INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SURVEY: A HIGH CERTIFICATE AUTHORITY PROPOSAL FOR AUTHENTICATION IN MOBILE AD HOC NETWORKS

P.Poorniammal [1], J.Shanbagam[2], R.Umamaheswari[3]

[1]Assistant Professor, Department of Computer Science, Shri Sakthikailassh Women's College. Salem – 636 106, TamilNadu, India
[2]Assistant Professor. Department of Computer Science, Shri Sakthikailassh Women's College. Salem – 636 106, TamilNadu, India
[3]Assistant Professor, Department of Computer Science, Shri Sakthikailassh Women's College. Salem – 636 106, TamilNadu, India

Abstract: - Mobile Ad-hoc Networks (MANET) is a network consisting of a collection of nodes which can communicate with each other without help from a network infrastructure. There has been a growing interest in Mobile Ad hoc Networks (MANETs) motivated by the advances in wireless technology and the range of potential applications that might be realized with such technology. Due to the lack of an infrastructure and their dynamic nature, MANETs demand a new set of networking protocols to harness the full benefits of the versatile communication systems. The CBC-X mode is used to complete message authentication, encryption and decryption concurrently before sending message. In order to provide the data integrity, an enhanced distributed certificate authority scheme (EDCA) is developed. This scheme makes the network more secure from both inside and outside attacks. It utilizes three components namely monitoring Routing Cum Forwarding (RCF), certificate revival and certificate revocation.RCF involves detecting misbehaviors in both the routing as well as the packet forwarding in the network. Certificate revocation provides the authority to isolate the malicious nodes or regain the nodes which turn up to its best state after any attack or failure. Certificate revival scheme is used for increasing the data integrity of the packets. In this revival scheme, every legitimate node carries a certificate which is issued by certificate authority to make the communication between the nodes inside the network. For providing certificate authority, the Shamir's secret sharing scheme and modified Shamir secret scheme are used. It provides security as well as is extendable and flexible. Based on the results, it is observed that the enhanced distributed certificate authority scheme achieves more packet delivery ratio while attaining less delay and overhead than the trust based cross layer security protocol.

1. Introduction

Wireless cellular systems have been in use since 1980s.Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when users roam from one place to the other. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems.

Recent advancements such as Bluetooth introduced a new type of wireless systems known as Mobile Ad-hoc Networks. Mobile Ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. It offers quick and easy network deployment in situations where it is not possible otherwise.

Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links. Each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. [D.Kim, et.al, 2003].

A mobile ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective.

Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into reality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places.

1.1 OVERVIEW OF MANET

MANET is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. Thus, the network's wireless topology may alter rapidly and unpredictably. However, due to the lack of any fixed infrastructure, it becomes complicated to exploit the present routing techniques for network services, and this provides some huge challenges in providing the security of the communication, which is not done effortlessly as the number of demands of network security conflict with the demands of mobile networks, largely due to the nature of the mobile devices.e.g. low power consumption, low processing load.

Figure 1.1 shows that MANETs does not depend on pre-existing infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network. It is a group of autonomous mobile nodes or devices connected through wireless links without the support of a communications infrastructure. The topology of the network changes dynamically as nodes move and the nodes reorganize themselves to enable communications with nodes beyond their immediate wireless communications range by relaying messages for one another, i.e. multi hop.

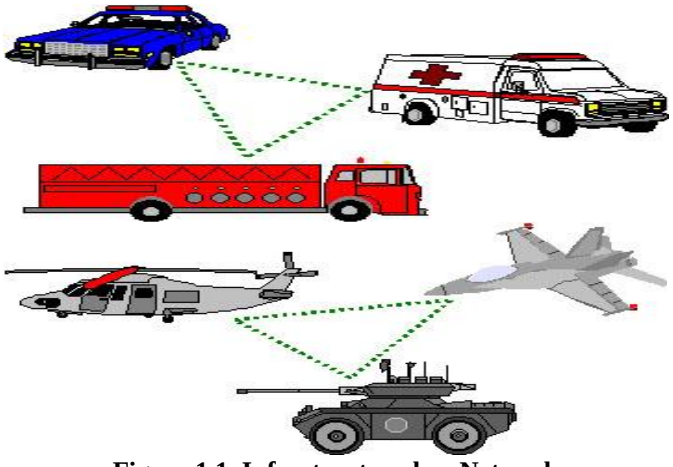

Figure 1.1. Infrastructure less Network

MANET relies on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET becomes. But supporting a MANET is a cost intensive activity for a mobile node. Detecting routes and forwarding packets consumes network bandwidth, local CPU time, memory and energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

MANET has various potential applications, which are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. Some typical examples include emergency search-rescue operations, meeting events, conferences and battlefield communication between moving vehicles and soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

1.2 Properties of Ad hoc Routing Protocols

1.2.1 Distributed operation

The protocol should of course be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks.

The difference is that nodes in an ad-hoc network can enter/leave the network very easily and because of mobility the network can be partitioned.

1.2.2 Loop free

To improve the overall performance, the routing protocol to guarantee that the routes supplied are loop-free. This avoids any waste of bandwidth or CPU consumption.

1.2.3Demand based operation

To minimize the control overhead in the network and thus not wasting network resources more than necessary, the protocol should be reactive. This means that the protocol should only react when needed and that the protocol should not periodically broadcast control information.

