A MANET

P.B.Ambhore, Ku.A.D.Wankhade, Prof.P.N.Chatur and Prof.A.V.Deorankar

Abstract: We have seen security architecture in a layered view and analyze the reasoning for such security architecture. We have seen a novel protocol to provide cluster based secure communication using ECC technique. Without the fixed infrastructure, provision of security model in mobile ad hoc networks is a challenging task and requires high computation. By adopting clustering based approach to provide secure communication, which requires less overhead in terms of computation and communication and provide high reliability in terms of throughput. The identification of a malicious node(s) and design of a robust security model that could be implemented, even in a hostile environment in the presence of a number of non-colluding nodes.

Keyword: Security, Layers, Mobile, Attacks

1. INTRODUCTION: The proliferation of mobile computing and communication devices (e.g., cell phones, laptops, handheld digital devices, personal digital assistants, or wearable computers) is driving a revolutionary change in our information society. We are moving from the Personal Computer age (i.e., a one computing device per person) to the Ubiquitous Computing age in which a user utilizes, at the same time, several electronic platforms through which he can access all the required information whenever and wherever needed. The nature of ubiquitous devices makes wireless networks the easiest solution for their interconnection and, as a consequence, the wireless arena has been

Experiencing exponential growth in the past decade. Mobile users can use their cellular phone to check e-mail, browse internet; travelers with portable computers can surf the internet from airports, railway stations, Starbucks and other public locations; tourists can use Global Positioning System (GPS) terminals installed inside rental cars to locate driving maps and tourist attractions, researchers can exchange files and other information by connecting portable computers via wireless LANs while attending conferences; at home, users can synchronize

Data and transfer files between portable devices and desktops. Not only are mobile devices getting smaller, cheaper, more convenient, and more powerful, they also run more applications

network services, commonly fueling the explosive growth of mobile computing equipment

market. The exploding number of Internet and laptop users driving this growth further.

Currently, most of the connections among these wireless devices are achieved via fixed infrastructure-based service provider, or private networks. For example, connections between two cell phones are setup by BSC and MSC in cellular networks; laptops are connected to Internet via wireless access points. While infrastructure-based networks provide a great way for mobile devices to get network services, it takes time and potentially high cost to set up the necessary infrastructure. There are, furthermore, situations where user required networking connections are not available in a given geographic area, and providing the needed connectivity and network services in these situations becomes a real challenge. More recently, new alternative ways to deliver the services have been emerging. These are focused around having the mobile devices connect to each other in the transmission range through automatic configuration, setting up an ad hoc mobile network that is both flexible and powerful. In this way, not only can mobile nodes communicate with each other, but can also receive Internet services through Internet gateway node, effectively extending Internet services to the non-infrastructure area. As the wireless network continues to evolve, these ad hoc capabilities are expected to become more important, the technology solutions used to support more critical and significant future research and development efforts can be expected in industry and academy, alike.

1.1. Basic MANET:A mobile ad-hoc network (MANET) is an autonomous system of mobile nodes, a kind of a wireless network where the mobile nodes dynamically form a network to exchange information without utilizing any pre-existing fixed network infrastructure. For a MANET to be constructed, all needed is a node willing to send data to a node willing to accept data. Each mobile node of an ad-hoc network operates as a host as well as a router, forwarding packets for other mobile nodes in the network that may not be within the transmission range of the source mobile node. Each node participates in an ad-hoc routing protocol that allows it to discover multi-hop paths through the network to any other node.

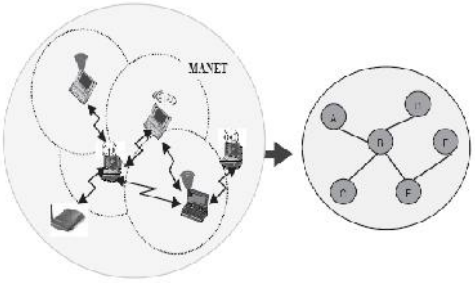

Figure 1.1. Mobile ad hoc network.

P.B.Ambhore is a Research Scholar, **Ku.A.D.Wankhade** is working as Assistant Professor, **Prof.P.N.Chatur** and **Prof.A.V.Deorankar** are working as Professor in Government College of Engineering, Amravati, Maharashtra State, India, Emails: pbambhore@gmail.com archanadwankahde@gmail.com, Chatur.prashant@gcoea.ac.in

1.2. Design Issues and Constraints

Ad hoc wireless networks inherit the traditional problems of wireless communications, such as bandwidth optimization, power control, and transmission quality enhancements, while, in addition, their mobility, multihop nature, and the lack of fixed infrastructure create a number of complexities and design constraints that are new to mobile ad hoc networks, as discussed in the following subsections.

They are Infrastructure less. Mobile ad hoc networks are multihop infrastructure less wireless networks. This lack of fixed infrastructure in addition to being wireless, generate new design issues compared with fixed networks. Also, lack of a centralized entity means network management has to be distributed across different nodes, which brings added difficulty in fault detection and management.

