Wireless Sensor Network, **2010, 2, 419-440**
doi:10.4236/wsn.2010.26054 Published Online June 2010 (http://www.SciRP.org/journal/wsn)

Classification and Review of Security Schemes in Mobile Computing

Sathish Alampalayam Kumar
Department of Computer Science and Information Technology PSG Institute of Advanced Studies, Coimbatore, India
E-mail: *sathish.ap@gmail.com*
Received October 13, 2009; *revised November* 20, 2009; *accepted December* 25, 2009

Abstract

In this paper, we present the classification and review of security schemes in mobile computing system. We classify these schemes based on types the infrastructure used in the mobile computing system-Mobile Ad Hoc Networks (MANET) and Mobile Agent model. Mobile Ad Hoc Networks are pervasive, ubiquitous and without any centralized authority. These unique characteristics, combined with ever-increasing security threats, demand solutions in securing ad hoc networks prior to their deployment in commercial and military applications. This paper reviews the prevailing mobile ad hoc network security threats, the existing solution schemes, their limitations and open research issues. We also explain the Intrusion detection and response technique as an alternate method to protect the MANET based mobile computing systems and their approaches. A literature review of important existing Intrusion Detection approaches and Intrusion Response Approaches for MANET is also presented. This paper also presents the limitations of existing Intrusion Detection and Response Approaches for MANET and open research issues in providing MANET security. With respect to Mobile Agent based mobile computing system, we have presented the classification of various types of security attacks in Mobile Agent based model and presented the security solutions for those type of attacks proposed by the various schemes and the open research issues in providing security for Mobile Agent based mobile computing system. Such classification enhances the understanding of the proposed security schemes in the mobile computing system, assists in the development and enhancement of schemes in the future and helps in choosing an appropriate scheme while implementing a mobile computing system.

Keywords: Wireless Sensor Networks, Beta Trust Model, Trust Routing Protocol, Network Security, Trust Evaluation

1. Introduction

Although the wonderful invention of Internet offers access to information sources worldwide, we do not expect to benefit from that access until we arrive at some familiar point-whether home, office, or school. However, the increasing variety of wireless devices offering IP connectivity, such as PDA's, handhelds, and digital cellular phones, is beginning to change our perceptions of the Internet.

Mobile computing and networking should not be confused with the portable computing and networking we have today. In mobile networking, computing activities are not disrupted when the user changes the computer's point of attachment to the Internet. Instead, all the needed reconnections occur automatically and none interactively. Mobile Internet implies changing the point of attachment as the host (mobile station) roams between cells.

Truly, mobile computing offers many advantages. Confident access to the Internet anytime, anywhere will help free us from the ties that bind us to our desktops. Having the Internet available to us as we move will give us the tools to build new computing environments wherever we go. This is especially convenient in a wireless LAN office environment, where the boundaries between attachment points are not sharp and are often invisible.

However, there are still some technical obstacles that must be overcome before mobile networking can become widespread. The most fundamental is the security management, which is almost an afterthought until the recent years. Providing security services in the mobile computing environment is challenging because it is

more vulnerable for intrusion and eavesdropping. Authentication mechanisms are designed to protect a system from unauthorized access to its resources and data. However, at present, completely preventing breaches of security seems unrealistic, especially in mobile computing systems [1,2]. A Personal Area Network (PAN) level firewall as envisioned for the next generation wireless networks can protect only if the users are at home and not when the users are roaming [3]. Even if such a firewall is provided, the communication would get fragmented by these 'check points' on the network, as each firewall needs maintenance of activities like log control, software update etc., creating unnecessary overhead. Thus existing technologies like firewalls and Virtual Private Network (VPN) sandboxes cannot be directly applied to the wireless mobile world. Even if the firewall concept were achieved by creating a private extranet (VPN) which extends the firewall protected domain to wherever the user moves, this would still lead to inefficient routing. Security is a fundamental concern for mobile network based system. Harrison *et al.* [4] identify security as a "severe concern" and regard it as the primary obstacle to adopting mobile systems.

2. Mobile Computing Systems Security

2.1. Mobile Computing Systems Security Classification

The security approaches for mobile computing systems can be classified as shown in the following **Figure 1**.

2.2. MANET and Security Attacks in MANET

2.2.1. MANET Background

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any centralized authority. In a MANET, each wireless mobile node operates not only as an end-system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. MANET does not require any fixed infrastructure such as base stations; therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. For instance, first responders at a disaster site or soldiers in a battlefield must provide their own communications. A MANET is a possible solution for this need to quickly establish communications in a mobile, transient and infrastructure-less environment. This is one of many applications where MANET's can be used. Mobile ad-hoc networks are the future of wireless networks. Nodes in these networks will generate both user and application traffic and perform various network functions.

In the last decade, wired and wireless computer network revolution has changed the computing scenario. The possibilities and opportunities due to this revolution are limitless; unfortunately, so too are the risks and chances of attacks due to intrusion by malicious nodes [4]. Intrusion is defined as an attack or a deliberate unauthorized attempt

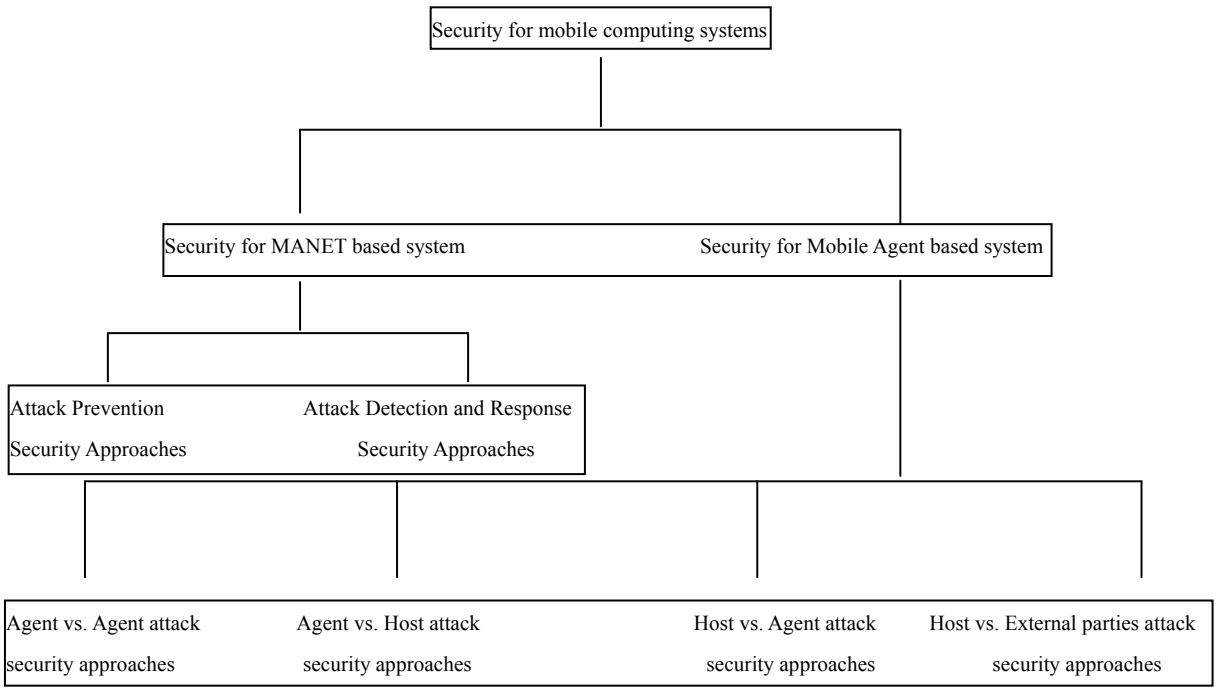

Figure 1. Taxonomy of security for mobile computing systems.

to access information, manipulate information, or render a system unreliable or unusable [5]. According to [6], threat can be defined as "the potential possibility of a deliberate unauthorized attempt to 1) access information, 2) manipulate information and 3) render a system unreliable or unusable. By security we mean protecting nodes from damages due to either voluntary or accidental attacks [7]. This protection is provided by predicting an attack by monitoring a set of metrics measured from the ad hoc network, and then responding and modifying the security of the network based on the vulnerability level at a given time.

Security in mobile ad hoc network is essential even for basic network functions like routing which are carried out by the nodes themselves rather than specialized routers. The intruder in the ad hoc network can come from anywhere, along any direction, and target any communication channel in the network. Compare this with a wired network where the intruder gains physical access to the wired link or can pass through security holes at firewalls and routers. Since the infrastructure-free mobile ad hoc network does not have a clear line of defense, every node must be prepared for the adversary. The centralized or hierarchical network security solution for the existing wired and infrastructure-based cellular wireless networks will not work properly for Mobile Ad Hoc Networks [8]. Securing the ad hoc networks, like any other field of computers, is based on the principle of confidentiality and integrity. These principles exist in every field, but the presence of malicious nodes, selfish nodes, covert channels and eavesdroppers in the mobile ad hoc network makes this an extremely important and challenging problem [9]. In the past several years, there has been a surge of network security research in the field of information assurance that has focused on protecting the network using techniques such as authentication and encryption. These techniques are applicable in the wired and infrastructure-based cellular network. In the case of infrastructure-free Mobile Ad Hoc Networks these techniques are not applicable [8]. In the infrastructure-free networks, the nodes themselves perform basic network functions like routing and packet forwarding. Therefore, mobile ad hoc network security is a pressing issue, which needs immediate research attention [10-13]. Providing security services in the mobile computing environment is challenging because it is more vulnerable for intrusion and eavesdropping. The challenge of mobile ad hoc network security has attracted several researchers with the aim of securing mobile ad hoc computer networks.

2.2.2. Security Attacks in MANET

A MANET can be subjected to active attacks and passive attacks. Active attacks refer to the direct attacks by a hostile entity during execution or transmission phase. Some of the major types of active attacks are routing attacks and active DoS attacks. Passive attacks refer to the indirect attacks by an entity in the network during collaboration. Some of the major types of passive attacks include actions like selfishness, eavesdropping, traffic analysis and passive DoS attacks.

1) Active Attack in MANET:

a) Routing Attacks:

Routing attack is a significant problem because nodes within the ad hoc network themselves performs routing functions and the security concepts are not incorporated in most of the routing protocols. Also, routing tables form the basis of network operations and any corruption to the routing table may lead to significant adverse consequences.

Designing a secure ad hoc network routing protocol is a challenge for the following reasons: Firstly, routing relies on the trustworthiness of all the nodes involved and it is difficult to distinguish selfish nodes from normal nodes. Secondly, rapid mobility of nodes that perform the role of routing and network topology makes the design of a secure routing protocol more difficult. Active routing attacks differ in their behavior depending on the nature of the routing protocol. In the case of link-state routing protocol, a router sends information about its neighbors. Hence a malicious router can send incorrect updates about its neighbors, or remain silent if the link state of the neighbor has actually changed. However, in the case of distance-vector protocols, routers can send wrong and potentially dangerous updates regarding any nodes in the network, since the nodes do not have the full network topology. These attacks in case of both link-state and distance-vector protocols are very difficult to prevent if the routers exhibit Byzantine faults [14].

In the MANET shown in **Figure 2**, let us assume that packets are supposed to traverse from source node A to destination node C. However, the intruder updates the routing table so that the packets traverse from B to D instead of C, and hence the packets from A never reach C. This also causes congestion on domains served by nodes A, D and E, due to the bombardment of packets whose actual destination was C. Thus the attack can lead to network performance degradation.