1.2.4Unidirectional link support

The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

1.2.5 Security

The radio environment is especially vulnerable to impersonation attacks, so to ensure the wanted behavior from the routing protocol, some sort of preventive security measures are needed. Authentication and encryption is probably the way to go and the problem here lies within distributing keys among the nodes in the ad-hoc network.

1.2.6Power conservation

The nodes in an ad-hoc network can be laptops and thin clients, such as PDAs that are very limited in battery power and therefore uses some sort of stand-by mode to save power. It is therefore important that the routing protocol has support for these sleep-modes.

1.2.7Multiple routes

To reduce the number of reactions to topological changes and congestion multiple routes could be used. If one route has become invalid, it is possible that another stored route could still be valid.

The routing protocol is saved from initiating another route discovery procedure.

1.2.8Quality of service support

Some sort of Quality of Service support is probably necessary to incorporate into the routing protocol. This has a lot to do with what these networks will be used for. It could for instance be real-time traffic support.

None of the proposed protocols from MANET have all these properties, but it is necessary to remember that the protocols are still under development and are probably extended with more functionality.

1.3 FEATURES OF AD HOC NETWORKS

1.3.1 The Media

The media in ad hoc networks is RF spectrum in space. It is not a shared link as in an Ethernet LAN or dedicated link that may be placed between two routers. The space that is used is unique to the Transmitter Receiver (TR) pairs but sufficient portions overlap with that of other TR pairs thus precluding the latter from using the media simultaneously. This interdependence between TR pair connectivity means there is no connected graph in ad hoc networks.

1.3.2 Limited Capacity

The Radio Frequency (RF) spectrum that is available for any MANET implementation is finite and limited. It is not expandable like wire line capacity. Thus, the use of the capacity it renders must be efficient. It is anticipated that the demand for the capacity in MANETs is frequently reaching saturation. Redundant exchange of common information by multiple layers should be avoided.

1.3.3 Radios Provide a Service

Radios and protocols generate information that is useful to applications. The more used capabilities are generating system synchronization and terminal positioning. The two functions are complementary and are very important in many radios and the applications that use them. If similar radios are combined with an IP protocol stack, then provisions would be needed to send this information from the radio to the application. Further, some services in MANETs can only be implemented in access protocols. The most important is prioritized and reserved access for the quality of service. Over provisioning techniques that are used elsewhere in the internet are not practical since capacity is insufficient in most MANET implementations. To access these services, applications need a way to communicate the Quality of Service requirements through the protocol stack to the MAC.

1.3.4 Similar Information Useful to Different Layers

The most obvious piece of information that is useful at multiple layers is the location of terminals. It is seen that there is a real need for applications to have location information and that it can even be generated by

the radio terminals. Location information can also support antenna pointing, transmission scheduling, routing, network management, and spectrum management. Congestion information at nodes and in spatial regions is useful for access protocols, routing, transport control, call admission and network management. Node mobility is useful to applications, routing, antenna pointing and scheduling. The energy status of nodes is useful to routers so paths can be chosen to avoid energy deficient nodes and to access protocols so that they can choose appropriate dozing strategies. Transmission schedules created by access protocols are useful to routing protocols so it is easy to know how resources have been allocated and can route through regions that are adequately provisioned.

1.3.5 Distributed Information Exchange

In addition to sharing information, many protocols of all types have a need to distribute information to support their operation. Routing protocols are obvious. Access protocols that use multiple channels need mechanisms to disseminate the use of channels. Access protocols may also require the dissemination of access schedules. Network and spectrum management protocols are useful to MANETs and require information distribution to function. Within the homogenous environment of a MANET, it is feasible to combine this distribution within a single protocol. Since multiple layers require common information, it is also more efficient.

1.3.6 Cross-Layer Decisions

Many proposed MANET implementations benefit from cross-layer decisions, especially between transport control, routing, and access protocols. Disruption Tolerant Networking (DTN) proposes a store and forward technique where proxies at the partition edges can store communications until the partitions are closed. The choice of the proxy is made based on knowledge of the networks current and anticipated connectivity, information that is generated by the routing protocols.

1.4 Main Characteristics of Ad Hoc Networks

1.4.1 Dynamic topology

Hosts are mobile and can be connected dynamically in any arbitrary manner. Links of the network vary and are based on the proximity of one host to another one.

1.4.2 Autonomous

No centralized administration entity is required to manage the operation of the different mobile hosts.

1.4.3 Bandwidth constrained

Wireless links have a significantly lower capacity than the wired ones; they are affected by several error sources that result in degradation of the received signal.

1.4.4 Energy constrained

Mobile hosts rely on battery power, which is a scarce resource; the most important system design criterion for optimization may be energy conservation.

1.4.5 Limited security

Mobility implies higher security risks than static operations because portable devices may be stolen or their traffic may cross insecure wireless links.

1.5 APPLICATIONS OF MANETS

As MANETs do not require a fixed infrastructure they have a number of benefits and versatility for certain environments and applications:

• Military Use – providing communication when a network is not available or not considered to be secure or safe to use an existing infrastructure.
• Search and Rescue – providing a communication network when existing network is not available or destroyed.
• Sensor networks – allowing a large number of sensors to communicate that may not be in the easiest of locations to place on a traditional network.