Dynamically Changing Network Topologies. In mobile ad hoc networks, since nodes can move arbitrarily, the network topology, which is typically multihop, can change frequently and unpredictably, resulting in route changes, frequent network partitions, and, possibly, packet losses.

Physical Layer Limitation. The radio interface at each node uses broadcasting for transmitting traffic and usually has limited wireless transmission range, resulting in specific mobile ad hoc network problems like hidden terminal problems, exposed terminal problem, and so on. Collisions are inherent to the medium, and there is a higher probability of packet losses due to transmission errors compared to wireline systems.

1.3. Security Challenge Background

Now-a-days, Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self-configuration and self-maintenance capabilities [16]. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless *MANET* presents a larger security problem than conventional wired and wireless networks. Although mobile ad hoc networks have several advantages over the traditional wired networks, on the other sides they have a unique set of challenges.

Firstly, MANETs face challenges in secure communication. For example the resource constraints on nodes in adhoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Secondly, mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Thirdly, static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like *DoS* (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information.

1.4. Related Work: A number of researches are done on security challenges and solutions in Mobile ad hoc network. Zhou and Haas have proposed using threshold cryptography for providing security to the network [18]. Hubaux et al. have defined a method that is designed to ensure equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates [3]. Kong, et al.[8] have proposed a secure ad hoc routing protocol based on secret sharing; unfortunately, this protocol is based on erroneous assumptions, e.g., that each node cannot impersonate the *MAC* address of multiple other nodes. Yi et al. also have designed a general framework for secure ad hoc routing [17]. Deng, et al. have focused on the routing security issues in *MANET*s and have described a solution of 'black hole' problem [2] . Sanzgiri, et al. have proposed a secure routing protocol *ARAN* which is based on certificates and successfully defeats all identified attacks[14]. Yang, et al. have identified the security issues related to multihop network connectivity, discussed the challenges to security design, and reviewed the state of- art security proposals that protect the *MANET* link- and network-layer operations of delivering packets over the multihop wireless channel [16].

Table 1.1[15] summarizes the attacks and Table 1.2 [16] represents the solutions in each
layer in MANET. Security should be taken into account at the early stage of design of basic networking mechanisms. In this report, I have identified the security threats in each layer and corresponding countermeasures. The following table summarizes the potential security attacks and the actions that can be taken to prevent the attacks.

SECURITY SERVICES: The ultimate goals of the security solutions for *MANETs* is to provide security services, such as *authentication, confidentiality, integrity, authentication, non repudiation, anonymity* and *availabilit*y to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. There is no single mechanism that will provide all the security services in *MANETs*. The common security services are described below.

Table 1.1: Security Attacks on each layer in MANET

Layer	**Attacks**
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping

Table 1.2: Security Solutions for MANET

Layer Security	**Issues**
Application layer	Detecting and preventing viruses, worms, malicious codes,and application abuses
Transport layer	Authentication and securing end-to-end or point-to-point communication through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Data link layer	Protecting the wireless MAC protocol and providing link layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

Table 1.3: Security threats and countermeasures

Layers	**Attacks**	**Solutions**
Application Layer	Lack of cooperation attacks ,Malicious code attacks (virus,worms, spywares, Trojan horses) etc.	Cooperation enforcement (Nuglets,Confidant, CORE) mechanisms, Firewalls, IDS etc.
Transport Layer	Session hijacking attack, SYN flooding attack, TCP ACK storm attack etc.	Authentication and securing end-to-end or point-to-point communication, use of public cryptography (SSL, TLS, SET,PCT) etc
Network Layer	Routing protocol attacks (e.g. DSR, AODV etc.), cache poisoning, table overflow attacks Wormhole, blackhole, Byzantine, flooding, resource consumption, impersonation, location disclosure attacks etc.	Source authentication and message integrity mechanisms to prevent routing message modification, Securing routing protocols (e.g. IPSec, ESP, SAR, ARAN) to overcome blackhole, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack etc.
Data link Layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness etc.	No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP, using WPA etc.
Physical Layer	Jamming, interceptions,eavesdropping	Using Spread spectrum mechanisms e.g.FHSS, DSSS etc.

1.5Availability: Availability is concerned with the (unauthorized) upholding of resources. A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures such as authentication and encryption whereas others require some sort of action to prevent or recover from loss of availability of elements or services of a distributed system. Availability ensures the survivability of network services despite of various attacks. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service.

1.6 Confidentiality: Confidentiality ensures that certain information is only readable or accessible by the authorized party. Basically, it protects data from passive attacks. Transmission of sensitive information such as military information requires confidentiality. Release of such information to enemies could have devastating consequences e.g. *ENIGMA*. Routing and packet forwarding information must also remain confidential so that the enemies could never take the advantages of identifying and locating their targets in a battlefield. With respect to the release of message contents, several levels of protection can be identified.

Integrity: Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted. As with confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message. But, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under integrity service. Thus it addresses both message stream modification and denial of service.

1.7Authentication: Authentication ensures that the access and supply of data is done only by the authorized parties. It is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function is to assure the recipient that the message is from the source that it claims to be from. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes [18].