Some of the important and common methods of routing attacks are:

i) Router Protocol Poisoning: In this attack an intruder causes the disruption by poisoning the routing protocol. Securing these attacks is important because the routing protocol forms the basis of network operations, and any corruption of the protocol may lead to significant consequences. These attacks on the Mobile Ad Hoc Networks can lead to looping, congestion, sub optimal routing and partitioning [15]. Thus, they can ultimately affect the performance of an ad hoc network.

ii) Injecting incorrect information in the routing table: In this type of routing attack, malicious nodes or an intruder would inject incorrect routing information, which

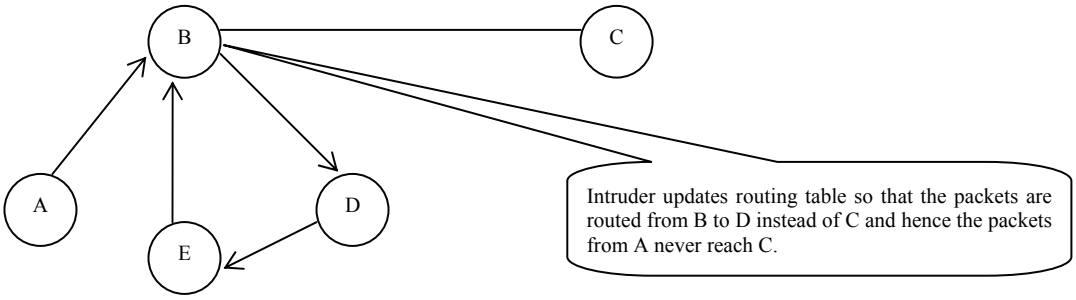

Figure 2. Routing loop attack.

in turn would poison the routing tables. These attacks would result in the artificial partitioning of the network, and the hosts residing in one partition would not be able to communicate with hosts residing in the other partition.

iii) Routing Loop Attacks: In this attack, intruder or malicious nodes update the routing table to create a loop, so that packets can traverse in the network without reaching the destination, thereby conserving energy and bandwidth.

b) Active DoS Attacks:

These attacks can be defined as the direct denial of service attacks on a node by another hostile node through packet flooding, packet modification, deletion or forging of packets or routing table. Following are some of the common types of active DoS attacks by selfish nodes or adversaries: replay of expired routing information, bogus nodes create traffic by bombarding the neighboring nodes with the packets, radio jamming, flooding centralized resource with the requests, ability to change routing protocol to operate as the user wants, Byzantine failure, sleep deprivation torture (Battery Exhaustion) and injecting incorrect routing information.

Active DoS attack is depicted in **Figure 3**, where node B is a host node and C is the intruder. The intruder node C creates a huge traffic resulting in the exhaustion of the node B's resources. This results in the inability of node B to serve genuine nodes A, D, E and F fairly. Thus, DoS attacks on the mobile ad hoc networks can lead to network performance degradation.

2) Passive Attack in MANET

a) Selfish Attacks:

Passive attacks could be caused by selfishness, eavesdropping and traffic analysis. In this section we explain selfishness attacks to give an idea of passive attacks. In the selfishness attacks, the selfish node abuses constrained resources, such as battery power, for its own benefit [16]. They do not intend to directly damage other nodes in the network. Attackers may also get hold of a node and modify its behavior to make it malicious, so the node would perform selfish attacks in need of resources. These attacks have limited effectiveness compared to the routing-table "poisoning" and DoS attacks [17]. This is because, the attacks are limited to a part of the network rather than the whole network as in the case of routing protocol attacks.

Some of the common types of selfish node attacks in mobile ad hoc network are packet mistreatment and energy consumption attacks. In this kind of attack, a node in mobile ad hoc network does not perform the expected network functions, like packet forwarding or routing, and later claims that the transaction or communication never took place [17]. It could be deliberate or accidental, due to false repudiation of a transaction or due to scarce resources in the mobile ad hoc networks.

As shown in **Figure 4**, the packets are supposed to traverse from source node A to destination node C. However, selfish node B discards the packets from A and hence the packets from A never reach C. This results in 'black hole' attacks. This in turn may result in deadlock issues which result in performance degradation. Some of the important and common methods of selfish attacks are:

i) Packet mistreatment or interception: In this kind of attack, a selfish node does not perform the function of packet forwarding. As mentioned earlier, interruption

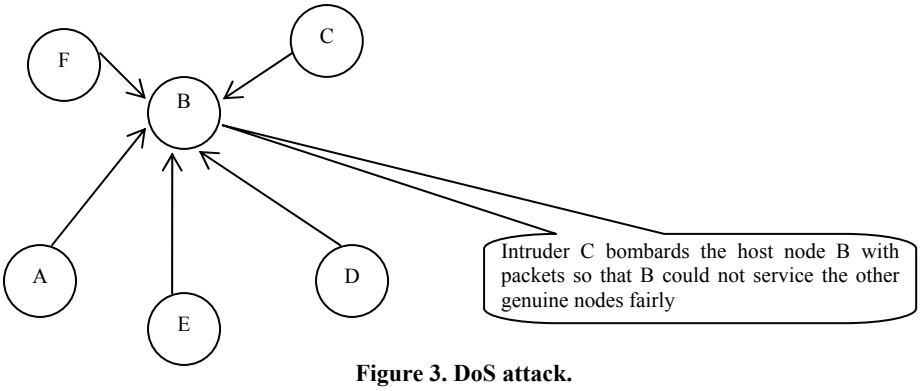

Figure 3. DoS attack.

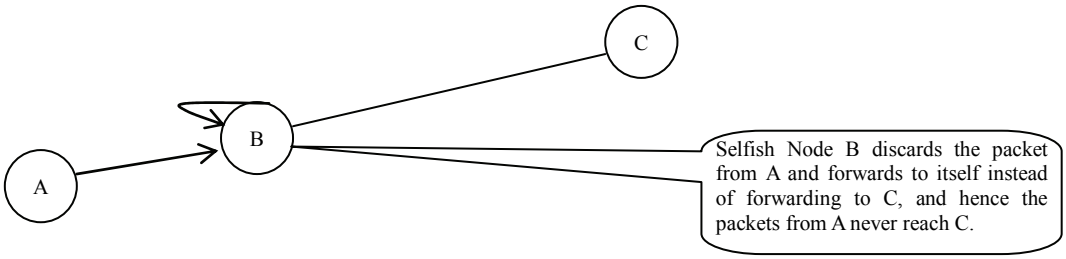

Figure 4. Packet mistreatment attack.

of packets may reduce the overall throughput of the network. In a specialized form of packet discarding, selfish nodes do not forward the packets to host destination, but to itself. This result in black hole and DoS attacks.

ii) Energy consumption: In this kind of attacks, nodes try to save significant battery power by not performing networking functions such as routing. This is due to the fact that in ad hoc network most of the energy is consumed by routing of packets. For instance, experiments have shown that if the average hop from source to destination is 5, approximately 80% of the available energy is spent in sending packets from source to destination by packet forwarding [17].

2.3. Mobile Agent Model and Security Threats in Mobile Agent Model

2.3.1. Mobile Agent Model Background

A distributed mobile agent system model for a wireless internet host environment involves the following parties, mobile agents and fixed base stations as shown in **Figure 5**. Some of the wireless models [18] applied for special applications like mobile military networks assumes mobile base stations. However, in this discussion we assume the base station is fixed.

Mobile Agent:

The Mobile Agent (MA) is a software component [19] like

- A thread as in Telescript, that can migrate among different nodes carrying its execution state (*i.e.*, program counter, call stack etc.) Here the run-time image of the component is transferred as a whole, including its execution state.

The task to rebuild the execution state is carried out by the run-time support of the Mobile Code System.

- Or just a code fragment as in TACOMA [20] associated with initialization data that can be shipped to a remote host. They don't have the ability to migrate once they have started their execution. These systems claim to be able to move the state of a component along with its code. This assertion is justified by the availability of mechanisms that allow the programmer to pack some portion of the data space of an executing component before the component's code is sent to a remote destination.

It is the programmer's task to rebuild the execution state of a component after its migration, using the data transferred with the code.

Thus a mobile agent (with respect to design paradigm) contains.

- Code component-Executing Unit (EU) (Sequential flows of computation), which encapsulate the know-how to perform a particular computation.
- Resource component-(entities that can be shared among multiple EUs such as a file in a file system, an object shared by threads in a multi-threaded object-oriented language, or an operating system variable) that represents data or devices used during the computation.

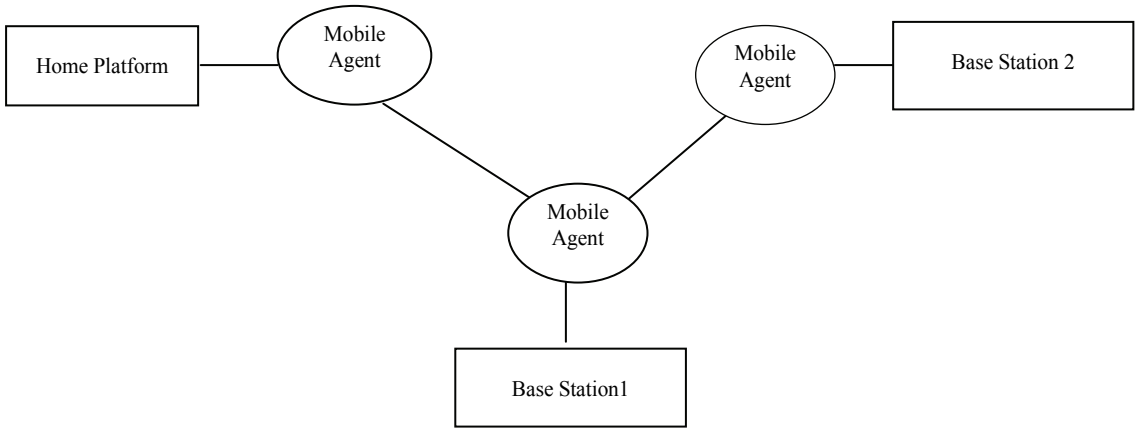

Figure 5. Mobile agent model in mobile computing.

- Computational components that are active executors capable to carry out a computation.

Mobility allows an agent to move or hop among base station. The base station provides a computational environment in which an agent operates. The purpose of Mobile Agent in terms of Artificial Intelligence (AI) research paradigm is a software component that is able to achieve a goal by performing actions and reacting to events in a dynamic environment. The behavior of this component is determined by the knowledge of the relationships among events, actions and goals. However, in terms of Distributed Systems research paradigm, the purpose of the mobile agent is to allow the migration of the whole computational component to a remote site, along the code it needs, some resources required to perform the task along with its execution state of an EU to a different CE (Computation Environment or Host).

Mobile Agents are increasingly becoming popular with the ubiquitous and widespread deployment of wireless and internet technologies. With the help of mobile agents it is possible to create distributed applications where the programs can autonomously traverse from one computer to another and get executed. They are more powerful than an ordinary applets [21] due to the AI component, they decide themselves where and when to traverse and execute. They are prominently applied in mobile computing systems. Connection management for mobile computing requires continuous reconfiguration of the data links. If connectivity fails, the mobile computing system requires applications to handle extended off-line periods. "Mobile software agents are very useful in this context, since they could encapsulate long-lasting transactions. They could carry a request to server, cause its execution and bring back the result as soon as the connectivity is reestablished [21]." Due its ability to preprocess the results, it makes use of the slow communication link between the mobile device and the network.

2.3.2. Security Threats in Mobile Agent Based Model: In the mobile agent-host model the security attacks or threats could be classified into four categories:

- mobile agent attacked by another mobile agent
- mobile agent attacking by the host
- host attacked by a mobile agent
- host attacked by external unauthorized party like an agent or host

For the ease of understanding, any agent or host attack could be further classified into active or passive attacks. Before further classification, it is essential to define active and passive attacks.

Active attacks can be defined as the direct attacks on an entity by another hostile entity during its execution or transmission like code/message modification, deletion or forging.

Passive attacks can be defined as the indirect attacks on an entity by another hostile entity during its execution or transmission like eavesdropping and traffic analysis.

Mobile Agent Attacked by another Agent:

Different types of attacks by a MA against another MA can be classified as shown in the following taxonomy.

1) Active Attacks:

Denial of service: In these attacks agent could spam other agents causing resource constraints by repeatedly sending messages to another agent, may place undue burden on the message handling routines of the recipient. Agents can also intentionally distribute false or useless information to prevent other agents from completing their tasks correctly or in a timely manner.

Unauthorized Access: In these attacks agent would invoke other agent's public methods by accessing or modifying agent's code or data, which could change the behavior of agent from trusted to harmful one.

2) Passive Attacks:

Repudiation: Agent participating in a transaction or communication later claims that the transaction or communication never took place—could be deliberate or accidental, due to false repudiation of a transaction or due to imperfect business transactions within an organization.