2. LITERATURE SURVEY

The literature survey mainly focuses on the existing challenges, threats and the earlier methodologies followed to overcome certain problems.

2.1 General

Farooq Anjum [Farooq Anjum and Dhanant Subhadarabandhu, 2003] has proposed an initial approach in which NID (Network Intrusion Detection) deals with information passing on the entire network between any pair of communicating hosts. while it is very good at detecting unauthorized outsider access, bandwidth theft, DOS, it is incapable of operating in encrypted networks and in high-speed networks. In addition, NID is effective when the network has certain chokepoints at which detection can be done. As is obvious the NID approach is not effective in ad-hoc networks on account of absence of any choke points in such networks. As a result one might have to depend on having the intrusion detection mechanisms on all or some of the hosts in the system.

The absence of any choke points in ad hoc networks leads to introduction of intrusion detection mechanisms on all nodes. A trust based packet forwarding scheme in MANETs without using any centralized infrastructure is used. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding the intermediate node is marked as malicious.

The objective of an intruder in any network is to have malicious packets delivered to the endpoint of interest resulting in harm to the endpoint. The intrusion detection system tries to detect the occurrence of these packets while in transit between the intruder (source of packets) and the endpoint of interest (destination of packets) so as to take proper corrective action. It is here that the routing protocols have an effect on the intrusion detection capabilities of the network.

Routing protocols determine the path taken by packets traversing between a source and destination node. And if individual hosts have to be able to determine intrusions based on attack signature recognition, it would be necessary for the packets in a given flow (at least all the packets that constitute the attack) to pass through a node that is part of the intrusion detection subsystem. But this would not always be possible for nodes other than the destination node on account of the fact that the packets might traverse different paths. Mobility would cause the path of packets to change and intruders can take advantage of this. In addition, in ad-hoc networks with many nodes there might be redundant paths between a given source destination pair. The routing protocols might switch packets between these paths. Due to this, it might be difficult to detect attacks knowing their signatures even when mobility is not allowed.

In the proposed protocol, by dynamically calculating the nodes trust counter values, the source node can be able to select the more trusted routes rather than selecting the shorter routes. This protocol marks and isolates the malicious nodes from participating in the network. So the potential damage caused by the malicious nodes is reduced. The proposed protocol makes changes to the AODV routing protocol. An additional data structure called Neighbor's Trust Counter Table (NTT) is maintained by each network node.

Anand Patwardhan [Anand Patwardhan and Jim parker, 2005] proposed a Collaborative Intrusion Detection Systems (IDS) is performing best in a densely populated MANET with limited mobility, and performing worse in a sparsely populated MANET with significant mobility. The effectiveness of collaborative IDS also depends on the amount of data that can be collected by each node. The longer the nodes are members of the MANET, the greater the availability of meaningful data for further analysis. The degree of mobility of each node in the network has a significant impact on its effectiveness. In a MANET with a high degree of mobility, if the number of routing error messages causes by legitimate reasons far exceeds the number of routing error messages caused due to the presence of malicious nodes, the effectiveness or benefit of such an IDS may be minimal.

Using the Shamir secrecy model secrecy among a set of nodes from N nodes such that at least k nodes are needed to reconstruct the secrecy among the nodes is provided. A sharing key among subset of k shares out of n shares. Modified Sharing Scheme with Redundancy helps in reconstructing shared keys even if the minimum set of necessary key (k) is not available during reconstruction. For this, it is provided with q shares of value to each node against the traditional value which is 1 shared value for each node. Hence it overcomes the IDS method to perform densely populated MANET with limited mobility.

The AODV protocol is comprised of two basic mechanisms, i.e., route discovery and maintenance of local connectivity mechanisms. The Route Discovery mechanism is employed in an "Ad Hoc, On Demand" fashion. The source node S the device that requests communication with another member of the MANET referred to as destination D initiates the process by constructing and broadcasting a signed Route Request message RREQ. The format of the RREQ message differs. An AODV message contains the RSA (Rivest, Shamir, and Adleman) public key of the source node S and that it is digitally signed to ensure the node's authentication and message integrity. Upon receiving a RREQ message, each node member of the MANET authenticates the source node S and verifies message integrity by checking the IP address using the same secure bootstrapping algorithm and by verifying the signature against the provided public key.

Upon successful completion of the verification process, the node updates its routing table with the source and router IP addresses, if any, and then checks the destination IP address. If the message is not addressed to it, it rebroadcasts the RREQ. If the current node is the destination, it constructs a Route Reply message (RREP) addressed to the source node S. The message is signed and it includes the destination's public key. The destination node D unicasts the RREP back to the neighboring node that initially forwarded the RREQ. The neighbor address is retrieved from its own routing table, under source address.

Upon receiving a RREP, any routing node verifies the destination D's IP address and signature against the included public key, updates its own routing table with the destination D and router addresses, if any, and unicasts the message to the router listed in its routing table under the source S address entry. If the route entry to S does not exist or has expired, the message is dropped and an error message is sent to all affected neighbors. If the source node does not receive any reply in a predetermined amount of time, it rebroadcasts new route requests.