2 TYPES OF ATTACKS IN MANET The current Mobile ad hoc networks allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Current *MANETs* are basically vulnerable to two different types of attacks: **active attacks and passive attacks**.

Passive attack signifies that the attacker does not send any message, but just listens to the channel. A passive attack does not disrupt the operation of a protocol, but only attempts to discover valuable information. Passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

During an active attack, on the other hand, information is inserted into the network. Passive eavesdropping is a passive attack that attempts to discover nodes information (e.g., IP addresses, location of nodes, etc.) by listening to routing traffic. In a wireless environment it is usually impossible to detect this attack, as it does not produce any new traffic in the network. Active attacks involve actions such as the replication, modification and deletion of exchanged data. Certain active attacks can be easily performed against an ad hoc network. On the other hand, In this topic, my focus is on vulnerabilities and exposures in the current ad hoc network. I can classify the attacks as *modification, impersonation, fabrication, wormhole* and *lack of cooperation.*

2.1 Attacks Using Modification

Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct *.DoS* attacks by modifying message fields or by forwarding routing message with false values. In *fig. 3.1*, ***M*** is a malicious node which can keep traffic from reaching ***X*** by continuously advertising to ***B*** a shorter route to ***X*** than the route to ***X*** that ***C*** advertises [14]. In this way, malicious nodes can easily cause traffic subversion and denial of service *(DoS)* by simply altering protocol fields: such attacks compromise the integrity of routing computations. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.

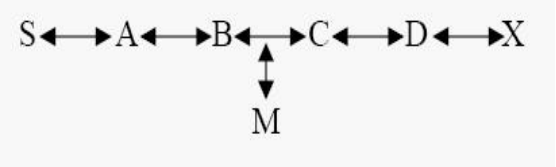

Figure 3.1: Ad hoc network and a malicious node

Consider the following *fig. 3.2*. Assume a shortest path exists from ***S*** to ***X*** and, ***C*** and ***X*** cannot hear each other, that nodes ***B*** and ***C*** cannot hear other, and that ***M*** is a malicious node attempting a denial of service attack. Suppose ***S*** wishes to communicate with ***X*** and that ***S*** has an unexpired route to ***X*** in its route cache. ***S*** transmits a data packet toward ***X*** with the source route ***S --> A --> B --> M --> C --> D --> X*** contained in the packet's header. When ***M*** receives the packet, it can alter the source route in the packet's header, such as deleting ***D*** from the source route. Consequently, when ***C*** receives the altered packet, it attempts to forward the packet to ***X***. Since ***X*** cannot hear ***C***, the transmission is unsuccessful [14].

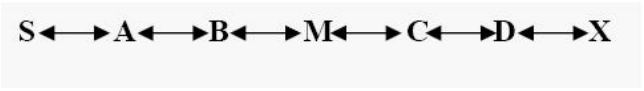

Figure 2.1 : Ad hoc network with DoS attack

2.1 Attacks Using Impersonation

As there is *no authentication* of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its *MAC* or *IP address* in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network.

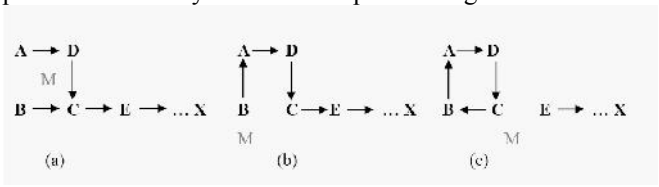

Figure 3.3: A sequence of events forming loops by spoofing packets

In the above *fig. 3.3(a)*, there exists a path between five nodes. ***A*** can hear ***B*** and ***D***, ***B*** can hear ***A*** and ***C***, ***D*** can hear ***A*** and ***C***, and ***C*** can hear ***B***, ***D*** and ***E***. ***M*** can hear ***A***, ***B***, ***C***, and ***D*** while ***E*** can hear ***C*** and next node in the route towards ***X***. A malicious node ***M*** can learn about the topology analyzing the discovery packets and then form a routing loop so that no one nodes in his range can reach to the destination ***X***. At first, ***M*** changes its MAC address to match ***A***'s, moves closer to ***B*** and out of the range of ***A***. It sends a message to ***B*** that contains a hop count to ***X*** which is less than the one sent by ***C***, for example *zero*. Now ***B*** changes its route to the destination, ***X*** to go through ***A*** as shown in the *fig. 3.3(b)*. Similarly, ***M*** again changes its *MAC* address to match ***B***'s, moves closer to ***C*** and out of the range of ***B***. Then it sends message to ***C*** with the information that the route through ***B*** contains hop count to ***X*** which is less than ***E***. Now, ***C*** changes its route to ***B*** which forms a loop as shown in *fig. 3.3(c)*. Thus ***X*** is unreachable from the four nodes in the network.