Masquerade: In this category an agent posing as host could deceive other agents and it harms both the agent that is being deceived and the agent whose identity has been assumed, especially in agent societies where reputation is valued and used as a means to establish trust.

Mobile agent attacked by the host:

Different types of attacks by a host against MA can be classified as shown in the following taxonomy.

3) Active Attacks

Denial of Service: In these attacks host would ignore agent service request by not executing the agent or turning away the request. This would introduce unacceptable delays for critical tasks like handoff in the mobile computing world. Agents on other platforms waiting for the results from a non-responsive agent in the malicious host platform could cause deadlock or livelock problems.

Alteration: Since agent visits various base stations or hosts during its life time, it could be altered by any of the hosts an agent passes through its lifetime. Thus a mobile agent is exposed to a new risk each time it is in transit and each time it is instantiated on a new platform.

Copy and Replay: In these attacks an agent or its message could be copied and replayed several times by the host.

4) Passive Attacks

Masquerade: In these attacks host deceives a mobile agent as to its true destination and corresponding security domain. Thus it harms both the agent and the host or platform it assumes. This is a more serious problem than an agent masquerading as other agent.

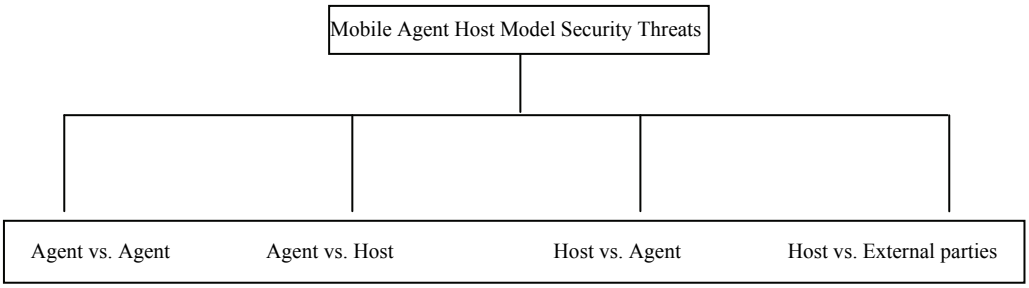

Figure 6. Taxonomy of mobile agent model security threats.

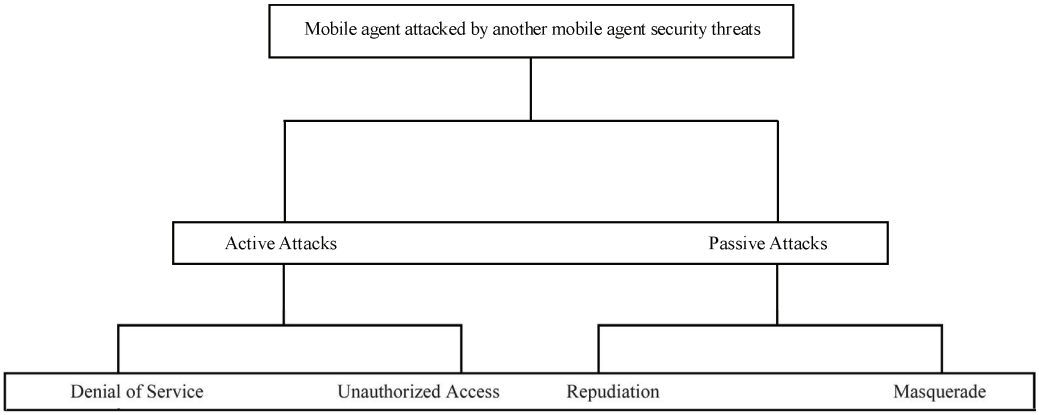

Figure 7. Taxonomy of mobile agent attacked by another agent attacks.

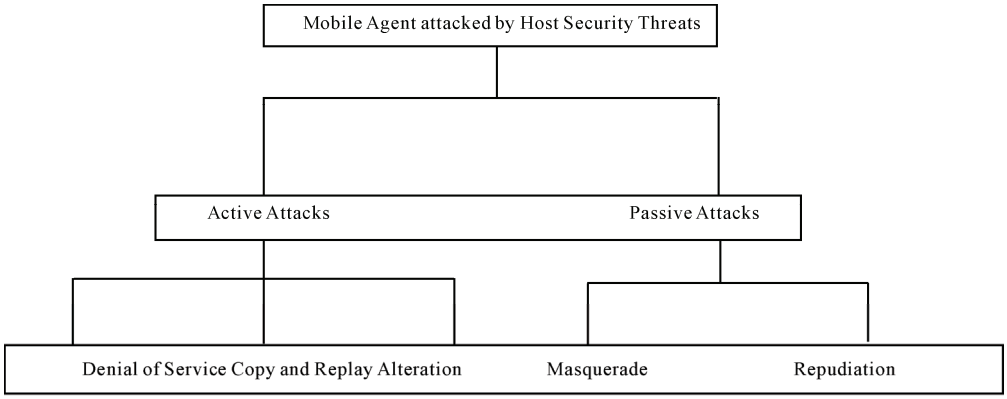

Figure 8. Taxonomy of mobile agent attacked by host security threats.

Repudiation: Host participating in a transaction or communication with an agent later claims that the transaction or communication never took place-could be deliberate or accidental, due to false repudiation of a transaction or due to imperfect business transactions within an organization.

Host attacked by mobile agents

Different types of attacks by a MA against host can be classified as shown in the following taxonomy.

5) Active Attacks:

Denial of Service: In these attacks agent consume excess amount of host resources so that the host can not service other agents properly.

Unauthorized access: In these attacks, agent without proper authorization could harm the host.

6) Passive Attacks

Masquerading: In these attacks agent may pose as an authorized agent to gain access to services and resources to which it is not entitled, to shift the blame for any actions for which it does not want to be held accountable and to damage the trust the legitimate agent has established in an agent community and its associated reputation.

Host attacked by other unauthorized external parties including host and agents:

Different types of attacks by an external party like an

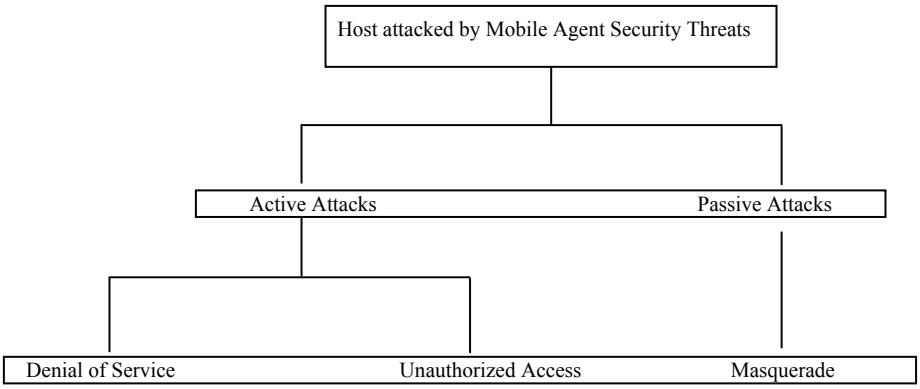

Figure 9. Taxonomy of host attacked by mobile agent security threats.

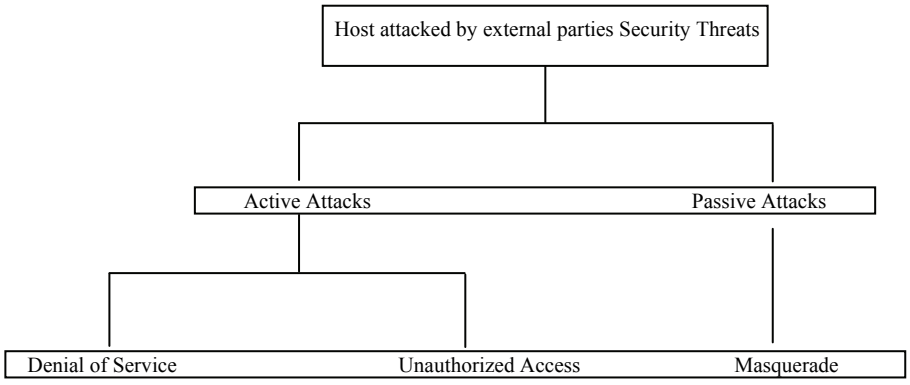

Figure 10. Taxonomy of host attacked by external parties security threats.

external MA or an external host against the host can be classified as shown in the following taxonomy.

7) Active Attacks

Unauthorized Access: In these attacks, remote users, processes, and agents may request resources from the host, for which they are not authorized.

Denial of service: In these attacks, the agent services offered by the host or base station can be disrupted by common denial of service attacks.

8) Passive Attacks

Masquerade: An agent on a remote base station can masquerade as another agent and request services and resources for which it is not authorized. They may act in conjunction with its platform (base station) to deceive the host.

3. MANET Security Approaches

3.1. MANET Attack Prevention Approaches

In this section, we classify the MANET security work into two broad categories based on the type of attack: active attack or passive attack.

3.1.1. Review of MANET Attack Prevention Security Schemes for Active attacks

In ad hoc networks, a mobile node or host may depend on other node(s) to route or forward a packet to its destination. The security of these nodes could be compromised by an external attacker or due to the selfish nature of other nodes. This would create a severe threat of Denial of Service (DoS) and routing attacks where malicious nodes combine and deny the services to legitimate nodes. Unlike nodes in a wired network, the nodes of MANET may have less processing power as well as battery life and consequently would try to conserve resources. In this scenario, the usual authentication and encryption methods would not apply to a MANET the same way they would in a wired network [22]. However, both authentication and encryption are even more important in a MANET [23,24]. Steiner *et al.* have developed a Group key Diffie-Hellman (GDH) model that provides a flexible solution to group key management. Yi *et al.* [25] have developed the MOCA (MObile Certification Authority) protocol that helps manage heterogeneous mobile nodes as part of a MANET. MOCA uses Public Key Infrastructure (PKI) technology.

The impact of authentication attacks is quite widespread and it includes unauthorized access, denial of service, masquerading, information leakage, and domain hijacking. Capkun *et al.* [26] have developed some solutions using a concept that they introduce, called Maximum Degree Algorithm (MDA), for preventing denial of

service due to poor key management.

Routing is an important aspect of moving packets around in a network. It is a challenging problem because nodes within the ad hoc network themselves performs routing function and the security concepts were not incorporated into the routing protocols when they were designed. It is important because the routing table forms the basis of the network operations and any corruption of routing table may lead to significant consequences. Routing attacks in mobile ad hoc network are more challenging since routing relies on the trustworthiness of all the nodes involved and it is difficult to distinguish selfish nodes from normal nodes. Basically there are two methods used for routing: AODV (Ad hoc On-demand Distance Vector) routing and DSDV (Destination Sequenced Distance Vector) routing. These two methods can be classified as reactive and proactive respectively since AODV method discovers a route only when needed whereas the DSDV method maintains a dynamic routing table at all times.

A reactive routing method was proposed by Yang *et al.* [27]. In this method, a unified network layer prevention method known as Self Organized Security (SOS) scheme that uses AODV routing is used. This scheme takes a self-organized approach by exploiting full localized design, without assuming any apriori trust or secret association between nodes. In this model, each node has a token in order to participate in the network operations, and its local neighbors collaboratively monitor it to detect any misbehavior in routing or packet forwarding services. Upon expiration of the token, each node renews its token via its multiple neighbors. The period of the validity of a node's token is dependent on how long it has stayed and behaved well in the network. A well-behaving node accumulates its credit and renews its token less frequently as time evolves. In essence, this security solution exploits collaboration among local nodes to protect the network layer without completely trusting any individual node.

Another reactive scheme, called Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) was proposed by Ramanujam *et al.* to detect and eliminate DoS [28]. This model presents a new approach for building intrusion resistant ad hoc networks in the wake of DoS attacks using wireless router extensions. This approach relies on extending the capabilities of existing ad hoc routing algorithms to handle intruders without modifying the existing routing algorithms. This scheme proposes a new network layer mechanism for detecting and recovering from intruder induced malicious faults that work in concert with existing ad hoc routing algorithms and augment their capabilities.

