CHAPTER 5

THREATS AND SECURITY ISSUES IN MOBILE COMPUTING

Mobile computing is a form of human–computer interaction by which a computer is expected to be transported during normal usage. Mobile Computing is a variety of wireless devices that has the mobility to allow people to connect to the internet, providing wireless transmission to access data and information from where ever location they may be. Mobile computing has three aspects: mobile communication, mobile hardware, and mobile software. The first aspect addresses communication issues in ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. The second aspect is on the hardware, e.g., mobile devices or device components. The third aspect deals with the Mobile computing is taking a computer and all necessary files and software out into the field. With the rapid growth in the wireless mobile communication technology, small devices like PDAs, laptops are able to communicate with the fixed wired network while in motion. Because of its flexibility and provision of providing ubiquitous infrastructure, the need to provide security increases to a great degree.

5.1 Mobility and Security

The fact that both users and the data that they carry have become a mobile component in computing has in itself introduced a set of security problems different to that in traditional computing. In the traditional case of fixed (non-mobile) computing physical protection could easily be afforded by making a computer and database system physically isolated from the other components in the environment. In such a configuration it was possible to make the system self-sufficient, without any need to communicate with the external world. More recent firewall techniques may also be applied to achieve the same effect. In mobile computing this form of isolation and self-sufficiency is difficult to achieve due the relatively limited resources available to a mobile unit, thereby necessitating it to communicate with the mobile support station [145]. 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 (which is deemed to be data in them) and the secrecy and authenticity of the data exchanged between users and between a user and a fixed host.

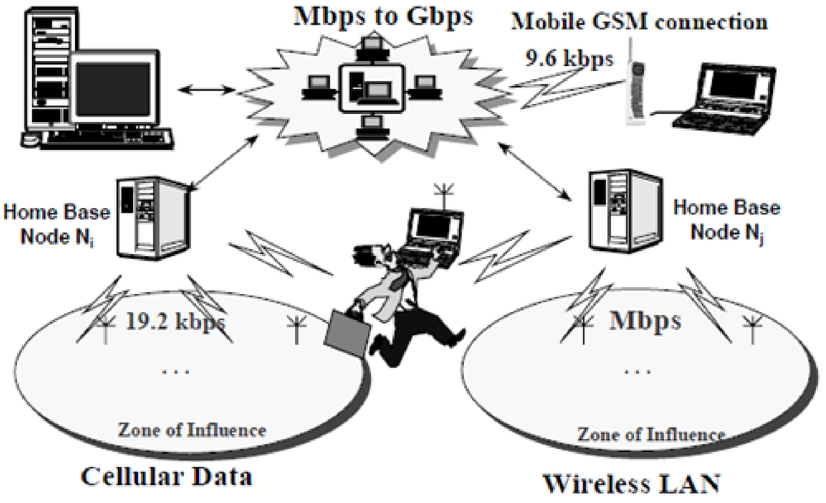


Figure 5.1: Mobile Computing Environments

More specifically, 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 majority of other users on the network, with the exception of a select number with whom the user often interacts. This problem of user 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 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 [150]. These nodes must provide some assurance to the user about his or her anonymity, independent of the differing levels of trust that may exist for each node. This requirement is of particular importance in the case of a user that crosses between two zones which are under two nodes respectively, each having a different trust level [141]. Equally important is the secure transfer of data between databases at nodes which hold location data and other information or parameters in the user profile. Here all traffic internal to the network and transparent to the nomadic user must be maintained secure and authentic. Another potential security problem lies in the possibility of information leakage through the inference made by an attacker masquerading as a mobile support station with or without the aid of a subverted mobile support station. The attacker which masquerades as a mobile support station 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 profile containing the patterns and history of the user's movements. Here again, security techniques are required both for the databases and for the identification of users and mobile support stations. Any scheme to be used must ensure that any queries submitted to a given database at a user's home-base is accompanied by sufficient proof that the user approves of the queries submitted by the (foreign) mobile support station controlling the zone under which the user is currently roaming or passing through [142]. It is, therefore, not unreasonable to assume that some method of delegation of rights will be employed between the user and the mobile support stations (and fixed hosts) in the network. Related to the management of these databases and the provision of performance transparency for the nomadic user is the issue of replication of certain parameters and user profiles with the aim of replicating the environments surrounding the users [144]. Thus, as the user roams across zones, the user must not experience degradation in the access and latency times. Again, security must be considered in the context of replication, both from the trust level of the mobile support stations and fixed hosts and from the point of view of data leakage. In general, as sensitive data is replicated across several sites, the security risks are also increased due to the multiplication of the points of attack [143].