2.1. Attacks through Fabrication

Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. In *MANET*, fabrication is used to refer the attacks performed by generating false routing messages. Such kind of attacks can be difficult to verify as they come as valid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted [11]. Consider the *fig. 3.1*. Suppose node ***S*** has a route to node ***X*** via nodes ***A***, ***B***, ***C***, and ***D***. A malicious node ***M*** can launch a denial-of-service attack against ***X*** by continually sending route error messages to ***B*** spoofing node ***C***, indicating a broken link between nodes ***C*** and ***X***. ***B*** receives the spoofed route error message thinking that it came from ***C***. ***B*** deletes its routing table entry for ***X*** and forwards the route error message on to ***A***, who then also deletes its routing table entry. If ***M*** listens and broadcasts spoofed route error messages whenever a route is established from ***S*** to ***X***, ***M*** can successfully prevent communications between ***S*** and ***X*** [14].

2.2 Wormhole Attacks

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers. In the *fig. 3.4,* ***M1*** and ***M2*** are two malicious nodes that encapsulate data packets and falsified the route lengths.

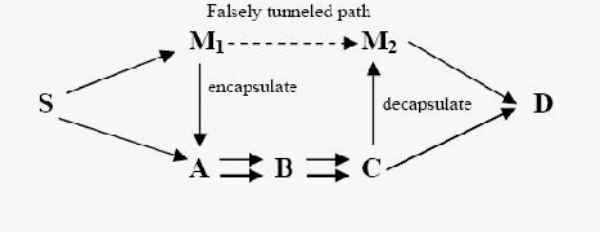

Figure 2.2: Path length spoofed by tunneling

Suppose node ***S*** wishes to form a route to ***D*** and initiates route discovery. When ***M1*** receives a *RREQ* from ***S, M1*** encapsulates the *RREQ* and tunnels it to ***M2*** through an existing data route, in this case {***M1 --> A --> B --> C --> M2***}. When ***M2*** receives the encapsulated *RREQ* on to ***D*** as if had only traveled {***S --> M1 --> M2 --> D***}. Neither ***M1*** nor ***M2*** update the packet header. After route discovery, the destination finds two routes from ***S*** of unequal length: one is of 5 and another is of 4. If ***M2*** tunnels the *RREP* back to ***M1***, ***S*** would falsely consider the path to ***D*** via ***M1*** is better than the path to ***D*** via ***A***. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

2.3 Lack of Cooperation

Mobile Ad Hoc Networks *(MANETs)* rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a *MANET* gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources. This can endanger the correct network operation by simply not participating to the operation or by not executing the packet forwarding. This attack is also known as the black hole attack and is described briefly in later section.

The motivation of dividing the security architecture into such five layers is rather straightforward. SL5 defines the security mechanisms related to end application system, like SET, thus it is necessary to differentiate this layer from the underlying layers. SL4 deals with network access control and network layer data packet protection. SL4 is in fact the security layer working at the end of network fabric. The mechanisms deployed in this layer tackle the network security problems that cannot be solved satisfactorily in the underlying routing protocols. Working at SL4 is a good example of security efforts done in the end systems as a remedy for the unreliable

routing protocol. The reason we include the routing protocol security, i.e., SL3 in the architecture is that the inherent cooperative nature in MANETs requires every node in the network acts both as a host which needs other nodes relaying information for it and also as a router to provide routing and relaying functions to other nodes. The security mechanisms in SL3 are highly related to the network topology and are always designed with respect to specific routing protocol in use. SL2 is a layer providing hop-to-hop communications security, i.e., it is related to the data link security and physical layer security in the wireless communications channel. We require a trust infrastructure in SL1 be established before communication begins to function securely, an example is the trust infrastructure established using distributed threshold cryptography.

The intrusion prevention mechanisms like encryption and signature do not eliminate the need for intrusion/misbehavior detection and response. Although the intrusion/misbehavior detection and response mechanisms are not distinctively specified in the system architecture, they are act usually very important in MANETs security system and can be deployed in any layer of the system architecture according to the security requirements in each layer.

3. SECURITY ARCHITECTURE OF MILITARY APPLICATIONS

For mission-critical applications such as a military application in a hostile environment there are more stringent security requirements than in a MANET for commercial or personal uses. A military scenario may have higher requirements regarding both information security and routing topology security. In such a scenario, we may design the functionalities of each layer in security architecture as follows:

3.1. Data information is protected in a most fine-granular way in application layer, so the best way to protect data information according to their different requirement is at SL5. For example, it is highly desirable to handle data confidentiality and integrity in SL5 layer, since this is the easiest way to protect data from altering, fabrication and compromise. This is especially important in a military scenario where strategic and tactical information is sent.

3.2. Since it is impossible to deploy a centralized firewall or security gateway in an ad hoc network, there is no way for any centralized security gateway to provide network access control services for mobile nodes. Thus the task of network access control and IP data packet protection lies on the end nodes. As IPsec protocol is not applicable to a mobile scenario, we need to exploit other means to protect data packet in SL4. For example, when the underlying routing protocol supports multi-path routing, mechanisms working at SL4 can be used to take advantage of multi-route between the communicating routes to achieve higher reliability and increased data confidentiality when data packets are transmitted along the route from source to destination.

3.3. Military applications require keeping network topology secret and allowing no traffic analysis in SL3. Routing protocol designers should strive to hide the network topology from unauthorized party and should be designed carefully to prevent routing level attacks, like false routing updates, DoS attacks at routing protocols, thus security services such as confidentiality and integrity are expected to be provided in SL3.