In the proposed scheme, monitoring of routing packets and forwarding packets are done by the proposed work of trust based packet forwarding scheme by punishing or rewarding the nodes with decreasing or increasing a trust counter. Each intermediate node marks the packets by adding its hash value and forwards the packet towards the destination node. The destination node verifies the hash value and check the trust counter value. If the hash value is verified, the trust counter is incremented, otherwise it is decremented. If the trust counter value falls below a trust threshold, the corresponding the intermediate node is marked as malicious. The incentive value provided to each successful node helps in determining the trustworthiness of the node and shows the misbehaving nodes apart from the network. To increase the integrity of these forward packets certification revival scheme is introduced using redundancy to guarantee that genuine nodes can continue to stay in the network by revival of their certificates along a periodical time period.

a. SECURE DATA COMMUNICATION

The problem of secure and fault-tolerant communication in the presence of adversaries across a multihop wireless network with frequently changing topology is addressed [Panagiotis Papadimitratos, et.al, 2006]. To effectively cope with arbitrary malicious disruption of data transmissions, evaluation of the Secure Message Transmission (SMT) protocol and its alternative, the Secure Single Path (SSP) protocol. Among the salient features of SMT and SSP is their ability to operate solely in an end-to-end manner and without restrictive assumptions on the network trust and security associations.

As a result, the protocols are applicable to a wide range of network architectures. The highly reliable communication can be sustained with small delay and small delay variability, even when a substantial portion of the network nodes systematically or intermittently disrupt communication. SMT and SSP robustly detect transmission failures and continuously configure their operation to avoid and tolerate data loss, and to ensure the availability of communication. This is achieved at the expense of moderate transmission and routing overhead, which can be traded off for delay. Overall, the ability of the protocols to mitigate both malicious and benign faults allows fast and reliable data transport even in highly adverse network environments.

Secure Message Transmission (SMT) Protocol and Secure Single Path (SSP) protocol

A novel, general solution, proposed Panagiotis Papadimitratos [Panagiotis Papadimitratos, et.al, 2006] by tailored to the MANET requirements, to effectively and efficiently secure the data transmission phase, there are two schemes. One is the Secure Message Transmission (SMT) and another one is Secure Single-path (SSP) protocols. The goal of SMT and SSP is not to securely discover routes in the network. They assume that secure discovery of routes has been already performed, although routes may not be free of adversaries.

Then, the goal of SMT and SSP, whose basic ideas is to secure the data transmission.SMT and SSP operate without restrictive assumptions on the network trust and security associations, promptly detect and avoid non-operational or compromised routes, tolerate loss of data and control traffic, and adapt their operation to the network conditions. Their main difference is that SMT utilizes multiple paths simultaneously, in contrast to the single-path operation of SSP.

To analyze the operation of the two protocols, the details and analyses of their mechanisms is presented, including their interaction with the route discovery and the maintenance of multiple paths, the path-rating algorithm and a decision-theoretic model for the selection of its parameters, an algorithm to estimate the probability of path survival, and three alternative algorithms for automatic configuration of multipath transmissions. The performance of SMT and SSP in a realistic network, integrating SMT and SSP with the Secure Routing Protocol (SRP) and the IEEE 802.11 as the data link protocol, and investigate the interaction of SMT and Transmission Control Protocol (TCP).

SMT and SSP can support applications with differing objectives and operate in a wide range of network conditions. The simultaneous usage of multiple paths and the dispersion of transmitted data enable SMT to support real-time traffic or other time sensitive applications, even in highly adverse environments. In addition to highly reliable data delivery, SMT achieves low delay and low delay variability, at the expense of multipath transmission overhead.

The overall overhead increase is relatively low when real-time traffic comprises a small fraction of the overall network traffic. In resource-constrained environments, or when the supported application does not impose delay constraints, SSP is the appropriate lightweight alternative to SMT. SSP can provide secure and highly reliable data communication, trading off delay and delay variability for network overhead.

Moreover, it is found that node mobility can be both detrimental and beneficial in adversarial environments, in contrast to the established belief that mobility impairs MANET communication. It is identified that increased network load as a factor which can magnify the impact of attacks by relatively weakening the fault detection mechanisms. SMT combined with TCP to provide flow control, and investigate their interaction. SMT thwarts malicious and benign faults, while TCP adjusts the end-to-end data rate according to the network conditions.

Finally, the SMT persistent disruption of the data transmission is more effective, from the adversary's point of view, than intermittent or "low-profile" attacks. Overall, the experiments show that SMT and SSP are versatile, effective, and efficient in a wide range of settings.

2.2- MIDS ATTACK

Attacks in Mobile Adhoc networks [S.Madhavi and Tai, 2008] can be categorized as follows.

1. Unfair use of the transmission channel (ATTACK1).
2. Anomalies in Packet Forwarding (ATTACK2).

2.2.1 Unfair use of the transmission channel (ATTACK1)

A node can prevent other nodes in its neighborhood from getting fair share of the transmission channel. This misbehavior can be considered as DoS attacks against the competing neighbors in a contention-based network since the competing neighbors are deprived of their fair share of the transmission channel. Some of the possible methods for unfair use of the transmission channel are as follows:

2.2.1.1 Ignoring the MAC protocol

Protocols like 802.11 uses RTS (Request To Send) and CTS (Clear To Send) to notify the immediate neighbors of how long the transmission channel will be reserved for the successful transmission. Such methods minimizes collisions among competing neighbors and try to ensure that all the competing neighbors can get some share of the common channel. But a misbehaving node can generate RTS/CTS at an unacceptable rate by ignoring the back off mechanism. Hence the competing neighbors cannot get an adequate share of the transmission channel. This imposes a long delay at the output queues and they finally time out and get removed.