5.2 Threats to Mobile Computing

Mobile computing brings with it threats to the user and to the corporate environment. From personal information to corporate data, mobile devices are used for a wide variety of tasks by individuals and companies. Mobile devices have added a new threat to the corporate landscape as they have introduced the concept of bring your own device [134]. While this is not necessarily an entirely new concept, the wide acceptance of bring your own device with mobile devices has created a paradigm shift, where the security and safety of the device is not necessarily to protect the corporate data, but to keep the personal data out of the hands of corporate management.

- **Data Loss from lost, stolen, or decommissioned devices**: By their nature, mobile devices are with us everywhere we go. The information accessed through the device means that theft or loss of a mobile device has immediate consequences. Additionally, weak password access, no passwords, and little or no encryption can lead to data leakage on the devices. Users may also sell or discard devices without understanding the risk to their data. The threat level from data loss is high, as it occurs frequently and is a top concern across executives and IT admin.

- **Information stealing mobile malware:** Android devices, in particular, offer many options for application downloads and installations. Unlike iOS devices, which need to be jail broken, Android users can easily opt to download and install apps from third-party marketplaces other than Google's official Play Store marketplace. To date, the majority of malicious code distributed for Android has been disseminated through third-party app stores. Most of the malware distributed through third-party stores has been designed to steal data from the host device. This threat level is high, as Android malware in particular is becoming a more popular attack surface for criminals who traditionally have used PCs as their platforms. 3. Data Loss and data leakage through poorly written third-party applications: Applications for smart phones and tablets have grown exponentially on iOS and Android. Although the main marketplaces have security checks, certain data collection processes are of questionable necessity; all too often, applications either ask for too much access to data or simply gather more data than they need or otherwise advertise. This is a mid-level threat. Although data loss and leaking through poorly written applications happens across mobile operating systems.
- **Vulnerabilities within devices, OS, design, and third-party applications:** Mobile hardware, OS, applications and third-party apps contain defects (vulnerabilities) and are susceptible to ex-filtration and/or injection of data and/or malicious code (exploits). The unique ecosystem inherent in mobile devices provides a specialized array of security concerns to hardware, OS, and application developers, as mobile devices increasingly contain all of the functionalities attributed to desktop computing, with the addition of cellular communication abilities. This is a mid-level threat; although the possibility is high, the number of exploits is not.
- **Unsecured WiFi, network access, and rogue access points**: This has increased the attack surface for users who connect to these networks. In the last year, there has been a proliferation of attacks on hotel networks, a skyrocketing number of open rogue

access points installed, and the reporting of eavesdropping cases. This threat level is high. Increased access to public WiFi, along with increased use of mobile devices, creates a heightened opportunity for abuse of this connection.

- **Unsecured or rogue marketplaces:** Android users can easily opt to download and install apps from third-party marketplaces other than Google's official Play Store marketplace. To date, the majority of malicious code distributed for Android has been distributed through third-party app stores. This threat level is high: Android malware in particular is being distributed through these marketplaces more and more frequently.
- **Insufficient management tools, capabilities, and access to APIs (includes personas):** Granting users and developers access to a device's low-level functions is a double-edged sword, as attackers, in theory, could also gain access to those functions. However, a lack of access to system-level functions to trusted developers could lead to insufficient security [100]. Additionally, with most smart phone and tablet operating systems today, there is little, if any, guest access or user status. Thus, all usage is in the context of the admin, thereby providing excessive access in many instances. This is a mid-level threat.
- **NFC and proximity-based hacking:** Near-field communication (NFC) allows mobile devices to communicate with other devices through short-range wireless technology. NFC technology has been used in payment transactions, social media, coupon delivery, and contact information sharing. Due to the information value being transmitted, this is likely to be a target of attackers in the future. The threat level is low, as the threat is still in the proof-of-concept phase.

