Security Issues In Mobile Computing

Dineshkumar P[1], Ranjith T [2], Yogeswaran M[3], Prasanth P[4]
[1, 2, 3, 4] Dept of MCA
[1, 2, 3, 4] Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India-632102

Abstract- *In the present mobile communication environment,lot of research is going on,to improve the performance of issues like hanoffs,routing etc.mobile computing and mobile commerce is most popular now a days because of the server offered during the mobility.Mobile Computing has become the reality today rather than the luxury.Online transaction using mobile device must ensure high security for user credentials and it should not be possible for misuse. Laptop computers, cell phones, mobile data storage devices have become very popular because of their convenience and portability in issues.*

I. INTRODUCTION

The rapid development of wireless technology in particular mobile computing technology, that's make its device more popular and interesting by user these days. The mobile computing technologies are updated every second Thousands of mobile data applications which can access by many mobile users

Mobile Computing provides flexibility of computing environment over physical mobility. The user of a mobile computing environment will be able to access to data, information or other logical objects. From any device in any network while on the move to make a mobile computing environment are spread over wired and wireless device. Mobile computing is a any type of computing which use internet or intranet and respective communication links, as WAN,LAN,WLAN,etc.

II. TRADITIONAL SECURITY ISSUES

There are several traditional security issues in information systems in general that are addressed by any application developer and are more relavant in mobile computing system.

Confidentiality: This ensures that information stored on a system or transmitted over communication links, is only disclosed to those users who are authorized to have access to it. It protects the privacy of the information exchanged between any two or more devices or systems.

Integrity: This prevents against intentional or unintentional data modifications during transmission. It ensures that information exchanged between different parties is accurate, complete and not altered during transmission.

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.

Authorization: This ensures that the service requested as the right to access the information on different network or mobile resources.

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.

Availability: This ensures that the mobile computing environment or the services of the information systems are all the time available for users.

III. WIRELESS NETWORK SECURITY ISSUES

Wireless networks have their own 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.

Denial of Service: This attack is characterized by an explicit attempt by attackers to present legitimate users of a service from using that services.

Traffic Analysis: The attacker can moniter the transmission of data, measures the load on the wireless communication channel, capture packets, and reads the source and destination fields.

Eavesdropping: this is a well known security isstion:ues in wireless networks.Session interception and messages modification:The access point and the end host to form what is

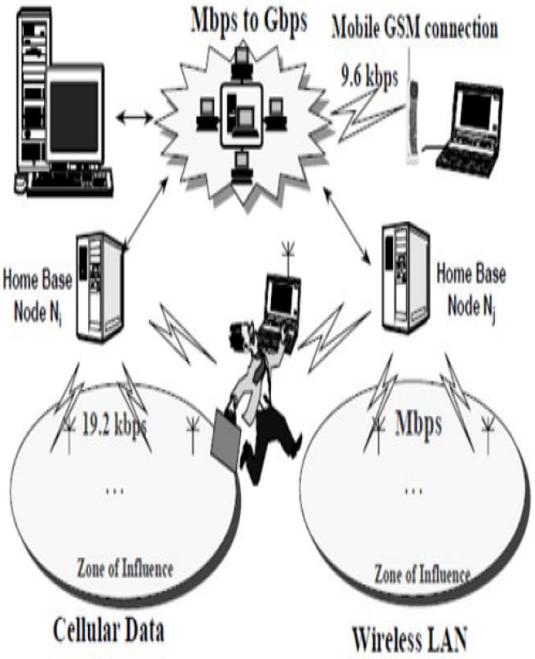
called man-in-the-middle.In this case all communications and data transmissions will go via the attacker's host.

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

Information leakage: This potential security issues lies in the possibility of information leakage, through the inference made by an attacker masquerading as a mobile support station.

IV. MOBILITY AND SECURITY

The fact that both users and the data that they carry have became a mobile component in computing has in itself introduced a set of security problems different to that in traditional computing.In the tradiational case of fixed (non-mobile)computing physical protection could easily be afforded by making the computer and database system physically isolated from the other components in the environment.The mobility of users and the data that they carry introduces security problems.From the point of view of the existence and location of a user



MOBILE COMPUTING ENVIRORNMENT

SECURITY ISSUES:

Many other seven have presented classification of security issues in communication networks.

Confidentiality, preventing unauthorized users from gaining access to critical information cannot take place.