Hu *et al.* [29] have developed a DSDV-based secure routing method called SEAD (Secure Efficient Ad hoc Distance vector). This method uses efficient one-way hash functions and does not use symmetric cryptographic operations in the protocol in order to support the nodes of limited CPU processing capability and to guard against Denial-of-Service (DoS) attacks. The primary reason for this is due to the fact that the nodes in an ad hoc network are unable to verify asymmetric signatures quickly enough for routing protocols to decide on the routing path.

Routing attacks differ in their execution depending on the nature of the routing protocol. In the case of link state routing protocol such as AODV, a router sends information about its neighbors. Hence, a malicious router can send incorrect updates about its neighbors or remain silent if the link state of the neighbor has actually changed. However, in case of distance vector protocols such as DSDV, routers can send wrong and potentially dangerous updates regarding any nodes in the network since the nodes do not have the full network topology. Awerbuch *et al.* [30] studies the behavior of routers in the presence of Byzantine faults. They use an On-demand Secure Routing Protocol (OSRP) that defines a reliability metric based on past records and use it to select the secure path. Reliability metric is represented by a list of link weights where high weights correspond to low reliability. Each node in the network maintains its own list, referred to as a weight list, and dynamically updates that list when it detects faults. Faulty links are identified using a secure adaptive probing technique that is embedded in the normal packet stream. These links are avoided using a secure route discovery protocol that incorporates the reliability metric. This protocol achieves these functionality by three successive phases: Route discovery with fault avoidance phase whose input is source node's weight list and output is the full least weight path from the source node to the destination node, Byzantine fault detection phase whose input is the full weight path and output is a faulty link and link weight management phase which takes a faulty link as an input and whose output is the weight list which in turn is used by the route discovery phase to avoid faulty paths. This is a very efficient approach to detect secure routes. In a related paper, Awerbuch [30] discusses a method for secure ad hoc routing.

Zhou *et al.* [31] have an alternative solution for the problems with AODV and DSDV routing methods. They have developed a hybrid approach using both AODV and DSDV methods. This method, known as the Key Management Service (KMS), defends routing from denial of service attacks in ad hoc networks by taking advantage of multiple routes between nodes. Due to the dynamic changes in topology, the routing protocols of ad hoc network need to handle outdated routing information, which is similar to that of the compromised routing attacks. The principle here is that as long as there are enough proper nodes, the routing protocol would be able to find the routes working around the compromised nodes. Thus, if the nodes can find multiple routes, nodes can switch to an alternate route when a fault has been

detected in the primary route. This method also uses replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of the security framework.

In addition to the methods discussed above, there are some additional methods proposed in the literature to handle various forms of attacks. For example, the Secure Routing Protocol (SRP) by Papadimitratos *et al.* [31] guarantees correct route discovery, so that fabricated, compromised, or replayed route replies are rejected or never reach the route requester. SRP assumes a security association between the end-points of a path only and so intermediate nodes do not have to be trusted for the route discovery. This is achieved by requiring that the request along with a unique random query identifier reach the destination, where a route reply is constructed and a message authentication code is computed over the path and returned to the source. The authors prove the correctness of the protocol analytically.

Another preventive solution for DoS attacks in ad hoc wireless networks is proposed by Luo *et al.* [32]. In this solution they distribute the functionality of authentication servers, thus enabling each node in the network to collaboratively self-secure themselves. This is achieved by using the certificate-based approach. This scheme supports ubiquitous security for mobile nodes, scales to network size, and is robust against adversary break-ins. In this method centralized management is minimized and the nodes in the network collaboratively self-secure themselves. This scheme proposes a suite of fully distributed and localized protocols that facilitate practical deployment. It also features communication efficiency to conserve the wireless channel bandwidth and independency from both the underlying transport layer protocols and the network layer routing protocols.

The ARIADNE method developed in Europe is another important secure on-demand routing protocol. Developed by Hu *et al.* [33], ARIADNE (Alliance of Remote Instructional Authoring and Distributed Networks for Europe) prevents attackers from tampering with uncompromised routes consisting of uncompromised nodes. It is based on Dynamic Source Routing (DSR) approach and relies on symmetric cryptography only. ARIADNE protocol is designed in three stages: The first stage presents a mechanism that enables the target to verify the authenticity of the Route Request. Second stage presents a key management protocol that relies on synchronized clocks, digital signatures, and standard MAC (Message Authentication Code) for authenticating data in Route Requests and Route Reply. The final stage presents an efficient per-hop hashing technique to verify that no node is missing from the node list in the Request. Hu *et al.* present simulations that show that the performance is close to DSR without optimizations.

Marti *et al.* [34] have taken another variation on the DSR method. This method shows increased throughput in Mobile Ad Hoc Networks by complementing DSR with a watchdog for detection of denied packet forwarding and a pathrater for trust management and routing policy rating that every path uses, thus enabling nodes to avoid malicious nodes in their routes as a detective and reactive protection measure. This reaction does not punish malicious nodes that do not cooperate, but actually relieves them of the burden of forwarding for others while having their messages forwarded, and it allows nodes to use better paths and thus increase their throughput.

The traditional Secure Routing Protocol (SRP) is well suited for a wired network. In developing a similar protocol for MANETs, Yi *et al.* [35] propose a new routing technique called Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols. Ad hoc routing protocols enable nodes in ad hoc networks communicate with their neighbors through Route REQuest (RREQ) packets and Route REPly (RREP) packets. In SAR, the security metrics are embedded into RREQ packets. Intermediate nodes receive these packets with particular security level and process these packets or forward the packets depending on the security level of the intermediate node. If it cannot provide required security level, RREQ packets are dropped. Otherwise RREP packets are sent back to the source from destination or intermediate nodes. This approach, though resource intensive is a useful alternative for preventing attacks.

So far we have looked at research that addresses authentication, denial of service, selfish node and routing protocol attacks in a MANET. One of the main requirements in a MANET is for each node to let other nodes know of their presence and readiness to participate in the MANET. In a wireless local area network, an Access Point (AP) is used to let the mobile nodes communicate with other nodes on the network. In a MANET, there is no Access Point and so each node must know the other nodes that participate in the MANET. One way to let the other nodes know of their presence, a mobile node sends out beacon signals. Binkley *et al.* [36] propose an authenticated routing protocol to address link security issues in this regard. This proposal also reduces the DoS threats like replay attacks caused by an Address Resolution Protocol (ARP) or ad hoc routing protocol spoof, which would destroy a link-layer route to a host. This protocol transmits beacons similar to that of mobile IP agents. When a host node or agent receives the transmitted beacons, they authenticate them and if it is authentic, they add the MAC-to-IP address binding contained in the beacon into their table of authentic bindings.

Another security scheme proposed by Kong *et al.* [37] and Luo *et al.* [32] supports ubiquitous security services

for mobile hosts through threshold secret sharing mechanism where they distribute certificate authority functions. These methods are based on RSA cryptography and provide distributed localized certificate services like certificate issuing, renewal and revocation. These methods employ localized certification schemes to enable ubiquitous services. This model uses RSA system key pair denoted by {Sk, Pk} where Sk is the system secret/private key and is used to sign certificates for all entities in the network. Pk is the system public key which verifies the certificate signed by Sk. In this scheme, Sk is shared among network entities but not visible or known by any component in the network, except at the boot strapping phase. Each entity Vi also maintains a secret share Pvi and a RSA personal public and private key pair {Ski, Pki} besides the system key pair. Thus, it uses the concept of threshold secret sharing and updating each entity's secret share periodically to further enhance robustness against break-ins. This scheme scales to network size and is robust against break-ins. In the threshold secret sharing mechanism each entity holds a secret share and multiple entities in a local neighborhood jointly provide complete services.

There are several open issues in the models that were reviewed. The important among them are explained as follows: The GDH method needs further study for the detection and resolution of inconsistent certificates, improvement of certificate graph models and enhancing the use of existing PKI infrastructure. The MOCA method uses a unicast approach that only exploits information in the local routing cache. One useful extension would be to devise a way for a node to browse neighboring nodes' routing tables. This would help in avoiding flooding. The CORE method considers only attacks from selfish nodes but not from active intruders. Hence one has to extend this method for intruder attacks as well. The solution for attack by selfish nodes presented in the nuglets method is focused just on packet forwarding attacks. Application-level issues like mutual provision of information services in an ad hoc network have to be addressed in order to better utilize the nuglet counter. The CONFIDANT method assumes that nodes are authenticated and that no node can pretend to be another in order to get rid of a bad reputation. This assumption could lead to misplaced trust in systems. The Guardian Angel method is not a comprehensive security scheme since it does not take into account the attacks like packet forwarding and denial of service or routing attacks, which are commonplace today.

3.1.2. Review of MANET Attack Prevention Security Schemes for Passive Attacks

We noted earlier some of the problems due to selfish nodes not performing their role properly in a MANET. Actions of a selfish node could lead to congestion, lower throughput and denial of service. Buttyan *et al.* [38] have shown by simulation that a selfish node does not participate actively in packet forwarding in order to conserve electrical energy. This study shows that typically every node spends 80% of the energy in forwarding packets. This work also introduces a special counter called nuglet counter that is used to keep track of selfish behavior of nodes. In trying to solve the selfish node problem, Michiardi *et al.* [39] have developed a model called CORE (Collaborative REputation). Under CORE's approach, every node monitors the behavior of the neighboring nodes for a particular requested function and collects data about the execution of that function. If the observed result of the function matches with the expected result, then the observation takes a positive value. This mechanism allows a node to detect if any of its neighbors are selfish nodes and gradually isolate them.

As seen above, the problem of selfish behavior by nodes in a MANET is something significant that needs to be addressed. In a MANET, many nodes try to conserve battery life and consequently resort to selfish behavior by dropping packets rather than forwarding them as they are supposed to do in a network. Buchegger *et al.* [40] study the vulnerabilities exposed by selfish nodes in a MANET. Buchegger *et al.* [40] introduce a new protocol called CONFIDANT (Cooperation of Nodes-Fairness In Distributed Ad hoc NETworks) to address this problem. Each node maintains reputation indexes about each of its neighbors based on their behavior and use these indexes to isolate misbehaving nodes. Avoine *et al.* [41] have developed a cryptography-based fair key exchange model called Guardian Angel. This model uses a probabilistic approach without involving a trusted third party in key exchange.

3.1.3. Limitations of Existing MANET Attack Prevention Schemes and Open Research Issues

1) Active Attack Security Approaches

The scheme GDH needs further exploration of mechanisms for the detection and resolution of inconsistent certificates, improvement of certificate graph models and making use of existing PKI infrastructure [26]. Scheme MDA does not provide authentication of the participants. In addition, more formal arguments need to be developed to support optimality claims [41]. Unicast approaches by the scheme MOCA only exploit information in the local routing cache. One potential extension is to let a node browse into neighboring nodes' routing tables. For example, a node may be short of one or two cached routes and that would lead to flooding. If the node has a way to peek into the neighbors' routing tables and find a couple of new cached routes, it can avoid flooding. Potential overhead for this approach would be the extra communication required between neighbors to exchange the information in routing tables. Whether the benefit would surpass the overhead is an interesting question to investigate [25]. All the unicast based approaches in the

MOCA protocol do not take into account the direction of Certification REQuests (CREQs). At a worst case, all the MOCAs picked by its unicast approach could reside on one side of the network from the requesting node. Then it is possible that all the CREQs are sent into one direction sharing the same next hop nodes, potentially causing unnecessary contention. This leads to a failure or at least delayed responses. One possible solution for such a scenario is to utilize the next hop field in the cached routing table entries. For example, by selecting a set of MOCAs with all the different next hops, one can expect to have a spatial load balancing effect in that each CREQ will go out in different directions [25].

