blackberry's, and others are loaded with sensitive information and are stolen or fallen into the hands of an unauthorized person. Hence **t**he new types of threats and security challenges introduced by mobile computing can be classified into two main classes:

- **Security issues:** related to wireless networks and the transmission of information 'over the air' between mobile units and mobile support stations and networks.
- **Security issues** related to the mobility of the devices and the information residing on them.

4.1. Wireless Networks Security Issues

Wireless networks have security issues and challenges. This is mainly due to the fact that they use radio signals that travel through the air where they can be intercepted by location-less hacker that are difficult to track down. In addition, most wireless networks are dependent on other private networks, owned and managed by others, and on a public-shared infrastructure where you have much less control of, and knowledge about, the implemented security measures. Although encryption aid to some extend in securing information moving across wireless networks, the moment the data leaves a mobile device and heads onto a communication network, it's the network operator's job to ensure that the information is securely transported to its final destination. In what follows, I will list and discuss the main mobile computing security issues introduced by the use of wireless networks. Most of these issues can fall under one of the following categories: Availability where the availability of information and services could be disrupted, confidentiality where the privacy of information when it passes through the wireless medium can be compromised, and integrity of data where data interchanged can be modified and retransmitted [1-3].

4.1.1. Denial of Service: *DOS* attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. DOS attacks are common in all kinds of networks, but they are particularly threatening in the wireless context. This is because, the attacker does not require any physical infrastructure and he gets the necessary anonymity in the wireless environment. The attacker floods the communication server or access point with a large number of connection requests so that the server keeps responding to the attacker alone hindering legitimate users from connecting and receiving the normal service.

4.1.2. Traffic Analysis: The attacker can monitor the transmission of data, measure the load on the wireless communication channel, capture packets, and reads the source and destination fields. In order to do this, the attacker only needs to have a device with a wireless card and listen to the traffic flowing through the channel. By doing such things, the attacker can locate and trace communicating users and gain access to private information that can be subject to malicious use.

4.1.3. Eavesdropping: This is a well known security issue in wireless networks. If the network is not secure enough and the transmitted information is not encrypted then an attacker can log on to the network and get access to sensitive data, as long as he or she is within range of the access point.

4.1.4. Session Interception and Messages Modification: The attacker can intercept a session and alter the transmitted messages of the session. Another possible scenario by an attacked is to intercept the session by inserting a malicious host between the access point and the end host to form what is called man in the middle. In this case all communications and data transmissions will go via the attacker's host.

4.1.5. Spoofing: The attacker may hijack a session and impersonate as an authorized legitimate user to gain access to unauthorized information and services.

4.1.6. Captured and Retransmitted Messages: The attacker can capture a full message that has the full credential of a legitimate user and replay it with some minor but crucial modification to the same destination or to another one to gain unauthorized access and privileged to the certain computing facilities and network services.

4.1.6. Information Leakage: This potential security issue lies in the possibility of information leakage, through the inference made by an attacker masquerading as a mobile support station. The attacker may issue a number of queries to the database at the user's home node or to database at other nodes, with the aim of deducing parts of the user's profile containing the patterns and history of the user's movements, mobile data storage devices. However, many defense technology experts feel that protection measures remain insufficient for defense needs and therefore must be strengthen with additional safety measures [2]. Mobile devices have extra stringent security needs and are vulnerable to new types of security threats and attacks. They need to operate in foreign networks, such as coffee shops, airport kiosks, or other hotspots, and therefore, can't rely on the organization's firewall for protection. The organization needs a means of managing security configuration, patch deployment and antivirus updates on their devices in the field. The main new mobile computing security issues introduced by the use of mobile devices include the following:

4.1.6.1. Pull Attacks: The attacker controls the device as a source of propriety data and control information. Data can be obtained from the device itself through the data export interfaces, a synchronized desktop, mobile applications running on the device, or the intranet servers [3].

4.1.6.2. Push Attacks: The attacker use the mobile device to plant a malicious code and spread it to infect other elements of the network. Once the mobile device inside a secure network is compromised, it could be used for attacks against other devices in the network [3].

4.1.6.3. Forced De-authentication: The attacker transmits packets proposed to influence a mobile end-point to drop its network connection and reacquire a new signal, and then inserts a crook device between a mobile device and the genuine network.

4.1.6.4. Multi-protocol Communication: This security issue is the result of the ability of many mobile devices to operate using multiple protocols, *e.g.*, one of the 802.11 family protocols, a cellular provider's network protocol, and other protocols which may have well-known security loop-holes. Althou1gh these types of protocols aren't in active usage, many mobile devices have these interfaces set "active" by default. Attackers can take advantage of this vulnerability and connect to the device, allowing them access to extract information from it or use its services.

4.1.6.5. Mobility and Roaming: The mobility of users and data that they carry introduces security issues related to the presence and location of a user, the secrecy and authenticity of the data exchanged, and the privacy of user profile. To allow roaming, certain parameters and user profiles should be replicated at different locations so that when a user roams across different zones, she or he should not experience any degradation in the access and latency times. However, by replicating sensitive data across several sites, the number of points of attack is increased and hence the security risks are also increased.

4.1.6.6. Disconnections: The frequent disconnections caused by hand-offs that occur when mobile devices cross different introduce new security and integrity issues [6]. The transition from one level of disconnection to another may present an opportunity for an attacker to masquerade either the mobile unit or the mobile support station.