If the indicated duration (Ti) is less than the actual duration (Ta) taken for successful transmissions, the transmission channel will remain occupied for an additional period, Ta - Ti. The competing neighbors may not be aware of this additional hidden period. Therefore, neighbors trying to access the channel within the hidden period are likely to face unexpected collisions, increase their back off intervals and hence may not get their share of the channel.

2.2.1.2 Jamming the transmission channel with garbage

Garbage can consist of packets of unknown formats, violating the proper sequence of a transaction (e.g. sending a data packet without exchanging RTS and CTS) or simply random bits used as static noise by misbehaving nodes. Garbage data may result in too many collisions, may consume a significant part of the available Channel capacity or both. Consequently, legitimate neighbors may not be able to access the channel properly when needed.

2.2.1.3 Ignoring the bandwidth reservation scheme

Nodes in a multi-hop wireless network reserves a slot for transmission channel before initiating a flow. If there is not enough bandwidth, new flows should not be admitted so that existing flows are not choked.

A misbehaving node may not abide by this rule and try to push out packets when there is not enough bandwidth left. As a result legitimate nodes may not get fair share of the transmission channel.

2.2.1.4 Malicious flooding

Deliver unusually large amount of data of control packets to the whole network or some target nodes.

2.2.1.5 Network Partition

A connected network is partitioned into k (k >= 2) sub networks where nodes in different sub networks cannot communicate even through a route between them actually does exist.

2.2.1.6 Sleep Derivation

A node is forced to exhaust its battery power.

.

3. SECURITY REQUIREMENTS

3.1 Availability

Sensors are strongly constrained by many factors, e.g., limited computation and communication capabilities [Shinqun Li, et.al, 2007]. Energy is another extremely limited resource in large scale wireless sensor networks. Moreover, wireless sensor networks are vulnerable to various attacks. The adversary is assumed to possess more resources such as powerful processors and expensive radio bandwidth than sensors. Equipped with richer resources, the adversary can launch even more serious attacks such as DoS attack, resource consumption attack and node compromise attack.

3.1.1 Confidentiality

Confidentiality, integrity and authentication security services are required to thwart the attacks from adversaries mentioned in the above section. These security services are achieved by cryptographic primitives as the building blocks. Confidentiality means that unauthorized third parties cannot read information between two communicating parties. Privacy communication should be kept confidential because wireless sensor networks are easy for eavesdropping. Generally, encryption is the most widely used mechanism to provide confidentiality.

The performance of public key computation on MICA2 platforms is quite reasonable for next generation sensor networks, i.e., the time for computing 1024 bit RSA with public key as 3 is 14.5 seconds and much longer for larger exponents. Malan et al. presented an implementation of Elliptic Curve Cryptography

(ECC) over F2p on MICA2 mote. It is demonstrated that public keys can be generated within 34 seconds. Gupta et al. implemented an end-to-end security architecture for MICA2 platform. Their work shows that ECC makes public-key cryptography feasible on these resource constrained devices. It also allows one to create a complete secure web server stack including SSL, HTTP and user application on these platforms.

An 8-bit Berkeley/Crossbow Mica2 mote platform can complete a full SSL handshake in less than 4 seconds (session reuse takes under 2 seconds) and transfer 450 bytes of application data over SSL in about 1 second. The above evidences show that it is quite promising that asymmetric cipher can be used in future version of sensors. And one can also expect the capability increasing of sensor node from Moore's Law. However, cryptography will cause increased overhead in the length of messages sent as well as in extra demands on the processor and RAM (Random Access Memory). The message length expansion would decrease message throughput and increase latency. It would also cause increased power consumption.

Transmitting one bit consumes about as much power as executing 800-1000 instructions. Any message expansion caused by security mechanisms will result in extra cost consumption. Considering the extreme resource limitations in wireless sensor networks and the strength of the security mechanisms, it is desired to carefully design security mechanisms.

3.1.2 Integrity and authenticity

Integrity means the message one receives is exactly what was sent and it was unaltered by unauthorized third parties or damaged during transmission. Wireless sensor networks use wireless broadcasting as communication method. Thus it is more vulnerable to eavesdropping and message alteration. Measures for protecting integrity are needed to detect message alteration and to reject injected message. Authentication ensures that the sender was entitled to create the message and that the contents of the message have not been altered.

In the public key cryptography, digital signatures are used to seal a message as a means of authentication. In the symmetric key cryptography, MACs are used to provide authentication. When the receiver gets a message with a verified MAC, it is ensured that the message is from an original sender.

4. EFFICIENT LINK LAYER SECURITY SCHEME

Due to the rapid development of wireless communications and embedded computing technologies, wireless sensor networks offer a wide range of applications, ranging from battlefield target tracking, environmental monitoring, hospital patient data gathering, to traffic motoring, to name a few [Shinqun Li, et.al, 2007].

Generally, a wireless sensor network consists of a set of distributed sensor nodes, each is equipped with a sensor to provide certain information such as temperature, light, moisture, and motion, depending on applications. While wireless sensor networks are quite useful in many applications, it appears that they are more vulnerable to attacks than wired networks: an attacker can easily eavesdrop on, inject or alter the data transmitted between sensor nodes.