The SEAD approach does not incorporate mechanisms to detect and expose nodes that advertise routes but do not forward packets [29]. In the Beacon scheme, scalability is an issue if there are large numbers of nodes compared to the available bandwidth. The proposed model assumes all nodes in a network share a symmetric key used only for beacon authentication. In addition to problems with scalability, every agent and mobile node at the site has to know the network authentication key. The symmetric keys might be replaced with public key cryptography. Public-key signature and verification of beacons and Mobile-IP registration messages is feasible, even though transmitting such a signature requires more link bandwidth. Every node can possess its own key and simply sign its beacons and registrations. The distribution of certificates such that mobile nodes and agents can verify a beacon is again a higher-level problem [36]. SOS model provides fully localized design, easy support of dynamic node membership, limited intrusion tolerance capacity and decreasing overhead over time. While these characteristics are appealing, this scheme also has limitations as this is achieved at the increased computational overhead (associated with asymmetric cryptography primitives) compared with other hash function based designs [27]. In the TRUST model when a new node enters the system, it assumes that the node already has an initial certificate. This results in the problem of registering users. Also when two ad hoc networks merge, this model does not provide mechanisms for nodes originated from different networks to certify and authenticate each other [32]. In SRP model, fair utilization of network resources is an issue. Possible ways to dismay nodes from broadcasting at the highest possible rate is still an issue [36]. Since the ARIADNE model does not possess the optimizations of DSR, the resulting protocol is less efficient than the highly optimized version of DSR that runs in a trusted environment [33]. An important aspect of OSRP scheme is that the algorithm can be used to detect a fault. However, it is difficult to design such a scheme that is resistant to a large number of adversaries. The method suggested in this paper uses a fixed threshold scheme. This scheme does not explore other methods, such as adaptive threshold or probabilistic schemes which may provide superior performance and extensibility. Also this scheme does not provide means of protecting routing against traditional denial of service attacks [30]. The Watchdog and Pathrater model assumes that there are no apriori trust relationships. Performance of model is bound to suffer when trusted node lists in ad hoc networks are also taken into account. Also, in this model, all the simulations are based on Constant Bit Rate (CBR) data with no reliability requirements. The analysis should be extended to explain how the routing extensions perform with TCP flows common to network applications [34].

2) Passive Attack Security Approaches

The scheme CORE considers only attacks from selfish nodes but not from active intruders. Hence the scheme needs to be extended and tested for intruder attacks as well. Also there is no definition of formal method to analytically prove robustness of CORE [39]. The solution for attack by selfish nodes, presented in Nuglets model is focused just on packet forwarding attacks. This model also does not address application-level issues like mutual provision of information services in an ad hoc network [38]. The CONFIDANT protocol assumes that nodes are authenticated and that no node can pretend to be another in order to get rid of a bad reputation [40]. The Guardian Angel model is not a comprehensive security scheme and does not take into account the attacks like packet forwarding and denial of service or routing attacks [41].

3.2. MANET Intrusion Detection and Response Security Approaches

3.2.1. Review of MANET Intrusion Detection Security Approaches

The following are some of the popular IDA models that we studied in our literature survey. Kachirski and Guha proposed an IDS model which is efficient and bandwidth-conscious [42]. It targets intrusion at multiple levels and fits the distributed nature of IDA for Mobile Networks. The method has clusters and the IDA on cluster head employs independent detection decision-making after gathering information from other nodes. It utilizes mobile agent for communication among various nodes. This model provides a framework to work with multiple types of audit data. It is expandable, meaning, if the IDA needs to work with new types of audit data, it can do so by just incorporating extra agents that can monitor the new type of audit data. Unfortunately, its performance is not verified by any implementation. Once its performance is proved to be on an acceptable level, this framework can serve as a generic and expandable architecture for commercial products, since having a possibility to add in more functionality is an important property for successful products. Because it utilizes the cluster heads, it is supposed to make the network more efficient by

limiting the resources usage for IDA purposes to only a few nodes. Such a framework can be applied in an environment where the security requirement is medium and efficiency requirement is high. Also, it may easily be expanded for multi-layered mobile networks.

IDS model for wireless Mobile Ad Hoc Networks proposed by Zhang and Lee implements local and collaborative decision making with anomaly detection [43]. In this approach, individual IDA agents can work by themselves and also collaborate in decision making. Each IDA agent runs on a node and monitors local activities. If a node detects local intrusion with strong evidence, then the node concludes that intrusion has happened and initiates an alarm response. However, if the evidence is not strong enough but needs investigation in a wider area in the network, then the IDA agent can start collaboration procedure which is a distributed consensus algorithm. This model provides a framework that fits the distributed nature of mobile networks as well. It also works with multiple types of audit data. If the IDA needs to work with new types of data, it can add in more data collection module in the IDA agent. It uses data mining as the local intrusion detection mechanism. The data mining is supposed to be superior in terms of both detection rate and false alarm rate. Also, because this IDA does not use mobile agents for communication, it can be designed for high security need, if it can find an effective way to protect from Byzantine nodes.

Huang and Lee have proposed a cluster-based scheme in which a cluster head is elected by a group of nodes in a neighborhood (citizen nodes) and the head node monitor the citizen nodes [44]. Once the cluster head is elected, the other nodes need to transmit the features they obtain locally to the cluster head. This IDA uses anomaly detection implemented with data mining as its detection technique [44]. This model improves the efficiency of mobile networks by limiting the resources usage for IDA purposes to only a few nodes. The implementation proves it can also achieve satisfactory level of detection rate. Such a framework can be applied in environments where the security requirement is medium but efficiency requirement is high. Also, it may easily be expanded for multi-layered mobile networks [45].

Patrick and Camp have designed architecture for ad hoc networks, where each node runs a local IDA [46]. Each node detects intrusion locally and uses external data to confirm the detection. The nodes use mobile agents to communicate and collaborate. This model provides a scalable architecture by using mobile agents. If the IDA needs more functionality, it can just incorporate more mobile agents with new tasks. It is supposed to reduce network traffic for intrusion detection purpose. However, since this architecture relies heavily on the use of mobile agents, it incurs computational complexity in creating and managing all the agents. This architecture needs an implementation to verify its performance.

Bo, Wu and Pooch have proposed an IDA model which uses collaboration mechanism with anomaly detection [47]. In this model, a network is divided into logical zones. Each zone has a gateway node and individual nodes. Individual nodes have an IDA agent to detect intrusion activities individually. Once an individual node detects intrusion, it generates an alert message. Gateway node aggregates and correlates the alerts generated by the nodes in its zone. An algorithm is used to aggregate the alerts based on the similarities in the attributes of the alert [45]. Only gateway nodes utilize the alert to initiate an alarm [46]. This method does not use mobile agents but has gateway nodes, which work just like a cluster head. This architecture can be applied in environment where the requirement for IDA performance and security is high.

Huang *et al.* have proposed a detection algorithm scheme that uses the statistics of packets, namely, the relation between different features such as the correlation between the number of packets dropped and the percentage of change in routing table [48]. This algorithm can be used as an intrusion detection engine in other IDA architectures. This model has low overhead, but was designed only for one routing protocol-OLSR and needs modification for other protocols.

Tseng *et al.* have proposed an IDS system where the normal behavior of critical objects in the network is constructed with the normal specification first. Then the actual behavior is compared to the normal specification [49]. It uses distributed network monitor to trace the request-reply flow in the routing protocol. The network monitor runs a specification based detection algorithm to make decisions [50,51]. This model is novel with no conventional local detection mechanism, but has low efficiency since packet is checked at each hop.

Neighborhood Watch, an IDS protocol proposed by Sowjanya and Shah has two neighboring nodes of which one node is used to ensure that the packets are not modified while traveling in the network [52]. This is done by comparing the information in each packet at each hop. It has two modes: passive mode-to protect a single host and active mode-to collaboratively protect the nodes in a cluster. In active mode, a cluster head starts a voting algorithm to determine whether intrusion really happens.

Puttini *et al.* have proposed an IDS architecture where information in the management information base (MIB) is used as input data [53]. It also uses mobile agent and a collaborative decision making mechanism. This model is distributed and efficient in use, with high scalability and can detect attack at multiple levels, but has security, computational cost and management problems related to mobile agents.

IDS Model proposed by Brutch and Ko is a statistical anomaly detection algorithm [54]. It works by first assuming that the audit trail generated from a host has been converted to a canonical audit trail (CAT) format. It then

uses a CAT file to generate session vectors representing the activities of the users' sessions. These session vectors are then analyzed against specific types of intrusive activities to calculate "anomaly scores". If the scores cross some thresholds, warnings reports are generated. The algorithm analyzes a session vector in three steps:

1) it calculates a Bernoulli vector,

2) it calculates the weighted intrusion score, and

3) it calculates the suspicion quotient. The Bernoulli vector is generated from the session vectors as well as some threshold vectors. It is a simple binary vector in which the values in the vector are set to one if the corresponding arbitrary counts fall outside the threshold for a particular user group. The weighted intrusion score is generated for a particular session and for a particular intrusion type. It can be used to assign a suspicion value to the session. This suspicion value, or suspicion quotient, for a session is determined by what percentage of random sessions have a weighted intrusion score less than or equal to the weighted intrusion score of the current session. It describes how closely a session resembles the intrusion type as compared to all other sessions. The Haystack algorithm gets its name by being the algorithm implemented in the IDA called Haystack. Haystack is a host-based system, which attempts to detect several types of intrusions: attempted break-ins, masquerade attacks, penetration of the security system, leakage of information, denial of service, and malicious use. It was initially developed for use in the US military network. This algorithm is designed for use in a secured wired military network. If in a wireless ad hoc environment, it requires a designated node to act as a central administrator and all the other nodes to allow the central administrator to retrieve audit trails from them. The central administrator can be pre-designated by the human initiator of the ad hoc network or can be assigned by programming. The audit trails requested can be submitted by the nodes themselves or by the mobile agents allowed to run on the nodes.

An IDS approach, Indra, proposed by Janakiraman *et al.* is a distributed intrusion detection scheme based on sharing information between trusted peers in a network to guard the network as a whole against intrusion attempts [55]. It is a detection tool that takes a proactive and P2P approach to network security. The basic idea behind this model is cross monitoring or simply called "neighborhood watch," and is very simple. In this method, the hosts on the P2P network join together to form some sort of an immune system where each host distributes information on attempted attacks among the interested peers in the network. Such information is usually gathered by the intended victim of an attack and by notifying its adjacent hosts, an alarm can be sounded. This allows the system to react proactively or retroactively. When an alarm is sounded, subsequent attacks to other hosts are repelled straightaway as the adjacent hosts would have forewarned other hosts.

Most of the surveyed models use packets and network traffic related information such as updates in routing table or request-reply flow in the network. Among the ones that use packets related information, IDS approach proposed in [50,51] uses the information inside the packets header directly, such as network address or port number. Other models using packet or network traffic related information mainly use statistical data processes from packet information, such as the statistics of the number of packets received and sent or the statistics of change in routing table. IDS Model as described in [48] utilizes the statistics derived from packet or traffic related statistics, for instance, the correlation between the number of packets dropped and the percentages of updates in routing table. Intrusion Detection approaches illustrated in [43] allow the IDA to work on different types of audit data or the possibility to adapt to different types of audit data. This property is valuable and should be an important consideration for the future design of IDA. Most of the architectures detect only the fact that an intrusion happens. Some models go further to obtain more information, such as the type of attack and the location of the intruder. For instance, Zone based IDA can detect both the type and location of the attack [46].

Some of the intrusion detection models utilize cluster head or gateway nodes [42]. The advantage of cluster head is that some of the resource consuming computation, such as intrusion detection, can be carried out only on some nodes of the network. Therefore, most other nodes can focus on the real work of network traffic. The cluster head usually collects information from cluster member to make the detection decision. In some methods, the original input data is further processed or formatted before it is sent to the cluster head. By doing this, the network traffic for transferring such data is reduced. The computation on the cluster head can also be reduced because the incoming data from member nodes is already formatted for the IDA use. The security communication between the cluster head and its member nodes should receive attention of research.

Most of the methods in our review, except the model proposed in [49], utilize anomaly detection. The anomaly detection is more suitable than misuse detection in Mobile Ad Hoc Networks. In Mobile Ad Hoc Networks, the anomaly detection has a weakness: the profile of normal behavior needs to be updated periodically. This places a heavy burden on the limited network resources.

3.2.2. Review of MANET Intrusion Response Security Approaches

Although intrusion response component is related and coexist with the intrusion detection framework, it receives considerably less attention than detection framework owing to the inherent complexity in developing and deploying response in an automated fashion [56]. Most

of the security models generate an alarm informing the administrator, who then decides the response. However, it is desirable that the response consists of an automated corrective action to protect the network from an identical future attack.

