International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 4, July-August 2014 **ISSN 2278-6856**

Secure Retrieval of Information for MANETs using Self Manageable Clustering

Mr. Praveen Tripathi[1], Mr. B. K. Yadav[2]
[1]Scholar, M.Tech(CSE)
GRD Institute of Management & Technology
Rajpur Road, Dehradun

[2]Assistant Professor (CSE)
GRD Institute of Management & Technology
Rajpur Road, Dehradun

Abstract
Networking technology is developed for connecting computers together to facilitate its users. We use the internetworking either using wired or wireless networks topologies. But, in the current scenario, as the size of the network has been increased as the number of nodes are increasing every moment, there is still a challenge for us to develop such technologies which will run smooth even if the load is increased. To achieve it there were various technologies emerged starting from dial-up technologies, DSL technologies and so on. Now-a-days we are almost all of the time are surrounded by the various signals generated by various technologies viz. Bluetooth signals, wifi signals and other adhoc signals etc. MANETs are one of the networking model in this area of networking which is getting very popular in terms of entertainment, education and businesses as well. But security on the existing system is still a challenge for its users. There are so many attacks which can disturb the basic functionality of the system by taking control over few components. Moreover, it is also possible to masquerade the existing system and stealing the data on fake request. Today, data security is one of the big issue. This paper focuses on few existing systems and provides a refined model after observing the present anomalies in the existing system. As a result one of the model will be proposed for better applicability.

Keywords: MANETs, GSM , UMTS , WLL WLAN, Security attacks, SYN Flooding Attack, Session hijacking, secure multicasting, Threshold of battery, Lagrange's Interpolation.

1. INTRODUCTION

As we know that networking technology is developed for connecting computers together to facilitate its users. We use the internetworking either using wired or wireless networks topologies. But, in the current scenario, as the size of the network has been increased as the number of nodes are increasing every moment, there is still a challenge for us to develop such technologies which will run smooth even if the load is increased. To achieve it there were various technologies emerged starting from dial-up technologies, DSL technologies and so on. Now-a-days we are almost all of the time are surrounded by the various signals generated by various technologies viz. GSM, UMTS, WLL, WLAN etc. MANETs (Mobile Adhoc Networks) are one of the networking model in this area of networking which is getting very popular in terms of entertainment, education and businesses as well. But security on the existing system is still a challenge for its users. There are so many attacks which can disturb the basic functionality of the system by taking control over few components. Moreover, it is also possible to masquerade the existing system and stealing the data on fake request. Today, data security is one of the big issue. This paper focuses on few existing systems and provides a refined model after observing the present anomalies in the existing system.

2. ROLE OF NETWORK IN COMMUNICATION

The use of the internet and its applications became ubiquitous. A need for providing network access to entities while not physically attached to the wired network arose. To enable this wireless networking was developed, providing devices with methods to connect to a wired Network using radio wave technologies through wireless access points. Simultaneously telephone networks were going a similar transformation. Cellular network technologies were developed to allow mobile phones to connect via base stations and communicate in a circuit switched environment. In general, mobile wireless networks can be classified into two types:

2.1 Infrastructure Based Networks

Wireless mobile networks have traditionally been based on the cellular concept and Relied on good infrastructure support, in which mobile devices communicate with Access points like base stations connected to the fixed netwo rk infrastructure (Figure 1.1). Typical examples of this kind of wireless networks are GSM , UMTS , WLL WLAN etc.

2.2 Infrastructure less mobile network

Wireless nodes can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure (Figure1.2) This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on

rapid configuration of a wireless connections on-the-fly.
Wireless mobile networks have traditionally been based on the cellular concept and Relied on good infrastructure support, in which mobile devices communicate with Access points like base stations connected to the fixed netwo rk infrastructure (Figure 1.1). Typical examples of this kind of wireless networks are GSM , UMTS , WLL WLAN etc.

2.3 No fixed topology

The network topology in an ad-hoc wireless network is highly dynamic due to the mobility of nodes. They may move in and out of the range of each other. The topology changes if one of those events happens, e.g. the route table and the multicast table must be changed accordingly. This increases the difficulty to management the network.