Thus security must be ensured in mission-critical sensor applications such as in military section. Providing security in wireless sensor networks turns out not trivial due to the fact sensor nodes are strongly limited by resources such as power, bandwidth, computation, and storage. Efficiency is thus a crucial desideratum, as sensors are usually deployed in remote area for a long time.

Security issues in wireless sensor networks are explored, and in particular, an efficient link layer security scheme inspired by the proposal of TinySec. To meet the desideratum of minimizing computation and communication overhead, our focus is the CBC-X mode Encryption/Decryption algorithm, which enables encryption/decryption and authentication of packets a one-pass operation. In particular, the main contributions are as follows:

It is presented with an efficient link layer security scheme that attains confidentiality and authentication of packets in wireless sensor networks. Security services are provided transparently to the upper (link) layers of the protocol stack.

It is devised with a CBC-X mode symmetric key mechanism to implement our link layer security scheme. Encryption/Decryption and authentication operations are combined as a one-pass operation, which reduces half of the computational overhead of computing them separately.

The padding technique makes the scheme have no cipher text expanding for the transmitted data payload. Hence it significantly reduces communication overhead. Clearly, the CBC-X mode symmetric key mechanisms in combination with the padding technique enable the scheme to substantially save power consumption of sensor nodes.

By using the CBC-X mode encryption mechanism and the padding techniques, the scheme completes encryption and authentication without cipher expanding. Therefore, it can significantly decrease message transmission energy which is of great important to wireless sensor networks. Experiments show that the CBC-X mode encryption mechanism and the padding techniques is more efficient than TinySec.

5. SECURITY GOALS

5.1 Outsider vs. insider nodes

An outsider node is a node that is not an authorized member of the MANET whereas an insider node is an authorized member [Akbani R, et.al, 2008]. For instance, in a military setting each authorized soldier might possess a signed certificate from a trusted third party granting membership permission in the MANET. Such a node is an insider node. Any node not possessing such a certificate or possessing a revoked certificate is considered an outsider node. In essence, attacks are thwarted from outsider nodes. Detecting the attacks from insiders is left to the Intrusion Detection Systems. However, a foundation on which a response system can be based by providing the capability to effectively cut off a compromised insider from the MANET is provided. In addition, HEAP offers some level of protection against insiders who try to forge packets and impersonate other insiders. But because insiders already have access to the MANET, it is easy for them to launch more sophisticated attacks rather than simply trying to forge packets. Following is the list of keys security goals in defending the underlying network against outsider nodes.

Any packet transmitted by an outsider node should be immediately dropped by the receiving insider node at the first hop with a very high probability. In other words, packets sent by outsiders should not be allowed to propagate through the MANET. By fulfilling this requirement, it can be successfully guarded against a myriad of attacks by the outsider, such as DoS attacks that attempt to flood the network, wormhole attacks, man-in-the-middle, SYN flooding etc. This is because it is by effectively disabling the outsider's ability to route any packets to any node that is not its neighbor. Even a neighboring node drops packets from the outsider. However, this requirement dictates that every packet is authenticated at every hop, which in turn means that the authentication mechanism should be extremely efficient.

The outsider node is assumed to have the capability to spoof its identity, such as spoofing its IP (Internet Protocol) and MAC addresses to impersonate an insider node. The reliability on these markers to verify the origin of a packet cannot be done.

The outsider is assumed to have access to the wireless channel so it can eavesdrop on legitimate traffic. If the traffic is supposed to remain confidential, end-to-end encryption should be used to protect it. However, it is assumed that the encrypted traffic and any associated MAC tags are visible to the outsider.

If a third party Intrusion Detection System (IDS) discovers an insider to be compromised, the ability to exclude that insider from propagating should be present

Any more packets within the MANET. Certificate Revocation Lists (CRL) may be used to revoke the certificates of compromised insiders.

5.2 ANALYSIS OF KNOWN SCHEMES

Several threshold RSA signatures are proposed in literature that might be used to construct the group access control protocol [Nitish Saxena, Gene, 2007]. Unfortunately, none of these schemes are directly applicable.

Schemes by Frankel and Rabin

The currently known provably secure threshold RSA signature schemes, two schemes by Frankel and a scheme by Rabin are not applicable for access control in ad hoc groups. In particular, the RSA signature scheme of is practical only for small groups, while in the other two provably secure threshold RSA schemes known today (which employ additive secret sharing as opposed to polynomial secret sharing) the members participating in the threshold signature protocol need to reconstruct the secret shares of the group members that are currently inaccessible to them. In this way both protocols essentially equate a temporarily inaccessible group member with a corrupt one, whose secrets might just as well be fabricated. This is an undesirable feature for asynchronous ad hoc groups where members are often inaccessible to one another. In such settings, it needs to enable isolated but large enough subgroups of members to operate without reconstructing everyone else secrets.