There are few IDA models that provide the integrated detection and response feature. Zhang *et al.* in their framework have explained that local response module triggers action local to the mobile node and the global response module coordinates actions among neighboring nodes, such as the IDS agents in the network electing a remedy work [43]. They have also explained that the type of response depends on the type of intrusion, the type of protocols, applications and the confidence in the evidence with examples. However, they have not provided any implementation details regarding the intrusion response aspect of the model. Similarly, there is no documentation on the simulation or experimental results on the response aspect of the model. However, there is a detailed explanation on the experimental results of the detection framework of the model. Thus, even though the idea of integrated detection and response model seems feasible, it appears that the implementation and simulation have not been conducted. Similarly, few related IDA models propose response actions/frameworks for responding to the attacks once it is detected [57-65]. However the response system incorporating all those actions is not implemented.

There are a few intrusion prevention approaches described in the literature for mobile ad hoc network security as well. Puttini *et al.* have proposed a secure routing protocol that combines a certificate based authentication service with intrusion detection model to provide preventive and corrective protections for Mobile Ad Hoc Networks [53]. Bhargava *et al.* have proposed a security model for AODV routing protocol to prevent attacks in mobile networks [66].

3.2.3. Limitations of existing MANET Intrusion Detection and Response Security Approaches and Open Research Issues

The misuse detection systems use patterns of known attacks to match and identify those intrusions [67]. Although it can accurately and efficiently detect instances of known attacks, it lacks the ability to adapt in detecting new type of attacks. The anomaly detection systems on other hand detect intrusions by finding deviations from the established user profiles. Anomaly detection should detect new types of intrusions but it could have higher false positive rate [68]. Traditionally, IDA are developed using expert knowledge of the system and attack methods [48]. Due to the complexity of modern network system and sophistication of attackers, expert knowledge engineering is often very limited and unreliable [43]. Some IDA schemes are very sensitive to the data representation. For instance, these schemes may fail to generalize an unseen data if the representation contains irrelevant information. In some instance, it has been observed that training of IDA requires a noise-free data (the data that is labeled 'normal') [42]. It has been observed that the existing IDA performs poorly in detection as well as the false positive rates at higher mobility rates [46]. It has recently been observed that Denial of Service (DoS) attacks are targeted even against the IDA [18]. Thus, IDA themselves needs to be protected. An IDA should also be able to distinguish an attack from an internal system fault.

The identification of intruder and appropriate response techniques to protect Mobile Ad Hoc Networks still represents a challenging issue. The need to coordinate intrusion detection and response techniques and the need to respond and control the identified attacks effectively, require further research. It can be noted that though the response concepts are explained in the existing intrusion detection models, implementation details and results for the response framework are not provided to demonstrate and validate their response techniques. Also according to our literature review, we observe that none of the existing models has proposed an intrusion control approach for mobile and senor networks, such that detection and response are done continuously to protect the mobile ad hoc networks.

To summarize, the related existing intrusion detection and intrusion response approaches suffer from one or more of the following limitations specifically with respect to mobile ad hoc networks:

- Lower detection rate when mobility is used as a pa rameter.
- Higher false positive rate when mobility is used as a parameter.
- Appropriate response techniques to protect Mobile Ad Hoc Networks after threat detection.

4. Review of Mobile Agent Model Security Approaches

In the following sections, we present the security approaches for the different attack scenarios explained earlier in Section 2.

4.1. Security Approaches for Mobile Agent Attacked by Another Agent

Location privacy through user smart card is proposed by [69]. This scheme takes care of the unauthorized access, masquerade attacks, which is achieved through secret keys for secure communication with network and the other users. It has some advantages like location and identification privacy in addition to just content privacy. This proposal uses digital mix proposed by Chaum [70]. A digital mix enables two parties to communicate with-

out unauthorized parties being able to determine either the message content or the source and destinations of the messages. In addition, the sender of a message can remain anonymous to the recipient. This is achieved through an intermediate computer called a 'mix' processes messages so that header information is hidden from following communications. The main idea is new authentication, digital mix, information leak and billing services. The architecture new security features for mobile networks with existing infrastructure be provided through additional intelligent network services.

Profiling mobile users by Bayesian decision algorithm [71] proposes to provide detection and response solution for an agent attacked by agent privacy problems like masquerade and unauthorized access. This proposal focuses on the application of anomaly detection techniques to mobile networks and generation of user profiles within GSM mobile networks.

Enhanced privacy and authentication for GSM by C. H. Lee *et al.* [72] proposes three improved methods to enhance the security, to reduce the storage space, to eliminate the sensitive information stored in VLR, and consequently to improve the performance of the system. It includes an improved authentication protocol for the mobile station, a data confidentiality protocol, and a location privacy protocol. This proposal tends to improve but not to alter the existing architecture of the system, which is a very useful feature for the practical reasons. This scheme attempts to provide a solution for unauthorized access and masquerading by means of improved authentication protocol which eliminated the redundant sensitive information stored in Virtual Location Register (VLR), data confidentiality protocol (with/without session key table in Home Location Register (HLR/SC) and location privacy protocol with/without conference key shared by HLR's.

4.2. Security Approaches for Mobile Agent Attacked by the Host

Mobile code cryptography [21] provides solution through encrypted functions and digital signing. This proposal uses cryptographic primitives and homomorphic encryption schemes (public key) and function composition schemes. This solution tries to prove that mobile code holds the key to uncouple the secure execution of programs from the trustworthiness of the underlying execution support. This solution tries to prove that one can obtain a system where a host can execute an encrypted function without having to decrypt it. The functions would be encrypted such that the resulting transformation can be implemented as a (mobile) program that will be executed on a remote host. The executing computer will see the program's clear text instructions but will not be able to understand the function that the program implements. This scheme attempts to provide a solution for masquerade and eavesdropping attacks by host on agent. This is achieved with the help of cryptography and encrypting agent functions that are executed by the host. This is realized via homomorphic functions and homomorphic encryption scheme.

Secure and open mobile agents (SOMA) [73] provide secrecy and integrity to the mobile agents by means of encryption and authenticated channels. Here agent is encrypted and digitally signed. This model has no overhead as in Trusted Third Party (TTP) solutions. The solution is an efficient, scalable and robust than multiple host (MH) protocols. However this proposal does not discusses about secrecy during the agent execution and secure delegation. This scheme attempts to provide a solution for eavesdropping, masquerade and alteration attacks on agent by host. This is achieved through a security infrastructure and layered security policies that imposes authorizations and authentications. The security infrastructure consists of a policy server, a domain server for domain management, a role server for role management, a certification authority for issuing and the lifecycle management of certificates, an authentication server, an authorization server.

Another proposal, AJANATA [74] provides secure access to system resources and supports isolated protection domains for agents by using supported thread groups and class loaders. This security architecture provides a solution for providing denial of service, alteration, eavesdropping and masquerade attacks by host on agent. This is achieved by authentication protocol, by generic Agent-Server class, Ajanta security manager. Authentication protocol's name services enforce its security policies. The architecture also provides protected name spaces for different users. This model uses proxy concept and protects the information of agent. The proposed architecture is built upon Java's security model and address problems related to protecting agent servers, agents and the name service information.

A solution through smartcards [9] by multifunctional trusted smart cards uses Java card for authentication and signing device, when user sends an agent and for trusted computing base attached to host environment. This scheme attempts to protect agent from alteration, denial of service and masquerade attacks by host on agent. This is achieved by allowing agents to carry encrypted code parts and protecting an agent's itinerary by means of security store. The decrypted form will be visible to smartcard only. This is achieved by using public key encryption with certified public keys. This approach protects specific parts of mobile agent better than just using Java Card alone. This proposal which uses trusted computing base claims better protection for the agents than the mobile code cryptography, encrypted functions, code obfuscation and cryptographic trace etc.

A public key based secure Mobile IP was proposed by Zao *et al.* [75] in their Mobile IP Security System (Mo-

IPS) was based on a DNS based X.509 PKI and the innovation in cross certification and zero-message key generation. This proposal attempts to provide solution for alteration, masquerading and eavesdropping attacks by means of key management and cryptographic keys for authentication, access control and using secure tunneling. The system supplies cryptographic keys for authenticating Mobile IP v4 location management messages and establishing IPSec tunnels for Mobile IP redirected packets. It was developed to support three services that are essential to the safe operation of Mobile IP: 1) authentication of Mobile IP control messages for location update, 2) access control of Mobile Nodes to resources in the foreign networks, and 3) secure tunneling to redirected IP datagram. Public key technology is used for the scalability reasons. A DNS based PKI has clear advantage over a distributed system of key distribution centers (KDC) since PKI solves the potentially complicated server discovery problem, and it eliminates the need for real-time key dispatches by the KDC.

Sufatrio and Lam [76] proposed a solution for the security aspect of the registration protocol, an extension in Mobile IP. This scheme provides solution for the masquerade, alteration, non-repudiation and eavesdropping attacks, through the public-key based authentication with a minimal use of public key cryptography. This scheme also attempts to provide solution for a replay attack on mobile agent's registration. It provides a scalable solution for authentication and non-repudiation and also strives for minimal computing and administration cost on the mobile agent.

Detecting malicious changes to an agent's state during its execution or data does not yet have a general solution yet.

4.3. Security Approaches for Host Attacked by Mobile Agents

Authentication protects host [3] by preventing agent pretending as host. This is achieved through shared key for encryption messages or privacy.

The issues that face this model are the authentication is needed whenever the agent traverses each new cell, especially with network partitions. This model tries to address the following security goals.

1) Walkstation (mobile agent or computer) and the basestation must be able to authenticate each other. It prevents a malicious station from pretending to be a base station and also it permits the walkstation to choose the services of a particular base station in the presence of collocated networks.

2) Once authenticated walkstation and basestation should be able to communicate securely. Privacy has two dimensions: data privacy and location privacy.

3) Walkstations should be provided location privacy. Some applications will require location privacy, while others may exploit the knowledge of walkstations. The goal is to provide location privacy at the lowest layer. Higher layers may disseminate location information according to the needs of the applications.

4) The security should be optional (due to the tradeoff in the limited resources and the security) and efficient. This scheme attempts to provide secured solution for unauthorized access and masquerade attacks. This is achieved by mutual authentication of base station and walk station and thereby generating a shared key for encryption of messages. This scheme relies on private/public key mechanism to achieve the solution.

The proposal of SOMA architecture provides authentication and authorization for the host security from mobile agents. This model addresses the issue of balanced trade off between several requirements, often contrasting security, flexibility, usability and efficiency. This scheme proposes a scheme for the protection of agents from malicious hosts (sites), which is fundamental for agent-based applications in untrusted environments and are still an active research area. This scheme attempts to provide a solution for masquerade and unauthorized access attacks by agents on host.

The solution through Proof Carrying Code (PCC) [77] provides a security for hosts in the masquerade and unauthorized attacks via proof checker ensured by code producer which is "tamper proof" and "self certifying code/agent". Necula suggests that the theory of programming languages, including formal semantics, type theory and applications of logic, are critical to solving the untrusted-code security problem essentially through the exploitation of static checking for achieving a high level of security in mobile-code applications. The advantages of PCC are that the burden of providing security is shifted to code producer; they are tamperproof and self certifying.

PCC is a technique by which host establishes a set of safety rules that guarantee safe behavior of programs, and the code producer creates a formal safety proof that proves, for the untrusted code, adherence to the safety rules. Then, the host is able to use a simple and fast proof validator to check, with certainty that the proof is valid and hence the foreign code is safe to execute.

Lu *et al.* [23] proposed an algorithm for fair service in error-prone wireless channels this algorithm provides short term fairness among flows which perceive a clean channel, long term throughput and fairness bounds for all flows with bounded channel error, an expanded schedulable region by decoupling delay/bandwidth weights, and supports both delay sensitive and error sensitive data flows. This wireless fair service algorithm attempts to provide solution for denial of service attacks, by providing a performance effective fair service in error-prone communication channels.