2.4 Limited energy

Mobile devices use generally battery power, which is exhaustible. In order to save the energy, some devices may be in sleepy mode. During this period they are possibly not reachable, or do not process traffic, or change to normal mode with latency. On one hand most wireless devices use spread spectrum communications, which need the receiving and decoding of the signal. These are expensive operations that consume much power. On the other hand some complex computations are also very expensive, for example modular exponentiation, which makes it difficult to implement the public key systems for ad hoc networks.

2.5 Limited processor

Most mobile devices have cheap and slow processors, because fast processors cost much more and the size should be as smart as possible to make it easy to take. Hence it takes2 Ad Hoc Networks much time to operate some complex computations. The most PDAs have currently processors of several hundred MHz.

2.6 Limited storage capability and other resources

Because of the size and cost restrictions, the most mobile devices are equipped with limited storage capability. For example, iPAQ hx4700 series of HP have only 192 MB memory. Due to the wireless technologies the network bandwidth is also limited. For example, some PDAs of HP are equipped with WLAN 802.11b, and Bluetooth 1.2.

2.7 Transient connectivity and availability

Many nodes may not be reachable at some time so that they can save power.

2.8 Each node is a router

The nodes out of the range of a fixed node cannot be directly reached by this node. They can only be reached by packet forwarding of other nodes.

2.9 Shared physical medium

Unlike wired networks, every device within the range can access the transmission medium.

2.10 Lack of central management

Ad hoc networks can be established everywhere and every time. Generally there is no central management available, and we can also not assume that any information is shared.

3. MANET

Mobile ad-hoc network deals with devices equipped to perform wireless communication and networking, but without any existing infrastructure such as base stations or access points. Wireless devices form a network as they become aware of each other's presence. They communicate directly with devices inside their Radio range in a peer-to-peer nature. If they wish to communicate with a device outside their range, they can use an intermediate device or devices within their radio range to relay or forward communications to the device outside their range. An ad-hoc network is self-organizing and adaptive. Networks are formed on-the-fly, devices can leave and join the network during its lifetime, devices can be mobile within the Network, the network as a whole may be mobile and the network can be deformed on-the-fly. All this needs to be done without any system administration and without the Requirement for any permanent devices within the network. Devices in mobile ad-hoc networks should be able to detect the presence of other devices and perform the necessary set-up to facilitate communications and the sharing of data and services. A MANET has the following features:

3.1 Autonomous terminal

In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

3.2 Distributed operation

Since there is no background network, for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

3.3 Multi-hop Routing

Basic types of ad hoc routing algorithms can be single-hop and multihop, based on Different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more

intermediate nodes.

3.4 Dynamic Network Topology

Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network (e.g. Internet).

3.5 Fluctuating link capacity

The nature of high bit-error rates of wireless connection might be more profound in a MANET . One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

3.6 Light-weight terminals

In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

4. MANET APPLICATIONS

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread applications. Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Typical MANET applications include:

- Military battlefield
- Sensor Networks
- Automotive Applications
- Commercial sector
- Personal Area Network

The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment.

5. CHALLENGES FACING MANETS

The ad hoc networks have its own share of challenges which are listed below:

5.1 Spectrum allocation

Issues such as interference, limited range, limited data throughput, device mobility and the sharing of the RF spectrum amongst devices all need addressing. Regulation Regarding the use of radio spectrum is currently under the control of FCC. Most Experimental Ad hoc networks are based on the ISM band. To prevent interference Ad hoc networks must operate over some form of allowed or specified spectrum range. Most microwave ovens operate in 2.4 GHz band, which can therefore interfere with wireless LAN systems.

5.2 Energy efficiency

Energy efficiency is a concern. Most existing protocols don't consider power consumption as an issue since they assume the presence of static hosts and routes, which are powered by mains. However mobile devices today mostly operated by batteries .Battery technology are still lagging behind the microprocessor technology. The lifetime of an Li-on battery today is only 2-3 hours. Such a limitation in operating hours of a device employs a need for power conversion. In particular for mobile ad hoc networks devices will have to perform the role of routers. Hence forwarding packets on the behalf of others will consume power and this can be quite Significant for nodes in mobile ad hoc networks.