3.4. It is desirable to conceal communications in military scenario, and this requirement is most effectively fulfilled in SL2. For example, we can take spread spectrum technologies to make the signal capture difficult or use antennas to influence signal power in space; and we can also deploy WEP or 802.11x to control the link access.

3.5. It seems quite natural to expect a PKI based on centralized or hierarchical offline CA to pre-establish the trust relationship for all the nodes due to the similar hierarchical relationships between soldiers and general, this is in fact infeasible due to the reasons that this cannot handle the situation of compromise since CRL is difficult to deploy in a distributed environment in a timely manner. There is one trust model particularly suited for military scenario: Resurrecting Duckling Security Model, where a secure transient association is handled in a master-slave way which is like the hierarchical relationship between soldiers and their general. The security lies in the sense that master and slaves share a common secret, while the security association is only controlled by the master.

4. SECURITY ARCHITECHTURE FOR TACTICAL MANET

Introduction Communication between any two nodes in MANETs might require the packets to traverse multiple hops. Several protocols have been proposed in the literature for routing in mobile ad hoc networks. Different with traditional wired networks, the intermediate nodes may be mobile and they can cause frequent link failures and staleness of routes. That in turn can result in route errors and trigger off a fresh route discovery process. So the performance of routing algorithm in MANETs is lower than those in traditional networks. With the increase in size of the networks, flat routing schemes do not scale well in terms of performance and the packets maintaining the routing will exhaust the whole bandwidth. Hence, some hierarchical organization is required in large ad hoc networks, such as encountered in battlefield communications, for solving this problem. Routing on top of clustered topologies is much more scalable than flat routing.So our security architecture only focuses on large tactical MANETs which are clustered into many small sub-networks. In fact, the flat networks can be seen as only one cluster networks. Conceptual security architecture of the network inspired by is described in Figure 1. It is layered as network model, trust model and security operations.

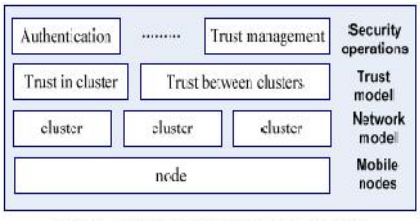

Figure 1. Security architecture for Tactical MANETs

For battlefield communications, trust among nodes is the most important thing. In traditional wired networks, most trust evidences are generated via potentially lengthy assurance processes, distributed offline, assumed to be valid for a long-term and certain at the time when trust relations derived from it are exercised. In contrast, few of these characteristics of trust relations and trust evidences are prevalent in mobile ad hoc networks. Lack of fixed networking infrastructure, high mobility of the nodes, limited range and lack of reliability of the wireless links are some of the characteristics of ad hoc networks that make design of a trust establishment scheme a very difficult and challenging task. In particular, trust relations may have to be established using only online evidence and may be short-term and largely peer-to-peer. Since solutions developed for the fixed wire-line networks are not suitable in such a scenario, some security solutions have been proposed for MANETs based on distributed trust model or fully self-organized trust model. Most of the distributed trust models applied in MANETs are based on threshold cryptography. Fully self organized trust model dose not suit the battlefield for the reason that the building of certificate chain is not efficient enough.

Based on the trust model, many security operations can be carried out. All these operations can be classified as security applications and network security maintenances. Authentication is the first thing for all security applications such as secret communications. Authentication can be easily achieved according to trust model in our security architecture and then confidentiality is a matter of encrypting the session using whatever key material the communicating parties agree on. For reasons that our security architecture combines the network model closely and MANETs are dynamic networks, trust model must be maintained according to network model and trust management though security operations such as trust evidences collecting and trust value evaluation. Node trust evaluation value will not only work on trust model but also network model, for example, the node whose trust value is lower than threshold will be excluded of network.

Trust evaluation:

Trust is a notion corresponding to a set of relations among entities that participate in various protocols. Trust relations are determined by rules that evaluate, in a meaningful way, the evidence generated by the previous behavior of an entity within a protocol. In our architecture the evidences are not only the previous behavior within a protocol but also the previous secure services and secure events such as intrusion and being captured. In battlefield, trust relations change frequently because of all kinds of inside and outside attacks. In previous work done related to intrusion/misbehaviour detection and response, proposed two mechanisms: pathrater and watchdog to improve throughput in the presence of nodes that agree to forward packets but fail to do so. Watchdog is used to identify misbehaving nodes while pathrater evaluates node ratings reported by all nodes and gets the result which can be as a path metric to help routing protocols avoid these misbehaving nodes. In, MANETs security system is presented based on a "neighborhood watch" concept. Recommended-trust is important for nodes that are not neighbors to decide their behaviors.

Secure Clustering:

Clustering protocols in the MANETs are grouped into six categories according to their objectives.

Dominating- Set-based (DS-based) clustering tries to find a DS for a MANET so that the number of mobile nodes that participate in route search or routing table maintenance can be reduced.