4.1.6.7. Delegation: The attacker can hijack mobile session during the delegation process. A delegation is a powerful mechanism to provide flexible and dynamic access control decisions [7]. It is a temporary permit issued by the delegator and given to the delegate who becomes limited authorized to act on the delegator's behalf [3]. Mobile devices have to switch connections between different types of networks as they move and some kind of delegation has to be issues to different network access points. Delegations may be issued and revoked frequently as mobile devices detach and reattach to different parts of the network system.

5. Summary and Conclusion

Mobile Computing is an umbrella term used to describe technologies that enable people to access network services anyplace, anytime, and anywhere. It offers a lot of benefits for everyone especially the end users; however, it requires high security measures and introduces new security issues and challenges. Earlier, when the wireless mobile environment came into existence security was not given a priority. But, as the time passed by, the extent to which this technology is used increased. This created a need to protect the information from unauthorized users and control the fraud. In the beginning, many security protocols where proposed, which were based on cryptographic techniques. In this paper, I have discussed the mobile computing systems, presented and discussed their new security issues and requirements, and presented measures that should be taken to handle wireless networking security issues. I have classified the issue of wireless networks and communication systems. With new loopholes coming up each time, a new protocol was proposed based on the existing one, to answer the problem. Presently, many researchers are concentrating on using the wired based security protocols over the wireless mobile communication. One such research is taking place at Sun Microsystems Labs, where the KSSL protocol is being tested within the corporate campus, using concepts like smart card and certificates. Most security experts agree that users operating or transporting

devices in an unsafe manner form the weakest link in the data security chain. They believe that creating and enforcing a mobile device use policy is the best way to ensure the highest possible level of data security [2]. The main ongoing challenges facing administrators and developers of mobile computing systems are related to how to maintain control over mobile device data with the rapid pace in the production of new mobile devices, mobile operating systems, mobile device applications, wireless network services/devices, and other new mobile technologies. New products typically have only a minimal security knowledge base and are more likely to contain undiscovered security vulnerabilities than technologies that have been around for several years. In addition to this, the ease of downloading and installing mobile devices applications adds to the above challenges in keeping mobile devices safe from malicious third-party applications and security vulnerability. Most significant and robust Encryption application may also lead mobile computing in secure and safe platform for strong communication.

References

[1] A. Leunga, Y. Shengb and H. Cruickshankb, "The security challenges for mobile ubiquitous services", Information Security Group, Royal Holloway, University of London, Egham, UK Centre for Communication Systems Research, University of Surrey, Guildford, Surrey, UK , **(2007)**.
[2] I. Mavridis and G. Pangalos, "Informatics Laboratory, Computers Division", Faculty of Technology Aristotle University of Thessaloniki Thessaloniki 540 06, Greece.
[3] S. Shriraghavan , S. Sundaragopalan, F. Yang and J. Jun, "Introduction to Information Security in mobile computing", **(2003)** November 5.
[4] http://www.naharnet.com/stories/en/676.
[5] http://www.nascio.org/publications/documents NASCIO-Security At The Edge.pdf, **(2009)** July.
[6] T. Imielinski and B.R. Badrinath, "Data management for mobile computing", SIGMOD RECORD, vol. 22, no. 1, **(1993)**, pp. 34-39.
[7] Q. Pham, J. Reid, A. McCullagh and E. Dawson, "Commitment issues in delegation process", Proceedings of the sixth Australasian conference on Information security, Wollongong, Australia. **(2008)** Jan.
[8] L. Zhuang, F. Zhou, B. Y. Zhao and A. Rowstron, "Cashmere: Resilient Anonymous Routing", The 2nd Symposium on Networked Systems Design and Implementation, Boston, MA, **(2005)**.
[9] J. R. Jiang, J. P. Sheu, C. Tu and J. W. Wu, "A secure anonymous routing protocol for wireless sensor networks", IEEE Journal of Information Science and Engineering, vol. 680, no. 2, **(2010)**, pp. 657- 680.
[10] G. J. Serrao, "Network access control (NAC): An open source analysis of architectures and requirements", IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, USA. **(2010)** October 5-8, pp. 94 – 102.
[11] A. Leung and C. J. Mitchell, "Towards Secure Zero Configuration", in Proceedings of Western European Workshop on Research in Cryptography (WeWoRC 2005), Leuven, Belgium, **(2005)** July 5-7, pp. 34-36.
[12] H. Jang, J. Jee, Y. Han, S. Park and J. Cha, "Mobile IPv6 Fast Handovers over IEEE 802.16e Networks," Jun. 2008, IETF RFC 5270.
[13] "Security Issues in Mobile Computing" Srikanth Pullela Department of Computer Science University of Texas at Arlington
[14] Research Dimensions of Advanced Mobile Computing Technology Security Issues for the Complex Applications Bedre Heeramani1, B. Nagaraj2.
[15] Asokan, "Security Issues in Mobile Computing", Univ. of Waterloo, Dept. of Computer Science, Technical Report CS690B, **(1995)** Apr.
[16] C. Perkins, "Mobile IP and Security Issue: An Overview".
[17] M. Pangalos, "Security Issues in a Mobile Computing Paradigm".
[18] M. Elkhodr, S. Shahrestani and K. Kourouche, "A Proposal to improve the security of mobile banking applications", IEEE International conference on ICT and Knowledge Engineering, **(2012)**.
[19] A. K. Talukder and R. R. Yavagal, "Mobile Computing", TaTa McGraw Hill Education, **(2005)** January.
[20] H. Ye, "Design and Implementation of M-Commerce system applied to 3G Network platforms based on J2ME", IEEE International conference on Electrical and Control Engineering, **(2010)**.