Scheme by Shoup

Another well-known and more recent provably secure threshold RSA scheme was proposed by Shoup. This scheme is more elegant than the above ones because the signature generation and verification is fully non-interactive and it also avoids the inaccessibility problem by employing the polynomial (t, n) secret sharing of shamir. However, since the secret sharing is performed over secret modulo/ (N) (unlike over publicly known integers in the schemes discussed above), it is not possible for the group members to provide a new member with its secret share. Moreover, Shoup's scheme requires a trusted dealer to generate the RSA keys, which is an undesirable feature in ad hoc groups. Boneh and Franklin developed a method to generate an RSA modulus in a distributed fashion. Alas, it might not be possible to use this method, since Shoup's scheme requires that the common RSA modulus N be a product of two safe primes. Furthermore, that using any method to generate RSA keys in a distributed manner involves prohibitively high communication and/ or computation overhead which severely impact the practicality of such techniques in many group setting such as MANETs.

Scheme by Kong

In an effort to mitigate the above problem of the known threshold RSA signatures, Kong proposed a new threshold RSA scheme, geared toward providing security services in MANETs. Unfortunately, this scheme,

contrary to what its authors claimed, is neither robust (i.e., it cannot tolerate malicious group members) nor secure.

In this, the utility of various existing threshold signature schemes in building distributed access control mechanisms for ad hoc groups are explored. First none of the threshold (or proactive) RSA signature schemes in the literature are applicable for this purpose. Next, it is implemented with three access control mechanisms based on discrete-logarithm based threshold signatures, Threshold Digital Signature Algorithm (TS-DSA), Threshold Schnorr (TS-Sch) and Threshold BLS (TS-BLS), and evaluated them in a real MANET setting. Based on the evaluation, it is concluded that overall TS-Sch is the most efficient mechanism, followed by TS-BLS and TS-DSA.

6. FULLY DISTRIBUTED CERTIFICATE AUTHORITY

Partially distributed certificate authority scheme requires the use of specialized high energy nodes. This assumption is not always valid in an ad hoc network and hence becomes a bottleneck. To overcome this bottleneck, Luo and Lu proposed a fully distributed CA solution. It uses a (k, n) threshold scheme in order to distribute an RSA certificate-signing key to all the nodes in the network. If there are n nodes in a network, the CA (Certificate Authority) private key is divided into n shares. A minimum of k shares is required to recreate the CA key. This eliminates the necessity of having specialized high-energy nodes. It also uses proactive secret sharing mechanisms to protect against the compromise of the CA's signing key. When an intruder enters the network and compromises one node, it becomes as good as a valid node. To overcome this problem, an intrusion detection system [Deepti Joshi, et.al, 2005] is required to be present in the network. This intrusion system identifies the misbehaving/compromised nodes and removes them from the network. The services provided by the CA are share initialization, share update, certificate issuing, certificate renewal, and certificate revocation. The services provided by the CA are summarized.

6.1 Share update

Proactive secret sharing is used and the shares are updated periodically in order to make the protocol robust. A polynomial fupdate(x) is added to the existing sharing polynomial and a new sharing polynomial fnew(x) is formed. The shares are recalculated and distributed.

6.2 Certificate issuing

In a distributed CA system, the certificates are not issued. The certificates initially created, are only maintained. The dealer is responsible for initializing, registering, and certifying new nodes in the network.

6.3 Certificate renewal

Whenever a node p has to renew its certificate, it sends a request for renewal to a coalition of k nodes. Each node then checks its CRL to determine whether the old certificate has been revoked. If it has been revoked, then the nodes deny the request. Otherwise they agree to serve the request and a new partial certificate (certi) is generated and sent.

6.4 Certificate revocation

If a certificate is revoked, the public key interface provides a mechanism to inform users about the revoked certificate. Most common method used is Certificate Revocation List (CRL). A CRL consists of a list of revoked certificates. Every node maintains a CRL. If a node discovers that any other neighboring node is misbehaving, it adds that node to its certificate revocation list (CRL) and floods an accusation against the node in the network. The nodes which receive this broadcast check whether the node which broadcasted this CRL is a part of its own CRL. If it is, then this broadcast is ignored, otherwise it is accepted and changes are made to the CRL.

7. CONCLUSION

Mobile Ad-hoc Network (MANET) is an indivisible part for communication of mobile devices. It is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. Communication in MANET is done via multi-hop paths. Lot of challenges are there in this area: MANET contains diverse resources; the line of defense is very ambiguous; Nodes operate in shared wireless medium; Network topology changes unpredictably and very dynamically; Radio link reliability is an issue; connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no stationary infrastructure. Each node in MANET acts a router that forwards data packets to other nodes. Therefore, selection of effective, suitable, adaptive and robust routing protocol is of utmost importance.

In this research work, a trust based cross layer security protocol is developed for authentication. It includes trust based packet forwarding scheme which is designed for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious

