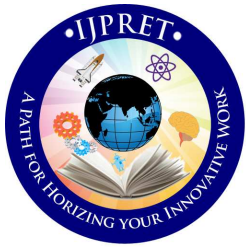
Review Article *ISSN: 2319-507X*
Gajendra Patil, IJPRET, 2012; Volume 1(8): 1049-1057 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

MOBILE COMPUTING AND SECURITY ISSUES

GAJENDRA Y PATIL[1], ANIKET K SHAHADE[1], Dr. GAJENDRA R BAMNOTE[2]

1. Department of Computer Science and Engineering/Information Technology, Shri Sant Gajanan Maharaj College of Engineering, Shegaon.

2. Department of Computer Science and Engineering/Information Technology, Prof. Ram Meghe Institute of Technology & Research, Badnera.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Mobile System,
Mobile Computing,
Security and Mobility

Corresponding Author

Mr. Gajendra Y Patil

Abstract

During the last decade decrease in the computing machinery, coupled with the increase in their computing power has prompted a new concept of computing, called mobile computing. This concept of computing is currently employed in the flourishing number of mobile devices and various portable units. In this paper we included different type of mobile systems ranging from traditional type to nomadic, ad-hoc and finally ubiquitous ones. In this paper we also focus on the concept of informational security in mobile computing.

INTRODUCTION

In the field of computing the birth of "mobile computing" has signalled a new era. The concept of mobile computing is derived from the realization that has computing devices increases in power level and decreases in size and users demand these devices to be a part of their everyday life.

In the last 15 years, the advent of mobile phones as well as laptops and many other mobile devices has dramatically increased the availability of these mobile devices to businesses and home users. Recently the many standard devices such as PDAs and especially embedded devices such as washing machine and sensors changed the think of computers and also a human live.

Mobile Computing is associated with the mobility of hardware, data and software in computer applications. The area of mobile computing has prompted the need to think about the way in which mobile and traditional distributed system may appear to be closely related, there are number of different factor that differentiate the two, especially in terms of type of devices, network connection and execution context.

2. TYPES OF MOBILE SYSTEM

There are different types of mobile system in computer application. In order to understand different mobile systems, we must first understand where the similarities and the differences of distributed and mobile systems lie.

2.1 Traditional Distributed System

Traditional distributed systems are attached to a network and it consists of a collection of fixed hosts – if hosts are disconnected from a network this is considered to be a abnormal whereas in mobile system this is quite the norm. These connected hosts are fixed and are usually very powerful devices with fast processor and large amount of memory. The bandwidth of this system is very high too.

Traditional distributed systems also need to guarantee some requirements which is non-functional such as scalability, openness, Heterogeneity (integration of components written with the help of different programming languages, running on

different operating systems, executing on different hardware platforms), fault tolerance and finally the resource-sharing.

2.2 Nomadic Distributed System

The system which is composed of a set of mobile devices and core infrastructure with some fixes and also wired nodes is known as a Nomadic Distributed System. Mobile devices are move from one location to another location, while maintaining a connection to a fixed network. There may be some problems that arises when shifts in location. The mobile host has a home IP address and thus any packet send to the mobile host will be delivered to the home network and not the foreign network where the mobile host is currently located. Such problem can be solved by forwarding packets to the foreign network with the help of mobile IP also suffers from efficiency (routing issues), QoS Security and wireless access problems.

These systems are susceptible while operating to the uncertainty of location, a repeated lack of connections and the migration into different physical and logical environments while operating. The requirements which is not functional mainly differ, compared to the traditional distributed systems, in the resource sharing (must take into account different issues when the resource need to be discovered), heterogeneity (affected by the presence of both mobile and fixed devices across the network and also the variation in technologies) and fault tolerance of the system.

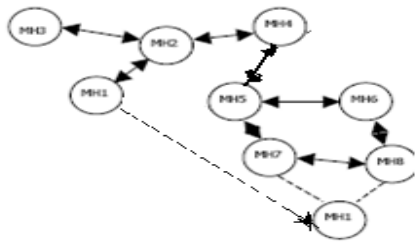
2.3 Ad-Hoc Mobile Distributed System

The network that comes close to the mobile networks in the sense that every node is a mobile is an Ad-Hoc distributed system. It is this network that are very much seen as the system of the network which is executed in dynamic environment and through very high variable quality links.