Trost and Binkely proposed [24] an authenticated link-level ad hoc routing protocol for Mobile IP, which ad-

dresses link security issues. This scheme attempts to provide solution for unauthorized access and masquerade attacks. It addresses the issues of attacker stealing host's packets. The protocol also eliminates denial of service attacks caused by an ARP spoof destroying data link layer towards a host. The protocol also tries to limit the eavesdropping, copy and replay, alteration attacks an unwanted visitor to do for a host. This is achieved by not only correct implementation of sound protocols but also by proper maintenance methodologies. In this protocol, mobile agent's and node's packets are authenticated and security problems associated with ARP spoofing are also reduced by this scheme. The authentication is provided through network authentication key and adhoc key. This scheme also attempts to provide a solution for the replay attacks by agent.

Perkins proposed a Mobile IP/AAA trust model [78] which relies on the existence of servers that are capable of performing accounting, authentication, and authorization (AAA) services. This new infrastructure is designed to meet the emerging needs of cellular telephony [79] for mobile data service to a large population of mobile telephone users, and eventually over VoIP. Several schemes like security infrastructure in CDMA networks [80] uses the Mobile IP/AAA trust model for their solution. This model attempts to provide a solution for alteration, eavesdropping and masquerade attacks by satisfying the AAA security requirements and protocols.

4.4. Security Approaches for Host Attacked by Other Unauthorized External Parties Including Host and Agents

Protection of dumb host by a scheme for authenticating host in a secure mobile network [81] attempts to provide solution for masquerade and unauthorized attacks. This is achieved using a hierarchy of mobile agents and relies upon the computation priorities to determine which agent is to be active in each authentication request. The scheme attempts to solve the This scheme proposes a hierarchical simulation model and analyzes several factors involved in the computation of priorities, to determine the optimal weightings of each factor involved and the dependence, if any, of these weightings on the factors of the hierarchy itself.

Protection for host by fault tolerant authentication [13] has some positive aspects like fault tolerance and scalability issues taken care, clusters of a node than single over the other proposals like Virtual Router Redundancy Protocol (VRRP), which are not scalable. This proposal attempts to solve the masquerade and unauthorized access attacks on hosts by using hierarchical authentication and a flat model as in a LAN environment. These techniques make use of backup servers. However, the performance issues that affect performance are still the issues that are to be taken care by partitioning the secret key database and through analysis to discover the parameters that affect the performance of the system and study how the priorities depend on these factors.

MACKMAN [82] propose a solution motivated by the deficiencies found in the registration and authentication service of the existing protocols such as GSM, CDPD, and IS-41. This solution employs mutual authentication and digital signatures to provide a more secure registration and authentication service for mobile computing by using Elliptic Curve RSA (ECRSA) for the efficiency reasons. This scheme provides solution for unauthorized access, denial of service and masquerade attacks by addressing the following issues:

- Trustworthiness of Intermediate Network.
- Mutual Authentication between a mobile agent and mobile host.
- Data Confidentiality against both active and passive intrusion by malicious agents.
- Untraceability requires protection of registered users from unauthorized entities. A mobile host should be able to request network services without divulging any access control information to eavesdroppers. The degree of untraceability availability to mobile host depends upon the policies enforced by the underlying system and the tradeoffs between cost and benefits.
- Time Synchronization, since the mobile agents travel across various time zones and administrative authorities and hence the time synchronization in security systems for mobile environments is not recommended.
- Optional Security and Modes of Security: Due to the scarce mobile environment resources likes bandwidth and power and hence various modes of security should be made optional.
- Flexibility: The security system for mobile environments should provide enough flexibility to incorporate future advances in shared-key cryptographic techniques.
- Interoperability: The security system for mobile environments should provide for interoperability between numerous variations and versions of cryptographic products.

Multicast security proposed by LiGong and N. Shahchum [83] tries to provide security in a group-oriented secure data exchange in a multicast environment which could be extended to a mobile environment, where it attempts to solve identity of the originator of a message and group-oriented authentication. These mechanisms are incorporated into session, presentation, and network layers of the network architecture, where they consist of authentication, encryption, and physical access to the tree, respectively. This scheme attempts a solution for masquerade, unauthorized access and denial of service attacks in a multicast environment. Masquerade attack is solved through authentication (using pair wise authenti-

cation model) and secure session membership policies, registration, deregistration, secure session communication (using a common encryption key) and secure broadcast using polynomial interpolation. The problem of message eavesdropping and masquerading is achieved through encryption and decryption. The problem of unauthorized access attacks is solved through pair wise authentication model.

Joseph and Kaashoek proposed [84] proposed building reliable mobile computing applications using the Rover toolkit, to add server-side support for reliable operation, in addition to the existing client-side support. In this scheme they attempted to provide solution for denial of service attacks by implementing server failure recovery procedures and server failure detection.

4.5. Limitations of the Existing Schemes and the Open Research Issues

Since security in mobile computing is an after thought until the recent years, there are many open issues that need to be addressed. Many proposals address the issue of site protection against malicious agents. The complementary problem of protecting agents while executing in potentially malicious sites (host or base station) is specific to MA technology. The secrecy and integrity during agent execution need to be preserved in order to leverage the MA exploitation in wide application contexts. The agency secrecy of both code and state parts represents a challenging issue [85]. It seems rather impossible to hide the agent code from the site responsible for its execution. The same applies to the state part if the code has to work on it.

So far a little research was done on protecting a mobile agent from malicious hosts: the main focus was on making the execution of mobile code efficient and safe for the host. This is due to the assumption that mobile code is impossible to protect without resort to special hardware, simply because the code has to be executed by the hosting system.

However protecting a mobile agent against malicious hosts is not a "nice-to-have" feature but is essential for an agent system's usefulness [21]. The security research issues could be summarized as follows:

- Can a mobile agent protect itself against tampering by a mobile host? (code and execution integrity)
- Can a mobile agent remotely sign a document without disclosing the user's private key? (computing with secrets in public).
- Can a mobile agent conceal the program it wants to have executed? (code privacy)
- Secure routing or denial of service attacks protection.
- Can a host (computer) execute a cipher program without understanding it?

Other relevant issues include

- The protection of the executing host from malicious actions of mobile code.
- The protection of the network as a whole (e.g., from spamming agents or hosts).
- The secure routing of mobile code.
- The detection of tampering by and the identification of a malicious host.
- The protection of mobile code against input/output analysis.

In a dynamic system, mobile agents entering remote domains need to have the ability to inherit permissions from their home agents while maintaining information and location security. The security mechanism should be designed so that the provision of security does not add significant delays during call setup and communication and does not waste the scarce resources like wireless link bandwidth and the battery power [10]. Proposed security schemes should be efficient in the number and size of messages exchanged and should not cause the channel bandwidth to increase or cause propagation of errors nor should it result in increased error rates.

Another issue typical to mobile computing environment is the issue of time synchronization, since the mobile agents travel across various time zones and administrative authorities and hence the time synchronization in security systems for mobile environments is not recommended. Also, any security system for mobile environments should provide enough flexibility to incorporate future advances in shared-key cryptographic techniques and numerous variations of cryptographic products.

5. Conclusions

In this paper we have presented the taxonomy of security schemes for mobile computing systems. We have classified them based upon the infrastructure that makes up the mobile computing system and then by the type of attacks. The classification helps increasing our understanding of the security issues and requirements of the mobile computing and the schemes that could solve these issues and requirements. In general, there are tradeoff between the resource constraints, performance, scalability and the provision of security features. Also, there is a no single scheme that provides a general solution for the different kind of security threats in the mobile computing environment. With respect to the MANET based mobile computing system, our analysis shows that the potential threats faced by MANETs come in the form of denial of service, selfish node behavior, or routing attack. Also majority of the recent effort is spent to secure active MANET attacks rather than passive MANET attacks. With respect to the mobile agent model based mobile computing system, providing security for the mobile agent from the fixed host seems to be more challenging than providing the security for fixed host from mobile

agent. The taxonomy developed in this paper highlights the contributions for different types of attacks and shows the different types of approaches taken to provide security. This taxonomy should help researchers focus on underlying methods, limitations of the existing schemes and open research issues needed to secure MANETs.

6. References

[1] H. Reiser and G. Vogt, "Security Requirements for Management Systems Using Mobile Agents," *Proceedings of the 5th IEEE Symposium on Computers and Communications*, Antibes-Juan Les Pins, 2000, pp. 160-165.

[2] J. E. Canavan, "Fundamentals of Network Security," Artech House, Boston, 2001.

[3] S. Funfrocken, "Protecting Mobile Web-Commerce Agents with Smartcards," *Proceedings of the 1st International Symposium on Agent Systems and Applications*, Palm Springs, California, 1999, pp. 90-102.

[4] H. Deng, Q. Zeng and D. P. Agrawal, "Network Intrusion Detection System Using Random Projection Technique," *Proceedings of the International Conference on Security and Management*, Las Vegas, 2003, pp. 10-16.

[5] A. Sundaram, "An Introduction to Intrusion Detection," *Crossroads*: *The ACM Student Magazine*, Vol. 2, No. 4, 1996, pp. 3-7.

[6] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance," James P. Anderson Co., Fort Washington, 1980.

[7] A. Mitrokotsa, N. Komninos and C. Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," *Proceedings of IEEE International Conference on Pervasive Services*, Los Alamitos, CA, USA, 2007, pp. 118-127.

[8] J. Hubaux, L. Buttyan and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," *Proceedings* of *the MobiHoc Conference*, California, 2001, pp. 146-155.

[9] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," *Proceedings of International workshop on Security Protocols*, Berlin, 1999, pp. 172-194.

[10] P. Vinayakray-Jani, "Security within Ad Hoc Networks," *Presented at First PAMPAS Workshop*, London, 2002, pp. 66-67.

[11] K. Wrona, "Distributed Security: Ad Hoc Networks and Beyond," *Presented at First PAMPAS Workshop*, London, 2002, pp. 70-71.

[12] L. Buttyan and J. Hubaux, "Report on a Working Session on Security," *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 7, No. 1, 2003, pp. 74-94.

[13] P. Michiardi and R. Molva, "Simulation-Based Analysis of Security Exposures in Mobile Ad Hoc Networks," *Proceedings of European Wireless Conference*, Florence, 2002, pp. 287-292.

[14] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *Proceedings of ACM Workshop on Wireless Security*, Atlanta, 2002, pp. 21-30.

[15] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, San Antonio, 2002, pp. 27-31.

[16] S. Buchegger and J. Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness and Robustness in Mobile Ad Hoc Networks," *Proceedings of* 10*th Euromicro Workshop on Parallel*, *Distributed and Network-based Processing*, Canary Islands, 2002, pp. 403-410.

[17] P. Michiardi and R. Molva, "Prevention of Denial of Service Attacks and Selfishness in Mobile Ad Hoc Networks," Research Report RR-02-063, Institute Eurecom, 2002.

[18] B. K. Bhargava, S. B. Kamisetty and S. K. Madria, "Fault Tolerant Authentication in Mobile Computing," *Proceedings of International Conference on Internet Computing*, Las Vegas, Nevada, USA, June 2000, pp. 395-402.

[19] A. Fugetto, G. P. Pivvo and G. Vigna, "Understanding Code Mobility," *IEEE Transactions on Software Engineering*, Vol. 24, No. 5, 1998, pp. 342-361.

[20] D. Johansen, R. V. Renessee and F. B. Schneider, "An Introduction to the TACOMA Distributed System-Version 1.0," Technical Report, Department of Computer Science, University of Tromso and Cornell University, 1995.

[21] T. Sander and C. Tschud, "Towards Mobile Code Cryptography," *Proceedings of IEEE Symposium on Security and Privacy*, California, 1998, pp. 215-224.

[22] B. Askwith, M. Merabti, Q. Shi and K. Whiteley, "Achieving User Privacy in Mobile Networks," *Proceedings of* 13*th Annual Computer Security Applications Conference*, USA, 1997, pp. 108-116.

[23] T. G. Brutch and P. C. Brutch, "Mutual Authentication, Confidentiality and Key Management (MACKMAN) System for Mobile Computing and Wireless Communication," *Proceedings of* 14*th Annual Computer Security Applications Conference*, Scottsdale, Arizona, 1998, pp. 308-317.

[24] B. K. Bhargava, S. B. Kamisetty and S. K. Madria, "Fault Tolerant Authentication in Mobile Computing," *Proceedings of International Conference on Internet Computing*, Las Vegas, Nevada, USA, 2000, pp. 395-402.