5.3 Security Countermeasures

Secure mobile computing is critical in the development of any application of wireless networks.

5.3.1 Security Requirements

Similar to traditional networks, the goals of securing mobile computing can be defined by the following attributes: availability, confidentiality, integrity, authenticity and non-repudiation.

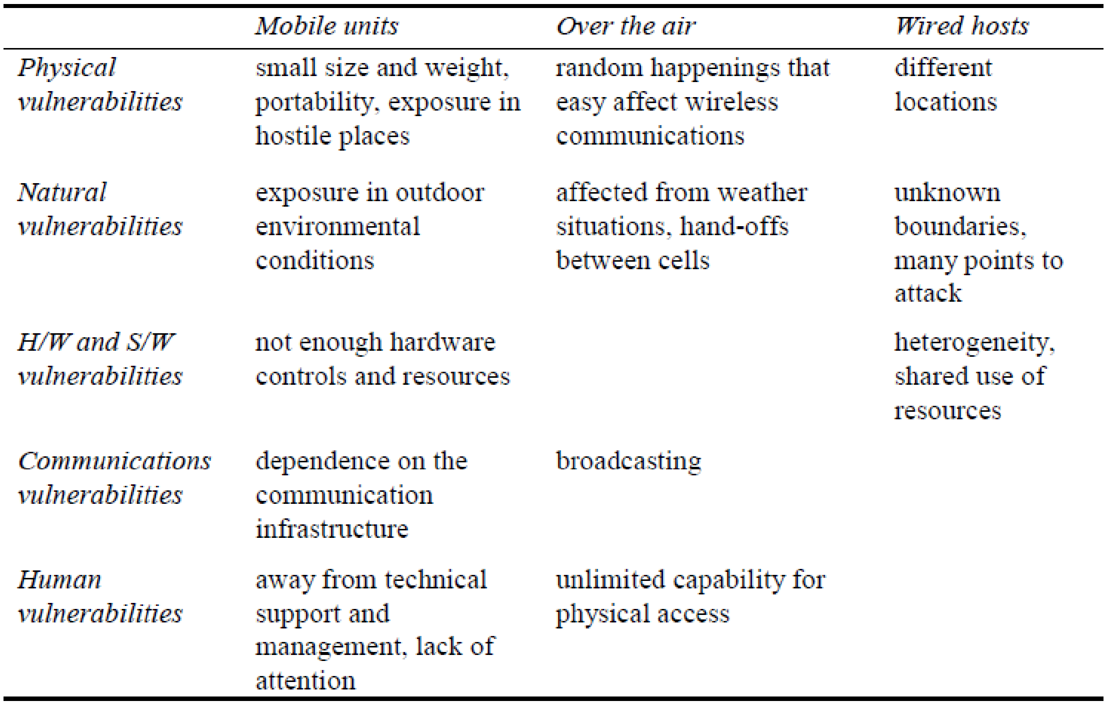
- Availability ensures that the intended network services are available to the intended parties when needed.
- Confidentiality ensures that the transmitted information can only be accessed by the intended receivers and is never disclosed to unauthorized entities.
- Authenticity allows a user to ensure the identity of the entity it is communicating with. Without authentication, an adversary can masquerade a legitimate user, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of users.
- Integrity guarantees that information is never corrupted during transmission. Only the authorized parties are able to modify it.
- Non-repudiation ensures that an entity can prove the transmission or reception of information by another entity, i.e. sender/receiver cannot falsely deny having received or sent certain data.
- In ad hoc networks, mobile hosts are not bound to any centralized control like base stations or access points. They are roaming independently and are able to move freely with an arbitrary speed and direction. Thus, the topology of the network may change randomly and frequently. In such a network, the information transfer is implemented in a multi-hop fashion, i.e., each node acts not only as a host, but also as a router, forwarding packets for those nodes that are not in direct transmission range with each other. By nature, an ad hoc network is a highly dynamic self-organizing network with scarce channels. Besides these security risks, ad hoc networks are prone to more security threats due to their difference from conventional infrastructure-based wireless networks.
- The Lack of Pre-fixed Infrastructure means there is no centralized control for the network services. The network functions by cooperative participation of all nodes in a distributed fashion. The decentralized decision making is prone to the attacks that are designed to break the cooperative algorithms. A malicious user could simply block or modify the traffic traversing it by refusing to cooperate and break the cooperative algorithms. Moreover, since there are no trusted entities that can calculate and distribute the secure keys, the traditional key management scheme cannot be applied directly.