Ad-Hoc system normally does not have any fixed infrastructure which differs them both from nomadic and traditional distributed systems. In fact, ad-hoc networks may come together as needed, not necessarily with any assistance from the existing infrastructure. When nodes detached from fixed/mobile network they may evolve independently and groups of hosts

opportunistically from mini-networks and clusters. The speed and ease of deployment make ad-hoc networks highly desirable.

These kinds of systems are extremely useful in condition where the infrastructure is absent, impractical to establish or even expensive to build. Security threats have to be dealt even more cautiously in ad-hoc networks. Secure key distribution in ad-hoc network might be an extremely hard task. Additional problem include the increased packet sizes required by authentication extension, Quality of Service support and power aware routing. Furthermore due to the limited transmitted range of wireless network interfaces, multiple hops may be needed to exchange data between nodes in the network.



Ad Hoc network of mobile nodes – these are able to move relative to each other. MH1 moves away from MH2 and establishes new links with MH7 and MH8. Most algorithms also allow for the appearance of new mobile nodes and the disappearance of previously available nodes.

3. Security issues in mobile computing

In this section we discuss some security issues pertaining to the mobility factor on mobile computing.

3.1 Security and Mobility

In the fact that data which is carried by the users have become a mobile component in computing has itself introduced s set of security problems different to that in traditional mobile computing. In the case of non-mobile computing that is in fixed mobile computing physical protection could easily be afforded by making database system and computer physically isolated from the other component in the everyday life. In such a configuration it was possible to make the system self-sufficient, without any need to communicate with the external world. Now-a-days a firewall technique may also be applied to achieve the same effect.

In mobile computing, this form of isolation and self-sufficiency is difficult to achieve due to the resources are limited to mobile unit, thereby necessitating it to communicate with the mobile support station. The mobility of users and data that

they carry introduces security problem from the point of view of the existence and location of a user on a mobile wireless network may choose to have the information concerning his or her existence treated as being confidential. That is, a user may choose to remain anonymous to the users majority on the network, with the exception of a select number with whom the user often interacts. This problem of anonymity in mobile computing is related to a more difficult problem of the trust level afforded by each node in the wireless network and the problem of the trust level afforded by the wireless network in each node and the problem of security of location data concerning a user when the location data is stored or transferred between nodes as the user moves in a nomadic fashion. These nodes must provide some assurance to the users about his or her anonymity, independent of the differing levels of trust that may exists for each node.

Most essential potential security problem lies in the possibility of information leakage through inference made by an attacker masquerading as a mobile support station with or without the aid of a mobile support station which is subverted. The attacker which masquerades as a mobile support station may issue a number of queries to the database to the user's home node and may also be to the database at other nodes, with the aim of deducing part of the users profile containing the patterns and history of the user's movements. Here again, security techniques are required both for the databases and identification of users and mobile support stations in the network. In general, if we replicated the sensitive data across several sites, the security risks are also increased due to the multiplication of the point of attack.

3.2 Security in Disconnections

The disconnection is the major issues in mobile computing which arises from battery power and mobility restrictions. The disconnection of mobile unit from a mobile support station is necessary requirement for the conservation of power of the mobile unit. A mobile unit can typically find itself running on a temporary form of power supply such as battery while its main power source is being recharged. In this situation differing levels of disconnection may be

introduced ranging from the normal connection to connections using the low bandwidth channels.

There are two aspects of disconnections as elective or non-elective nature of disconnections. The non elective disconnections is the case in which mobile unit disconnects due to some unforeseen event, such as system crashes or total communication crashes or total communication break-down when moving into certain geographic regions.

In both types of disconnections, a number of potential security loop-holes may be introduced. Any disconnection transition scheme must ensure that an attacker should not be able to "hi-jack" the communications of a mobile unit which is stepping down its level of connections and then masquerading as the mobile unit that is about to step-up its level of connection.