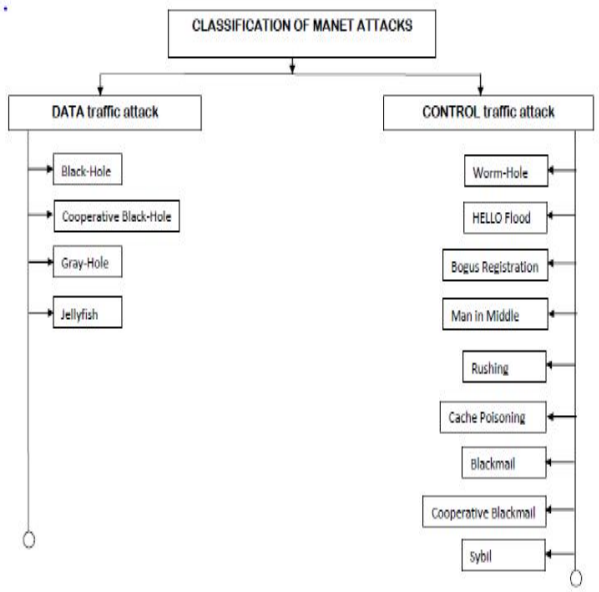
Integrity, ensures unauthorized modification, destruction or creation of information cannot take place.

Availability, ensuring authorized users getting the access they require.

Legitimate, ensuring that only authorized users have access to services.

Accountability, ensuring that the users are herd responsible for there security related activities by arranging the user and his/her activities are linked if and when necessary.

V. CLASSIFICATION OF SECURITY ATTACK



DATA Traffic Attack:

DATA traffic attack deals either in nodes dropping data packets passing through them or in delaying of forwarding of the data packets.This alsocauses significant loss of important data. For e.g., a 100Mbps wireless link can behave as1Mbps connection.

Black-Hole Attack: In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole.

Cooperative Black-Hole Attack: This attack is similar to Black-Hole attack, butmore than one malicious node tries to

disrupt the network simultaneously. It is one of the most severe DATA traffic attack and can totally disrupt the operation of an AdHoc network.

Gray-Hole Attack: Gray-Hole attack has its own characteristic behavior. It too drops DATA packets, but node's malicious activity is limited to certain conditions or trigger [102].

Jellyfish Attack: Jellyfish attack is somewhat different from Black-Hole & Gray-Hole attack.

Control Traffic Attack:
It can also eavesdrop on the network if the node can establish itself as the shortest route to any destination by exploiting the unsecure routing protocols.

Worm Hole Attack: Worm hole, in cosmological term, connects two distant points inspace via a shortcut route.

HELLO Flood Attack: The attacker node floods the network with a high quality route with a powerful transmitter.

Bogus Registration Attack: Encrypting packets before sending and secure authentication in route discovery (SRDP, SND, SNRP, ARAN, etc) will limit the severity of attack to some extent as attacker node has no previous knowledge of encryption method [138].

Man in Middle Attack: In Man in Middle attack, the attacker node creeps into a valid route and tries to sniff packets flowing through it.

Rushing Attack: Some of the protocols use duplicate suppression mechanism to limit the route request and reply chatter in the network.

Cache Poisoning Attack: If some malicious node performs a routing attack then they will stay in node's route table until timeout occurs or a better route is found.

Blackmailing and Co-operative Blackmailing Attack: In a blackmailing attack or more effectively co-operative blackmailing attack, attacker nodes accuse an innocent node as harmful node.

Sybil Attack: Sybil attack manifests itself by faking multiple identities by pretending to be consisting of multiple nodes in the network.

VI. OPERATIONAL PROBLEMS

Some of the problems that wireless communication introduces are:

Disconnection. Wireless communications suffer from frequent disconnections can be hidden by asynchronous operation.
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
Heterogeneous network. To achieve wireless communication a mobile host must get connected to different and heterogeneous networks.

Security Risks. Precisely because connection to a wireless link is so easy, the security of wireless communication can be compromised much more easily than that of wired communication.

Address Migration. This a consequence of mobility and several techniques such as selective broadcast, central services, home bases and forwarding pointers may provide solutions (Forman and Zahorian, 1994).

Location-dependent Information. Information needed to configure a computer, such as the local name server, available printers, time zone, etc., is location dependent. Mechanisms are needed for obtaining configuration data appropriate to each location.

Privacy. Answering dynamic location queries requires knowing the location of other mobile users. Such information should be protected against misuse and this can be achieved by denying users the availability to know other users' location (Spreitzer and Theimer, 1993).