[25] S. Yi and R. Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks," Technical Report UIUCDCS-R-2002-2290, Department of Computer Science, University of Illinois, 2002.

[26] S. Capkun, L. Buttyan and J. P. Hubaux, "Self Organized Public-Key Management for Mobile Ad Hoc Networks," *Transactions on Mobile Computing*, Vol. 2, No. 1, 2003, pp. 52-64.

[27] H. Yang, X. Meng and S. Lu, "Self-Organized Network Layer Security in Mobile Ad Hoc Networks," *Proceedings of ACM MOBICOM Wireless Security Workshop*, Atlanta, 2002, pp. 11-20.

[28] A. A. Ramanujam, J. Bonney, R. Hagelstrom and K. Thurber, "Techniques for Intrusion-Resistant Ad Hoc

Routing Algorithms (TIARA)," *Proceedings of MILCOM Conference*, Los Angeles, 2000, pp. 660-664.

[29] Y. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Proceedings of* 4*th IEEE Workshop on Mobile Computing Systems & Applications*, New York, 2002, pp. 3-13.

[30] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *Proceedings of ACM Workshop on Wireless Security*, Atlanta, 2002, pp. 21-30.

[31] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, San Antonio, 2002, pp. 27-31.

[32] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks," Technical Report, Department of Computer Science, 2000.

[33] Y. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proceedings of the* 8*th Annual International Conference on Mobile Computing and Networking*, Atlanta, 2002, pp. 12-23.

[34] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proceedings of* 6*th Annual Conference on Mobile Computing and Networking*, Boston, 2000, pp. 255-265.

[35] S. Yi, P. Naldurg and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks," *Proceedings of Second ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Urbana, 2001, pp. 299-302.

[36] J. Brinkley and W. Trost, "Authenticated Ad Hoc Routing at the Link Layer for Mobile Systems," *Wireless Networks*, Vol. 7, No. 2, 2001, pp. 139-145.

[37] J. Kong, H. Lou, K. Xu, D. Gu, M. Gerla and S. Lu, "Adaptive Security for Multi-Layer Ad Hoc Networks," *Special Issue of Wireless Communication and Mobile Computing*, Vol. 2, No. 5, 2002, pp. 533-547.

[38] L. Buttyán and J. P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *ACM Journal for Mobile Networks* (*MONET*), Vol. 8, No. 5, 2003, pp. 579-592.

[39] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Proceedings of Communication and Multimedia Security Conference*, Portoroz, 2002, pp. 107-121.

[40] S. Buchegger and J. Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes-Fairness in Distributed Ad Hoc NeTworks," *Proceedings of MobiHoc Conference*, Switzerland, 2002, pp. 226-236.

[41] G. Avoine and S. Vaudenay, "Cryptography with Guardian Angels: Bringing Civilization to Pirates," *ACM Mobile Computing and Communications Review* (*MC*2*R*), Vol. 7, No. 1, 2003, pp. 74-94.

[42] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," *Proceedings of* 36*th International Conference on System Sciences*, Hawaii, 2003, pp. 57-64.

[43] Y. Zhang, W. Lee and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *Wireless Networks*, Vol. 9, No. 5, 2003, pp. 545-556.

[44] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks*, Fairfax, Virginia, 2003, pp. 135-147.

[45] H. Debar and A. Wespi, "Aggregation and Correlation of Intrusion Detection Alerts," *Proceedings of* 4*th International Symposium on Recent Advances in Intrusion Detection*, Davis, CA, USA, 2001, pp. 85-103.

[46] P. Albers and O. Camp, "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches," *Proceedings of* 1*st International Workshop on Wireless Information Systems*, Ciudad Real, Spain, 2002, pp. 1-12.

[47] B. Sun, K. Wu and U. W. Pooch, "Integration of Mobility and Intrusion Detection for Wireless Ad Hoc Networks," *International Journal of Communication Systems*, Vol. 20, No. 6, 2006, pp. 695-721.

[48] Y. Huang, W. Fan, W. Lee and P. S. Yu, "Cross-Feature Analysis for Detecting Ad Hoc Routing Anomalies," *Proceedings of* 23*rd International Conference on Distributed Computing Systems*, Providence, 2003, pp. 478-487.

[49] C. Tseng and P. Balasubramanyam, "A Specification-Based Intrusion Detection System for AODV," *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks*, Fairfax, 2003, pp. 125-134.

[50] R. Sekar, "Specification-Based Anomaly Detection: A New Approach for Detecting Network Intrusions," *Proceedings of* 9*th ACM Conference on Computer and Communications Security*, Washington, DC, USA, 2002, pp. 265-274.

[51] Y. Okazaki, I. Sato and S. Goto, "A New Intrusion Detection Method Based on Process Profiling," *Proceedings of Symposium on Applications and the Internet*, Nara City, Japan, 2002, pp. 82-91.

[52] R. Sowjanya and H. Shah, "Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile Ad Hoc Networks," UMBC Technical Report, 2002.

[53] R. Puttini, J. Percher, L. Me, O. Camp and R. De Souza, "A Modular Architecture for Distributed IDS in MANET Structures," *Lecture Notes in Computer Science*, Vol. 2669, 2003, pp. 91-113.

[54] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad Hoc Networks," *Proceedings of Symposium on Applications and the Internet Workshop*, Orlando, Florida, 2003, pp. 368-373.

[55] R. Janakiraman, M. Waldvogel and Q. Zhang, "Indra: A Peer-to-Peer Approach to Network Intrusion Detection and Prevention," *Proceedings of* 12*th IEEE International Workshops*, Linz, 2003, pp. 226-231.

[56] N. Stakhanova, S. Basu and J. Wong, "Taxonomy of Intrusion Response Systems," Technical Report 06-05,

Computer Science, Iowa State University, 2006.

[57] M. M. Islam, R. Pose and C. Kopp, "An Intrusion Detection System for Suburban Ad-Hoc Networks," *Proceedings of IEEE Tencon Conference*, Melbourne, 2005, pp. 41-46.

[58] G. Vigna, S. Gwalani, K. Srinivasan, E. Belding-Royer and R. Kemmerer, "An Intrusion Detection Tool for AODV-Based Ad Hoc Wireless Networks," *Proceedings of the* 20*th ACSA Conference*, Tucson, 2004, pp. 16-27.

[59] R. Puttini, J. Percher, L. Me and R. Sousa, "A Fully Distributed IDS for MANET," *Proceedings of IEEE Symposium on Computers and Communications*, Brasilia, 2004, pp. 331-338.

[60] B. Lu and U. W. Pooch, "Cooperative Security-Enforcement Routing in Mobile Ad Hoc Networks," *Proceedings of the* 4*th IEEE International Conference on Mobile and Wireless Communications Network*, 2002, pp. 157-161.

[61] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C. Y. Tseng, T. Bowen, K. Levitt and J. Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs," *Proceedings of the* 3*rd IEEE International Workshop on Information Assurance*, College Park, MD, USA, 2005, pp. 57-70.

[62] A. Patwardhan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad hoc Networks," *Proceedings of the* 3*rd International Conference on Pervasive Computing and Communications*, Hawaii, 2005, pp. 191-199.

[63] Y. Fu, J. He and G. Li, "A Distributed Intrusion Detection Scheme for Mobile Ad Hoc Networks," *Proceedings of Computer Software and Applications Conference*, 2007, pp. 75-80.

[64] N. Komninos, D. Vergados and C. Douligeris, "Detecting Unau-thorized and Compromised Nodes in Mobile Ad Hoc Networks," *Ad Hoc Networks*, Vol. 5, No. 3, 2007, pp. 289-298.

[65] A. Mitrokotsa, M. Tsagkaris and C. Douligeris, "Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms," *IFIP International Federation for Information Processing*, Palma de Mallorca, 2008, pp. 133-144.

[66] S. Bhargava and D. P. Agrawal, "Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks," *Proceedings of IEEE Vehicular Technology Conference*, Atlantic City, 2001, pp. 2143-2147.

[67] B. Sun, K. Wu and U. Pooch, "Routing Anomaly Detection in Mobile Ad Hoc Networks," *Proceedings of* 12*th International Conference on Computer Communications and Networks*, Dallas, 2003, pp. 20-23.

[68] R. Guha, O. Kachirski, D. G. Schwartz, S. Stoecklin and E. Yilmaz, "Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks," *Proceedings of* 17*th International Symposium on Computer and Information Sciences*, Florida, 2002, pp. 315-320.

[69] B. Askwith, M. Merabti, Q. Shi and K. Whiteley, "Achieving User Privacy in Mobile Networks," *Proceedings of the* 13*th Annual Computer Security Applications Conference*, San Diego, 1997, pp. 108-116.

[70] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete" *Communications of the ACM*, Vol. 28, No. 10, 1985, pp. 1030-1044.

[71] B. Roland, K. Dogan and R. Peter, "How to Increase Security in Mobile Networks by Anamoly Detection," *Proceedings of the* 14*th Annual Computer Security Applications Conference*, Phoenix,1998, pp. 3-12.

[72] C. H. Lee, M. S. Hwang and W. P. Yang, "Enhanced Privacy and Authentication for the Global System for Mobile Communications," *Wireless Networks*, Vol. 5, No. 4, 1999, pp. 231-243.

[73] P. Bellavista, A. Corrradi and C. Stefanelli, "SOMA Secure and Open Mobile Agent Programming Environment," *Proceedings of the* 4*th International Symposium on the Autonomous Decentralized Systems*, 1999, pp. 238-245.

[74] N. M. Karnik and A. R. Tripathi, "A Security Architecture for Mobile Agents in Ajanta," *Proceedings of the International Conference on Distributed Computing Systems*, Taipei, Taiwan, 2000, pp. 402-409.

[75] J. Zao, S. Kent, J. Gahm, G. Troxel, M. Condell, P. Heliek, N. Yuan and I. Castineyra, "A Public-Key Based Secure Mobile IP Wireless Networks," *Wireless Networks*, Vol. 5, No. 5, 1999, pp. 373-390.

[76] S. K. Y. Lam, "Mobile IP Registration Protocol: A Security Attack and New Secure Minimal Public-Key Based Authentication," *Proceedings of the* 4*th International Symposium on Parallel Architectures*, *Algorithms and Networks*, Singapore, 1998, pp. 364-369.

[77] G. Necula and P. Lee, "Research on Proof-Carrying Code for Untrusted-Code Security," *Proceedings of IEEE Symposium on Security and Privacy*, 1997, p. 204.

[78] C. E. Perkins, "Mobile IP Joins Forces with AAA," *IEEE Personal Communications*, Vol. 1, No. 4, 2000, pp. 59-61.

[79] T. Hiller *et al.*, "3G Wireless Data Provider Architecture Using Mobile IP and AAA," IETF Internet Draft, 1999.

[80] P. J. McCann and T. Hiller, "An Internet Infrastructure for Cellular CDMA Networks Using Mobile IP," *IEEE Personal Communications*, 2000, pp. 26-30.

[81] D. McClure and B. Bhargava, "On Assigning Priorities of Keying Parameters in a Secure Mobile Network," *Proceedings of IEEE Workshop on Reliable and Secure Application in Mobile Environment*, New Orleans, 2001.

[82] T. G. Brutch and P. C. Brutch, "Mutual Authentication, Confidentiality and Key Management (MACKMAN) System for Mobile Computing and Wireless Communication," *Proceedings of the* 14*th Annual Computer Security Applications Conference*, Phoenix, 1998, pp. 308-317.

[83] L. Gong and N. Shacham, "Multicast Security and its Extension to a Mobile Environment," *Wireless Networks*, Vol. 1, No. 3, 1995, pp. 281-296.

[84] A. D. Joseph and M. F. Kaashoek, "Building Reliable Mobile-Aware Applications Using the Rover Toolkit Wireless Networks," Vol. 3, No. 5, 1997, pp. 405-420.

[85] A. Corradi, R. Montanari and C. Stefanelli, "Mobile Agent Protection in the Internet Environment," *Proceedings of* 23*rd Annual International Computer Software and Applications Conference*, Phoenix, 1999, pp. 20-25.