Security and integrity problems may occur in the case when hand-offs occur between two mobile support stations as the mobile unit crosses zones. Other security problem may occur when a mobile unit deposits a "timed" transaction at a fixed node, which begins to execute when certain conditions are met and which transmits the result back to the nomadic mobile unit. These scenarios represent only a few potential security problems among many others in the context of disconnections and transaction management in mobile computing.

3.3 Secure Data Access Methods

One of the main advantages of mobile computing derives from the possible use of broadcasting techniques to provide services to varying sizes of audience groups of users with minimal change in the delivery cost of the services. Two methods of delivering information to the various mobile devices of users by a broadcast server, namely through data broadcasting and interactive requests serve the purpose. The possibility of continuous broadcasting of ever-changing data lends to the attractive notion of data broadcasting being a public form of "memory", where mobile units periodically refresh their limited memory such as caches and buffers using some data which is available. The two most essential parameter related to the broadcasting of data are access time and tuning time, the

first time referring to the time taken for a reply to be received by a mobile unit at the client side from the broadcast server, the later referring to the amount of time taken by the client in "listening" to the channel in order to obtain the needed data. Here, the mobile unit will first listen to an "index channel" that delivers a directory information as a guide as to when the mobile unit should access the stream of data.

There are a number of issues related to the security and the integrity of data. The first is the authentication of the source of the broadcast server by the mobile units. Since such a broadcast may carry public data whose accuracy is paramount and whose authority for publication is accepted by the community, source authentication and integrity becomes as minor inaccuracies may result in a great losses on the part of the users. Therefore, methods are needed for initial source authentication by the mobile units and for the periodic source re-authentication by the mobile units in such a way that it consumes less power than the initial authentication. Such methods would be attractive if they use some security parameters such as cryptographic parameter which is embedded within the stream of broadcast data and which are recognizable at a given time only by the mobile units that require performing re-authentication procedures for different mobile unit users at different moments in time.

Together with source authentication comes to the need to maintaining integrity of the broadcast data stream. There are number of possible attacks scenarios present themselves, one being the denial of service attack ranging from crude channel interference to the sophisticated modifications of the index channel resulting in the mobile unit listening to incorrect useless part of the broadcast stream. More sophisticated attacks may even attempts to substitute segments from both the index channel and the data stream in such a way that the mobile unit is unaware of the attacks.

The notion of a continuous broadcast of data being a public "memory" together with the limited physical memory such as cache available at the mobile unit lead to the

important issue of trust accorded by the users to the source of broadcast. Since the public memory will become the fleeting entity of a short lifetime, accountability of the source and the auditability of the broadcast data become necessary to prevent the source becoming a main big component that has control over the short memory of the public.

4. Conclusion

In this paper we have included different type of mobile systems ranging from traditional type to nomadic, ad-hoc and finally ubiquitous ones and also proposed security to be a major category for future developments in mobile computing. We have also discussed in brief, the issues of security in a mobile computing environment because considerable effort is being focused towards research in mobile computing, much of its concentrating on the performance and availability of mobile computing, with comparatively little attention being given to the security issues in a mobile communication.

References

1. L. Gong, "Increasing Availability and security of an authentication service," IEEE Journal on Selected Areas in Communication, vol. 11, no. 5, pp.657-662, 1993.

2. B. R. Badrinath and T. Imielinski, "Replication and Mobility," in Proceedings of the 2nd IEEE Workshop on management of Replicated Data, pp. 9-12, IEEE, November 1992.3

3. D. Brown, " Security planning for personal communication," in Proceeding of the 1st ACM Conference on computer and Communication Security, pp. 107-111, ACM Press, 1993.

4. Agrawal D P and Zeng Q A, "Introduction to Wireless and Mobile Systems",(CENGAGE)(2/e)

5. C. K. Toh, "Ad Hoc Mobile Wireless Networks: Protocol & Systems", (Pearson Edu.)

6. J. Seberry and J. Pieprzk, Cryptography: An Introduction to Computer Security. Sydney: Prentice Hall, 1989.

7. T. Imielinski and B. R. Badrinath, "Mobile wireless computing: Solutions and challenges in data management," Technical Report DCS –TR-296/WINLAB-TR-49, Department of computer science, Rutgers University, NJ, 1992.