- Dynamically Changing Topology aids the attackers to update routing information maliciously by pretending this to be legitimate topological change. In most routing protocols for ad hoc networks, nodes exchange information about the topology of the network so that the routes could be established between communicating nodes. Any intruder can maliciously give incorrect updating information. For instance, DoS attack can be easily launched if a malicious node floods the network with spurious routing messages. The other nodes may unknowingly propagate the messages.
- Energy Consumption Attack is more serious as each mobile node also forwards packets for other nodes. An attacker can easily send some old messages to a node, aiming to overload the network and deplete the node's resources. More seriously, an attack can create a rushing attack by sending many routing request packets with high frequency, in an attempt to keep other nodes busy with the route discovery process, so the network service cannot be achieved by other legitimate nodes.
- Node Selfishness is a specific security issue to ad hoc network. Since routing and network management are carried by all available nodes in ad hoc networks, some nodes may selfishly deny the routing request from other nodes to save their own resources (e.g., battery power, memory, CPU).

5.4 Security Issues Involved In Mobile Computing

- Mobile security or mobile phone security has become increasingly important in mobile computing. 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.

Table 5.1: Security Vulnerabilities of a general mobile computing system



	Mobile units	*Over the air*	*Wired hosts*
Physical vulnerabilities	small size and weight, portability, exposure in hostile places	random happenings that easy affect wireless communications	different locations
Natural vulnerabilities	exposure in outdoor environmental conditions	affected from weather situations, hand-offs between cells	unknown boundaries, many points to attack
H/W and S/W vulnerabilities	not enough hardware controls and resources		heterogeneity, shared use of resources
Communications vulnerabilities	dependence on the communication infrastructure	broadcasting	
Human vulnerabilities	away from technical support and management, lack of attention	unlimited capability for physical access	

- All smart phones, 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, WIFI NETWORKS. There are also attacks that exploit software vulnerabilities from both the web browser and operating system.
- 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.
- One of the key issues of these being, confidentiality and authentication, where the user must be protected from unauthorized eavesdropping. The goal of authentication protocol is to check the identity of other users or network centers before providing access to the confidential information on the user side. When designing any security protocol, there are certain conditions that need to be considered. Firstly, the low computational power of the mobile users and secondly, the low bandwidth available. Therefore, it is important to design the security protocols so as to minimize, the number of message exchanges and the message size. a few authentication protocols that were proposed to provide security between the users and the network. These

protocols are based on the use of certificates, which are built on the concept of security keys (cryptography). Another protocol that is discussed in this paper is the Kilo Byte Secure Socket Layer (KSSL) protocol, which is an extension of Secure Socket Layer (SSL) protocol used for wired networks.

5.5 Classification of Security Attacks

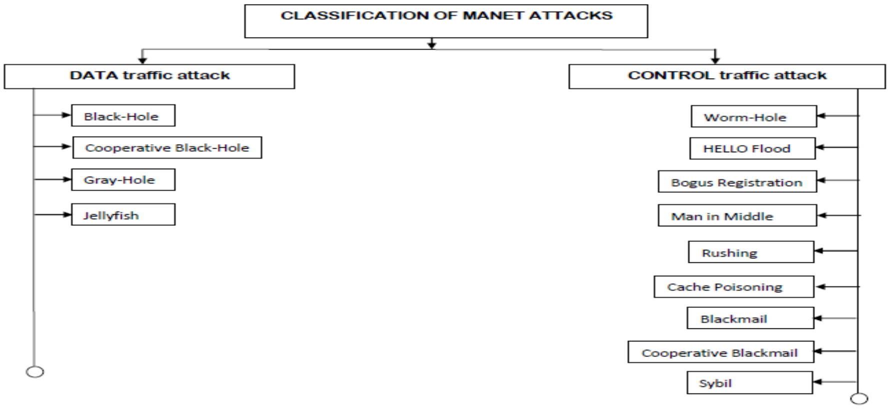


Figure 5.2: Classification of Security Attacks

5.5.1 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. Some types of attacks choose victim packets for dropping while some of them drop all of them irrespective of sender nodes. This may highly degrade the quality of service and increases end to end delay. This also causes significant loss of important data. For e.g., a 100Mbps wireless link can behave as 1Mbps connection. Moreover, unless there is a redundant path around the erratic node, some of the nodes can be unreachable from each other altogether.