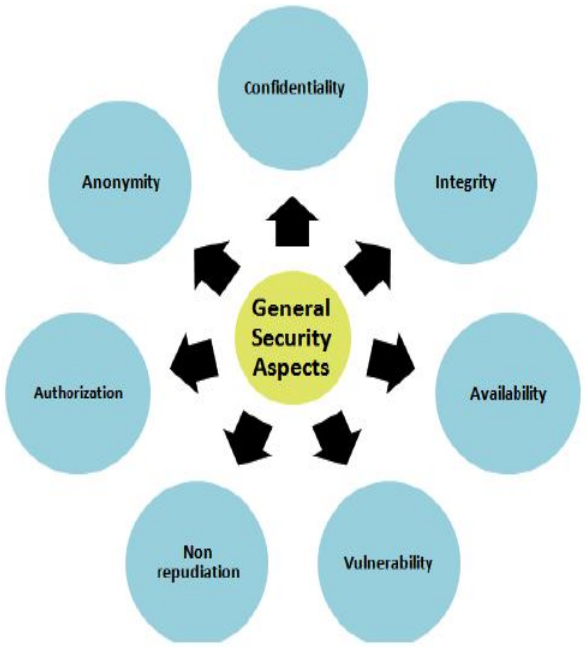
Inter-realm support. Designing distributed services to support the mobile user. Providing authentication, accounting and management over a wide area and across organisations (Duchamp, 1992).

VII. GENERAL SECURITY ASPECTS

Security is an important consideration and it should be taken in all aspects of computing, especially in mobile computing because the mobile user may face many security threats that may be not exposed to the traditional computing user

Security principles or aspects of computer systems are related to confidentiality, integrity, availability,

vulnerability, non-repudiation, authorization, and anonymity which is shown in Fig.



General security aspects

VIII. MOBILE SECURITY REQUIREMENTS

This is because the mobile devices, computers, and networks used for mobile computing may not be owned by these organizations and may be shared by anyone. Therefore,security controls implemented on the systems within the organizations are not enough and must be complemented by other security mechanisms on top of a mandatory good practice by their mobile users.

Encryptions: If critical information is held on a mobile device, data encryption should be done to protect the data and prevent access by unauthorized persons.

Compliance. Remote and wireless network access from mobile devices must be subject to the same organization's internal network security policies compliance and measures applied to inner users.Access and connection through public hotspots should be avoided.

Standards. Mobile users must ensure that the mobile devices they use and the information they contains are well protected at all times and adhere to a set of requirements such as strong password protection,full disk strong encryption, locking, regular backups, current antivirus software, firewalls with similar configuration to the organization network's configuration

Routing anonymity. To prevent communication endpoints from being linked, anonymous routing may be used at the network layer.

VPN and Wireless Encryption Protocol. A strong wireless encryption protocol should be used whenever possible, and all external connections to the internal organizational network must be over an encrypted virtual private network (VPN).

Network Access Control (NAC). Network Access Control system should be in place to check and analyze mobile devices trying to connect to the organization network.

IX. CONCLUSION

The paper analysis of security issues in mobile computing. These issues classified into catagories like mobility, security, and control traffics. we mainly discusses about the types of attack in the mobile adhoc network. there is a brief introduction about the classification of attack. According to these attacks we survey security issues in mobile networks. mobile computing is a generic term is evolved in morden usage requires in mobile computing and connecting wirelessly to and through the internet. Especially in wireless communication, mobile agent are used to provide a reliable solution given the wide range of existent application. In this paper,we presented the general technologies infrastructure. A brief history of the evolution of mobile technologies was reviewed; where it found that the first call phone of mobile was made in 1946.The prevalent different aspects of mobile computing with other computing are, wireless network connectivity, security aspects of compter system are confidentiality, integrity, availability, vulnerability, non repudiation and authorization.

In these paper mainly research about the mobile computing securities in work station to users.the user can securely used in the mobile communication in the internet and private network.

REFERENCES

[1] J. Korhonen, T. Savolainen, and J. Soininen, *Deploying IPv6 in 3GPP Networks: Evolving Mobile Broadband from 2G to LTE and Beyond*, John Wiley & Sons. E, 2013.

[2] J. York and P. C. Pendharkar, "Human–computer interaction issues for mobile computing in a variable work context," *International Journal of Human-Computer Studies*, vol. 60, no. 5, pp. 771-797, 2004

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2, pp. 293-315, 2003.
[4] J. Friedman and D. V. Hoffman, "Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses," *Information, Knowledge, Systems Management*, vol. 7, no. 1, pp. 159-180, 2008.
[5] Vipul Gupta and Sumit Gupta "Securing the Wireless Internet" IEEECommunications 2001.and Knowledge Engineering,2012

REFERENCE

1. RANJITH.T
9943180538,
ranjiththamo@gmail.com

2. DINESHKUMAR.P
9952270297, 9994210297
dineshtvmalai297@yahoo.in

3. YOGESWARAN.M
9486182010
yokesh.8593@gmail.com

4. PRASANTH.P
9751378045, 9566881349,
pprasanth9797.ahen@gmail.com