REFERENCES

1. D. Kim, J. Garcia and K. Obraczka (2003), "Routing Mechanisms for Mobile Ad Hoc Networks based on the Energy Drain Rate", IEEE Transactions on Mobile Computing. Vol.2, No. 2, 2003, pp.161-173.
2. H. Miranda and L. Rodrigues (2002), "Preventing selfishness in open mobile ad hoc networks", in Proc. of the Seventh CaberNet Radicals Workshop, pp.1-11.
3. S. Marti, T. Giuli, K. Lai, and M. Baker (2000), "Mitigating routing misbehavior in mobile ad hoc networks", In Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), pp.1-11.
4. L. M. Feeney and M. Nilsson (2001), "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment", In IEEE INFOCOM, pp.1-10.
5. M. Jakobsson, J.P. Hubaux, and L. Buttyan (2003), "A micropayment scheme encouraging collaboration in multi-hop cellular networks", In Proc. of Financial Crypto 2003, pp.1-19.
6. L. Buttyan and J-P. Hubaux, "Security and cooperation in wireless networks", available at http://secowinet.ep.ch/.
7. Johnson, D (1994), "Routing in Ad Hoc Networks of Mobile Hosts", Proc. of the Workshop on Mobile Computing Systems and Applications, pp. 158-163.
8. Perkins, C., and Royer, E. (1999), "Ad hoc On-Demand Distance Vector Routing", Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100.
9. Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar (2003), "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols" , in proceedings of IEEE 58th Conference on Vehicular Technology, pp.1-5.
10. Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis (2005), "Secure Routing and Intrusion Detection in Ad Hoc Networks", Third IEEE International Conference on Pervasive Computing and Communications, pp.1-12.
11. Chin-Yang Henry Tseng (2006), "Distributed Intrusion Detection Models for Mobile Ad Hoc Networks" University of California at Davis Davis, CA, USA, pp.1-144.
12. Tarag Fahad and Robert Askwith (2006),"A Node Misbehavior Detection Mechanism for Mobile Ad-hoc Networks", in proceedings of the 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, pp.1-6.
13. Panagiotis Papadimitratos, and Zyg munt J. Haas (2006), "Secure Data Communication in Mobile Ad Hoc Networks", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2,pp.343-356.
14. Ernesto Jimenez Caballero (2006), "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem", Seminar on Network Security, pp.1-5.
15. Yanchao Zhang, Wenjing Lou, Wei Liu, and Yuguang Fang (2007), "A secure incentive protocol for mobile ad hoc networks", Wireless Networks (WINET), Vol.13, No. 5,pp.1-11.
16. Liu, Kejun Deng, Jing Varshney, Pramod K. Balakrishnan and Kashyap (2007), "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, pp.1-35.
17. Li Zhao and José G. Delgado-Frias (2007), "MARS: Misbehavior Detection in Ad Hoc Networks", In proceedings of IEEE Conference on Global Telecommunications Conference, pp.941-945.
18. A.Patwardhan, J.Parker, M.Iorga, A. Joshi, T.Karygiannis and Y.Yesha (2008), "Threshold-based Intrusion Detection in Ad hoc Networks and Secure AODV", Elsevier Science Publishers B. V. , Ad Hoc Networks Journal (ADHOCNET), pp.1-37.
19. S.Madhavi and Dr. Tai Hoon Kim (2008) "AN INTRUSION DETECTION SYSTEM IN MOBILE ADHOC networks", International Journal of Security and Its Applications Vol. 2, No.3, pp.1-16.
20. Afzal, Biswas, Jong-bin Koh,Raza, Gunhee Lee and Dong-kyoo Kim (2008), "RSRP: A Robust Secure Routing Protocol for Mobile Ad Hoc Networks", In proceedings of IEEE Conference on Wireless Communications and Networking, pp.2313-2318.

21. Bhalaji, Sivaramkrishnan, Sinchan Banerjee, Sundar, and Shanmugam(2008), "Trust Enhanced Dynamic Source Routing Protocol for Ad hoc Networks", In proceedings of World Academy Of Science, Engineering And Technology, Vol. 36, pp.1373-1378.

22. Meka, Virendra, and Upadhyaya (2006), "Trust based routing decisions in mobile ad-hoc networks", In Proceedings of the Workshop on Secure Knowledge Management, pp.1-6.

23. Muhammad Mahmudul Islam, Ronald Pose and Carlo Kopp (2004), "A Link Layer Security Protocol for Suburban Ad-Hoc Networks", in proceedings of Australian Telecommunication Networks and Applications Conference, pp.1-4.

24. Shiqun Li, Tieyan Li, Xinkai Wang, Jianying Zhou and Kefei Chen (2007), "Efficient Link Layer Security Scheme for Wireless Sensor Networks", Journal of Information And Computational Science, Vol.4, No.2,pp. 553-567.

25. S. Schmidt, H. Krahn, S. Fischer, and D. Watjen (2004), "A Security Architecture for Mobile Wireless Sensor Networks", In proceedings of First European Workshop on Securssity in Ad-Hoc and Sensor Networks (ESAS 2004), pp.166-177.

26. S. R. Murthy and B. S. Manoj (2004), "Ad Hoc Wireless Networks: Architectures and Protocols", Prentice Hall.

27. P. Papadimitratos and Z. J. Haas (2003), "Secure Link State Routing for Mobile Ad Hoc Networks," in Proc. of the IEEE workshop on Security and Assurance in Ad hoc Networks,pp.1-5 .

28. Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain (2009), "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment**",** European Journal of Scientific Research, Vol.32, No.3, pp.430-443.

29. Mark E. Orwat, Timothy E. Levin, and Cynthia E. Irvine (2008), "An Ontological Approach to Secure MANET Management", In Proceedings of the Third International Conference on Availability, Reliability and Security, pp.787-794.

30. Sreedhar, S. Madhusudhana Verma and N. Kasiviswanath (2010), "A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols", International Journal on Computer Science and Engineering, Vol. 02, No. 02, pp. 224-232.