Low-maintenance clustering schemes aim at providing stable cluster architecture for upper-layer protocols with little cluster maintenance cost. *Mobility-aware clustering* takes the mobility behavior of mobile nodes into consideration.*Energy-efficient clustering* manages to use the battery energy of mobile nodes more wisely in a MANET. *Load balancing clustering* attempts to limit the number of mobile nodes in each cluster to a specified range so that clusters are of similar size. *Combined-metrics based clustering* usually considers multiple metrics, such as node degree, cluster size, mobility speed, and battery energy, in cluster configuration, especially in cluster head (CH) decisions.With the consideration of more parameters, CHs can be more properly chosen without giving bias to mobile nodes with specific attributes. Also, the weighting factor for each parameter can be adaptively adjusted in response to different application scenarios.

In order to gain a more secure environment in MANETs, clustering should combine security scheme closely. Distributed CA should be deployed in cluster naturally. The trust value should be an important factor in the selection of CH (cluster head). The node whose trust value is lower than threshold should be excluded of network. Some clustering schemes have been proposed partly considering the security goal. The relationship among trust evaluation, secure clustering and distributed CA is shown in Fig. 2.

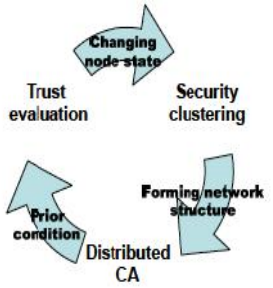

Figure3: Relationship among trust evaluation, secure clustering and distributed CA

The network is divided into clusters. Distributed CA is deployed in every cluster and responsible for the building of certificate chain between nodes inside the cluster. All CHs can form a distributed CA responsible for certificate chain between clusters. Thus, secure clustering forms the network model which is the basis of distributed CA. Distributed CA can build certificate chain for any two nodes either inside the same cluster or belong to different clusters. Certificate chain is prior condition for trust evaluation. Trust evaluation

changes node's state in cluster which will influence the network model. The more detailed security architecture for tactical mobile ad hoc networks is shown in Fig. 3.

5. MULTIHOP SECURITY PROTOCOL

Introduction: Cluster is a sphere with cluster head at the center such that the nodes within the sphere are reachable within a radius of one hop distance from the cluster head. A cluster head serves as a local coordinator for its cluster and to perform inter cluster routing and data forwarding functions. Moreover it is a special node, which has higher capacity in terms of its overhead function and has more capability in terms of its processing speed. It maintains cluster tables, which is used to forward packets from source to destination node. If it moves from its current performing zone then it needs to transfer its responsibilities to other nodes.

Nodes and cluster heads are initially registered with the Trusted Third Party and chipped with the certified token after successful verification of its credentials. This certified token acts as an authentication token and it is similar to public key infrastructure based certificate. In our novel approach, elliptic curve cryptographic technique is used to generate key pairs since the energy consumption of ECC algorithms is less than other PKI based cryptographic approaches. Cluster head and other nodes send beacon messages, which include usual information as well as certified token. Cluster head does not maintain a database to store secret keys and identities of nodes within its performing range. Every time when a node wants to communicate with other node, it needs to execute the proposed protocol in order to provide secure communication based on the position of the destination i.e. with intra cluster or with inter clusters.

$$4.\ N_j \rightarrow CH_j: AReq\ [Source\ ID, Destination\ ID, SNodeID, RNodeID, H_{NjCHj}, E_{SKNjCHj}, E_{SKCHjNj}(R1\|R2\|R3)]$$

$$H_{NjCHj} = Hash\ (H'_{CHj} \| SK_{NjCHj} \| R1 \| R2 \| R3)$$
$$E_{NjCHj} = Enc_{SK}\ (E'_{CHj} \| H'_{Nj} \| R1 \| R2 \| R3)$$
$$H_{NjNi} = Hash\ (H'_{Nj} \| SK_{NjNi} \| R1 \| R2 \| R3)$$

$$5.\ CH_j \rightarrow CH_i: AReq\ [Source\ ID, Destination\ ID, SNodeID, RNodeID, H_{NjCHj}, H_{NjNi}, E_{SKCHjCHi}(R1\ R2\ R3)]$$

$$6.\ CH_i \rightarrow N_i: AReq\ (Source\ ID, Destination\ ID, SNodeID, RNodeID, H_{NjNi}, E_{SKCHiNi}(R1\|R2\|R3))$$