- **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. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network in to two disconnected components the Black-Hole node separates the network into two parts. Few strategies to mitigate the problem: (i) collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found. (ii) Maintaining a table in each node with previous sequence number in increasing order. Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbors and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong.

- **Cooperative Black-Hole Attack:** This attack is similar to Black-Hole attack, but more 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 Ad Hoc network. Mostly the only solution becomes finding alternating route to the destination, if at all exists. Detection method is similar to ordinary Black-Hole attack. In addition another solution is securing routing and node discovery in MANET by any suitable protocol such as SAODV, SNRP, SND, SRDP etc. Since each node is already trusted, black hole node should not be appearing in the network [102, 135].

- **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]. Two most common type of behavior: (i) Node dependent attack – drops DATA packets destined towards a certain victim node or coming from certain node, while for other **nodes** it behaves normally by routing DATA packets to the destination nodes correctly. (ii) Time dependent attack – drops DATA packets based on some predetermined/trigger time while behaving normally during the other instances. Detecting this behaviorist attack is very difficult unless there exist a system wide detection algorithm, which takes care of all the nodes performance in the network. Sometimes nodes can interact with each other and can advise malicious nodes existence to other friendly nodes. Approach is similar to Black-Hole attack where sequence number feedback might detect some Gray-Hole attack. If multiple paths exist between sender and destination then buffering packets with proper acknowledgement might detect active Gray-Hole attack in progress. But dormant or triggered attack is difficult to detect with this approach.

- **Jellyfish Attack:** Jellyfish attack is somewhat different from Black-Hole & Gray-Hole attack. Instead of blindly dropping the data packets, it delays them before finally delivering them. It may even scramble the order of packets in which they are received and sends it in random order. This disrupts the normal flow control mechanism used by nodes for reliable transmission. Jellyfish attack can result in significant end to end delay and thereby degrading QoS.

5.5.2 Control Traffic Attack

Mobile Ad-Hoc Network (MANET) is inherently vulnerable to attack due to its fundamental characteristics, such as open medium, distributed nodes, autonomy of nodes participation in network (nodes can join and leave the network on its will), lack of centralized authority which can enforce security on the network, distributed co-ordination and cooperation [60, 131]. The existing routing protocols cannot be used in MANET due to these reasons. Many of the routing protocols devised for use in MANET have their individual characteristic and rules. Two of the most widely used routing protocols is Ad-Hoc On Demand Distance Vector routing protocol (AODV), which relies on individual node’s cooperation in establishing a valid routing table and Dynamic MANET On-Demand (DYMO) , which is a fast light weight routing protocol devised for multi hop networks [135]. But each of them is based on trust on nodes participating in network. The first step in any successful attack requires the node to be part of that network. As there is no constraint in joining the network, malicious node can join and disrupts the network by hijacking the routing tables or bypassing valid routes. 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. Therefore it is of utmost importance that the routing protocol should be as much secure as it can be [60].

- **Worm Hole Attack:** Worm hole, in cosmological term, connects two distant points in space via a shortcut route. In the same way in MANET also one or more attacking node can disrupt routing by short-circuiting the network, thereby disrupting usual flow of packets. If this link becomes the lowest cost path to the destination then these malicious nodes will always be chosen while sending packets to that destination [131]. The attacking node there have been few proposals recently to protect networks from worm-hole attack: Geographical leashes & temporal leashes: A leash is added to each packet in order to restrict the distance the packets are allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new leash. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet. A temporal leash provides an upper bound on the lifetime of a packet. Using directional antenna: Using directional antenna restricts the direction of signal propagation through air. This is one of the crude ways of limiting packet dispersion [136].