Security Requirement

Mutual Authentication Let us assume that N_i and N_j reside in the same cluster A_i, cluster head CH_i is responsible for cluster **Ai.** After validating CH_i**'s** , N_i sends an **AReq [**$Token_{Ni}$**,** H_{Ni}**,** $E_{SKNiCHi}(R_1)$**]** to CH_i**.** CH_i validates $Token_{Ni}$ using PK_{TTP} as an initial validation. CH_i calculates H'_{Ni} **()** and compares with HN_i, after the successful comparison of **H'Ni** and **HNi, CHi** authenticates node **Ni.** It sends **AReq [**$Token_{Ni}$ $Token_{CHi}$**,** H_{CHi}**,** H'_{Ni}**,** $E_{SKCHiNi}(R_2)$**,** $E_{SKCHiNj}$ **(Hash (**$R_1\|R_2$**))] to** N_j**.** N_j validates $Token_{CHi}$ using PK_{TTP} and calculates H'_{CHi} and compares with H_{CHi}**.** After the successful validation, N_j authenticates CH_i and sends **ARep (**$Token_{Nj}$**,** H_{Nji}**,** H_{NjCHi} **)** for mutual authentication to CH_i and N_i respectively. CH_i computes H_{CHiNj} and compares with the received H_{NjCHi} **.** If it is equal, CH_i**,** ensures node N_j as a right receiver of the **AReq ()** packet originated from node N_i**.** Thus it mutually authenticates N_j**.** CH_i sends **ARep (**$Token_{Nj}$**,** H_{Nji}**,** $E_{SKCHiNi}(R1\|R2)$**,** H'_{CHi}**) to** N_i**.**

N_i computes H'_{Nij} and compares with the received H_{Nji}**.** If it is equal**,** then N_i authenticates N_j mutually**.** Finally, **Hash** (R1||R2) is used to indicate the cluster head that the messages are coming from the authenticated users. While transmitting actual data, communicating nodes append this value with the message to announce that, they are already authenticated to the cluster heads.

Confidentiality:In this protocol N_i **and** N_j**,** generate shared secret key SK_{NiNj} **(**SK_{NjNi}**)** while authenticating each other. This key is used for encrypting the data transmission. In this way it achieves confidentiality. Cluster head and other nodes are not aware of the knowledge of shared secret key SK_{NiNj} **(**SK_{NjNi}**)** generated using ECDH key generation algorithm. It is highly difficult for any intruder, to infer the value of a secret parameter from the known ECC domain parameters. Since ECDH algorithm is based on the hardness of the ECDL problem.

Integrity:Integrity of the data transmitted between N_i and N_j is achieved by including the message authentication code with the original message, which is generated using the shared secret key SK_{NiNj}**.** It is known only to N_i and N_j**.** Generation of the **SKNiNj** is difficult since it is based on the hardness of ECDL problem.

Non-Repudiation: The public key of the principal must be certified by a trusted certification authority. In the proposed protocol shared secret key SK_{NiNj} between end-to-end communicating nodes N_i and N_j**,** can be used to do encryption. In this, secret keys SK_{NiCHi} and SK_{NiNj} can be generated **only** by those specific two entities (Node: Cluster head & Node: Node), which participate in the authentication and communication process.Though other nodes are aware of the elliptic curve domain parameters, it is difficult to generate the secret keys SK_{NiNj} and SK_{NiCHi} since it is based on the hardness of ECDL problem.

6 DETECTION AND PREVENTION FROM MALICIOUS NODES:

Four MAs: Discovery Agent (DA) to locate and identify network topology. DA constructs a request packet identified by a pair of identifier: a query sequence number and a random query identifier. Transport Agent (TA) to deliver topology and security information. Mobile Agent (MA) to police the network for any abnormal activity.

Behavior Agent (BA) to provide the trust mechanism.

Case 6.1: While some communication latency does exist inherently in all nodes, significant changes in latency can be dynamically determined by comparing thresholds set for each ad hoc group of nodes based on history of the network. In fact, this variation of latency from historical threshold values is one factor in determining the malicious behavior. Detection of a malicious node and hostile attack is primarily done through the awareness and determination of a NM malicious attack packet. Consider the extreme case when two colluding nodes, NM1 and NM2 launch a malicious attack. Assuming NM1

sends a corrupt DA. At first, it will appear that the DSP might get mislead into believing the validity of NM1, especially when it receives the DA from NM2. However, unlike conventional security mechanisms of MANET which would have failed under this attack, in our model, the DSP will have an opportunity to evaluate the DA packets from NM1 and NM2 with respect to its historical MA and BA data. This will enable the DSP to quickly determine the malicious nature of both NM1 and NM2 simultaneously. At this point, DSP has many choices to cut off the malicious nodes – from sending a TA to disable IP communication of NM1 and NM2 to redirecting these nodes to an IDS or Honey pot system.

Case 6.2: Consider case in which NM1 does not cooperate with its neighbors and discards packets arriving from the network in a selective manner, say, TA, MA or BA from a DSP. By discarding packets, a malicious node partially narrows the topology view impeding the network operation. In most circumstances this type of malicious act cannot be countered. However, in our model, not only the controlled flooding of the mobile agents provide the required robustness, but the very nature of mobile agent communications will render such nodes incapable of participating in this network. For all practical purposes, the malicious node, at best, can only hide its incident links, but by doing so it gets itself removed from the network as seen by the DSP. Since there is only one DSP at any given time in the network, NM1 cannot inflict harm to data flows originating from any node other than NM1. Damage resulting from NM1 is inconsequential because rest of the network will simply exclude NM1.

Case 6.3: In yet another case, where NM1 appropriately sends a DA, and upon arrival of TA from the DSP it relays a tampered reply with a fake source address routed over the reverse path. In our model, DSP readily discards the reply, due to the integrity protection provided by the MAC. Similarly, DSP discards fabricated route requests, since malicious nodes cannot generate valid request MAC.

Case 6.4: Consider a scenario where NM1 consumes network resources by replaying route requests. In our model these packets are discarded by intermediate nodes, since they maintain a list of query identifiers seen in the past via MA. This is achieved mostly by the underlying routing protocol itself, within the limitations imposed by the size of the query table. IP spoofing, where NM1 attempts to forward at the routing protocol level masking its identity is possible. While this is only serious in the absence of mobile agents, our model makes this type of IP spoofing moot.

CONCLUSION: We have seen security architecture in a layered view and analyze the reasoning for such security architecture. We have seen a novel protocol to provide cluster based secure communication using ECC technique. Without the fixed infrastructure, provision of security model in mobile ad hoc networks is a challenging task and requires high computation. By adopting clustering based approach to provide secure communication, which requires less overhead in terms of computation and communication and provide high reliability in terms of throughput. The identification of a malicious node(s) and design of a robust security model that could be implemented, even in a hostile environment in the presence of a number of non-colluding nodes.

REFERENCES

[1] S. Capkun, L. Buttyan, and J. Hubaux, "*Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks,"* 2003.

[2] Ammayappan, K.; Sastry, V.N.; Negi, A., "*Cluster based Multihop Security Protocol in MANET using ECC*", TENCON 2008 - 2008 IEEE Region 10 Conference, 19-21 Nov. 2008.

[3] Y. Hu, A. Perrig, and D. Johnson, *"Packet Leashes: A Defense AgainstWormhole Attacks inWireless Ad Hoc Networks,"* Proc. of IEEE INFORCOM, 2002.

[4] IEEE Std. 802.11i/D30, *"Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security,"* 2002.

[5] J. Kong et al., "*Providing robust and ubiquitous security support for mobile ad-hoc networks,"* In Proc. IEEE ICNP, pages 251–260, 2001.

[6] Shaikh, R.A.; Shaikh, Z.A, "*A Security Architecture for Multihop Mobile Ad hoc Networks With Mobile Agents* " 9th International Multitopic Conference, IEEE INMIC 2005.

[7] Shu-hwang Liaw , Pin-chang Su , Henry Ker-chang Chang , Erl-huei Lu , Shun-fu Pon, "*Secured Key Exchange Protocol In Wireless Mobile Ad Hoc Networks*" IEEE, 2005

[8] P. Michiardi, R. Molva, "*Ad hoc networks security,"* IEEE Press Wiley, New York, 2003.

[9] Hengjun Wang, Yadi Wang, Jihong Han, "*A Security Architecture for Tactical Mobile Ad Hoc Networks*," wkdd, pp.312-315, 2009 Second International Workshop on Knowledge Discovery and Data Mining, 2009

[10] R. Ramanathan, J. Redi and BBN Technologies, "*A brief overview of ad hoc networks: challenges and directions,"* IEEE Communication Magazine, May 2002, Volume: 40, page(s): 20-22, ISSN: 0163-6804

[11] Shuyao Yu, Youkun Zhang, Chuck Song, Kai Chen, "*A Security Architechture for Mobile Ad hoc Network"* In IEEE International Conference, Dept. of Comput. Sci., 2006,

[12] B. Wu, J. Chen, J. Wu, M. Cardei, "*A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,"* Department of Computer Science and Engineering, Florida Atlantic University, http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[13] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "*Security in mobile ad hoc networks: challenges and solutions,"* In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s): 38- 47, ISSN: 1536-1284

[14] S. Yi, P. Naldurg, and R. Kravets, "*Security-aware ad hoc is routing for wireless networks,"* In Proc. ACM Mobihoc, 2001.

[15] L. Zhou, Z.J. Haas, Cornell Univ., "*Securing ad hoc networks,"* IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044

Mr.Premchand Bhagwan Ambhore: received the B.E. Computer Science and Engineering Degree from at Government College of Engineering Amravati, India, in 1995 and M.E.Computer Science and Engineering 2004, respectively. He is currently PhD student at the Department of Computer Engineering at the Government College of Engineering Amravati, His research interest in firewall, IDS; System includes information security, and network security.

Ku.A.D.Wankhade: She is Head and Assistant professor in Information Technology at Government College of Engineering Amravati (M.S.), India. Received the B.E. Computer Science and Engineering Degree and pursuing Master of Technology in Computer Science and Engineering at the Department of Computer Science and engineering in Government College of Engineering Amravati, (M.S.), and India.

Dr.P.N.Chatur: Head, Associate Professor in Computer Engineering Government College of Engineering Amravati (M.S.), and received the B.E. Electronics Engineering Degree from at College of Engineering Badnera, Amravati, India, M.E. Electronics Engineering Degree from at Government College of Engineering, Amravati and also PhD In Computer Engineering India.

Prof.A.V.Deorankar: received the B.E. Electronics Engineering Degree from at College of Engineering Badnera, Amravati, India, M.E. Electronics Engineering Degree from at Government College of Engineering, Amravati, (M.S.) and India.