- **HELLO Flood Attack:** The attacker node floods the network with a high quality route with a powerful transmitter. So, every node can forward their packets towards this node hoping it to be a better route to destination. Some can forward packets for those destinations which are out of the reach of the attacker node. A single high power transmitter can convince that all the nodes are his neighbor. The attacker node need not generate a legitimate traffic; it can just perform a selective replay attack as its power overwhelms other transceivers [137].
- **Bogus Registration Attack:** A Bogus registration attack is an active attack in which an attacker disguises itself as another node either by sending stolen beacon or generating such false **beacons** to register himself with a node as a neighbor. Once registered, it can snoop transmitted packets or may disrupt the network altogether. But this type of attack is difficult to achieve as the attacker needs to intimately know the masquerading nodes identity and network topology. 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. To perform man in middle attack, the attacker first needs to be part of that route. It can do that by either temporarily disrupting the route by deregistering a node by sending malicious disassociation beacon **captured** previously or registering itself in next route timeout event. One way of protecting packets flowing through MANET from prying eyes is encrypting each packet. Though key distribution becomes a security issue [139].

- **Rushing Attack:** In AODV or related protocol, each node before transmitting its data, first establishes a valid route to destination. Sender node broadcasts a RREQ (route request) message in neighborhood and valid routes replies with RREP (route reply) with proper route information. Some of the protocols use duplicate suppression mechanism to limit the route request and reply chatter in the network. Rushing attack exploits this duplicate suppression mechanism. Rushing attacker quickly forwards with a malicious RREP on behalf of some other node skipping any proper processing [134]. Due to duplicate suppression, actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker node does send packets to proper node after its own filtering is done, so from outside the network behaves normally as if nothing happened. But it might increase the delay in packet delivering to destination node.
- **Cache Poisoning Attack**: Generally in AODV, each node keeps few of its most recent transmission routes until timeout occurs for each entry. So each route lingers for some time in node’s memory. 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. An attacker node can advertise a zero metric to all of its destinations [133]. Such route will not be overwritten unless timeout occurs. It can even advertise itself as a route to a distant node which is out of its reach. Once it becomes a part of the route, the attacker node can perform its malicious activity. Effect of Cache poisoning can be limited by either adding boundary leashes or by token authentication. Also each node can maintain its friend-foe list based on historical statistics of neighboring nodes performance [133].
- **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. This attack can effectively be done on those distributed protocols that establish a good and bad node list based on review of participating nodes in MANET [140]. Few of the protocols tries to make them more secure by using majority voting principle, but still if sufficient no. of attacker nodes become part of the MANET it can bypass that security also. Another generic method of this attack will

be, sending invalid RREP messages with advertising an unnecessarily high cost to certain nodes.

- **Sybil Attack**: Sybil attack manifests itself by faking multiple identities by pretending to be consisting of multiple nodes in the network. So one single node can assume the role of multiple nodes and can monitor or hamper multiple nodes at a time. If Sybil attack is performed over a blackmailing attack, then level of disruption can be quite high. Success in Sybil attack depends on how the identities are generated in the system.

5.6 Summary

This chapter presents an analysis of threats and security issues in mobile computing. These issues classified into categories like mobility, security, and control traffic attack and security countermeasures. In this part, we mainly discusses about the types of attack in the mobile ad hoc networks. The attacks in MANET can be briefly classified into two categories: external attacks and internal attacks, latter of which are far more dangerous to the mobile ad hoc network. Then there is the brief introduction about the attack in the mobile ad hoc network, like denial-of-service (DoS) attacks, impersonation attacks, eavesdropping attacks and attacks against routing. We analyze the main security criteria for the mobile ad hoc networks, which should be regarded as a guideline for us to find the solutions to the security issues in the mobile ad hoc networks. According to these attacks t, we survey several security schemes that can partly solve the security problems in the mobile ad hoc networks. During the last decade the decrease in the size of computing machinery, coupled with the increase in their computing power has led to the development of the concept of mobile computing. Mobile Computing is a generic term is evolved in modern usage such that it requires that the mobile computing activity be connected wirelessly to and through the internet or to and through a private network.