5.3 Routing

Routing of data between devices outside their RF range. The routing protocols , used on wired networks do not perform well on networks involving mobility and rapid membership changes. More effective routing protocols are required. In Ad Hoc networks, we need new routing protocols because of the following reasons:
Nodes in Ad Hoc networks, are mobile and
topology of interconnections between them may be quite dynamic. Existing protocols exhibit least desirable behavior when presented with a highly dynamic interconnection topology. Existing routing protocols place too heavy a computational burden on each mobile computer in terms of the memory-size, processing power and power consumption. Existing routing protocols are not designed for dynamic and self-starting behavior as required by users wishing to utilize Ad-Hoc networks.
Existing routing protocols like Distance Vector Protocol take a lot of time for convergence upon the failure of a link, which is very frequent in Ad Hoc networks.
Existing routing protocols suffer from looping problems either short lived or long lived. Methods adopted to solve looping problems in traditional routing protocols may not be applicable to Ad Hoc networks.

5.4 Existing IP Usage

For a mobile host to be able to communicate as it moves from one location to other, one of the following of the two things have to be in place: Mobile Hosts must changes its IP address whenever it moves to new place. Host specific routes must be propagated throughout Internet Routing fabric. There are problems with either of these options. If a host has an open TCP session with another host, that session will be terminated if the IP address changes. Also, if other hosts must be able to initiate communication with a mobile host, how can they do so if their IP address changes every time they move? How does the host obtain a new IP address as it joins a network? What is also of concern and it not addressed in this IETF draft or in any publications is the convergence of two separate auto configured ad-hoc networks, merging together to form one larger ad-hoc network. Depending on the amount of participating hosts in each network and given the size of the address space given to link local addressing in IPv4, there is a possibility of hosts having duplicate addresses. The main issue with using TCP in MANETs comes from the assumption that a packet being dropped is an indication of congestion occurring, not an indication of a lossy link or a data transmission error. This is due to the observation that that packet error/ loss rates over the internet due to transmission errors are of the order of 1%. However, in a wireless network, the amount of transmission errors is of a much higher order. The factors affecting the percentage of transmission errors include interference from other radio signals, device mobility, the sharing of a wireless link with other devices. All these can affect the delivery of TCP segments to the receiver, the timely return of ACK packets from the receiver and give variations in the RTT compared to the estimated value. Any of these occurring will result in the sender assuming that congestion is occurring and will use TCP's mechanisms to drastically reduce its transmission rate. MANETs also provide additional challenges to TCP operation. The mobility of hosts means that routes between hosts are open to change. When a route is broken due to host mobility, a route reconstruction procedure is invoked. This reconstruction results in a delay that the TCP sender is unaware of. Overall data throughput has had to suffer initially because of the route reconstruction delay, but TCP has now further drastically decreased the data throughput on false pretences.

6. SECURITY AND PRIVACY IN ADHOC NETWORKS

Following are the security and privacy challenges in the area of ad hoc networks. Firstly, use of wireless links renders an ad hoc network, susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Secondly, nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted. Thirdly, an ad hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP, nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes. Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

6.1 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 availability 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.

6.2 Availability

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

6.3 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.

6.4 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.

6.5 Authentication

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.

6.6 Non-repudiation

Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver Non repudiation is useful for detection and isolation of compromised nodes. When node A receives an erroneous message from node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

6.7 Scalability

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even Thousands of nodes. Security mechanisms should be scalable to handle such a large network. Otherwise, the newly added node in the network can be compromised by the attacker and used for gaining unauthorized access of the whole system. It is very easy to make an island-hopping attack through one rough point in a distributed network.

6.8 Other Advanced Attacks

In recent researches, more sophisticated and subtle attacks have been identified in MANET. Some protocols also enhanced their services and some other routing protocols are proposed to overcome the attacks. Still it is an area of interest for the security personnel. However, the blackhole (or sinkhole), Byzantine, wormhole, rushing attacks are the typical examples which are described below in detail.

6.9 Wormhole Attack

Wormhole attack is also known as tunneling attack. An attacker creates a tunnel and usesencapsulation and decapsulation to make a false route between two malicious nodes.

6.10 Blackhole Attack

The blackhole attack is performed in two steps. At first step, the malicious node exploits the mobile ad hoc routing protocol such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting the packets. In second step, the attacker consumes the packets and never forwards. In an advanced form, the attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected. In this way, the attacker falsified the neighboring nodes that monitor the ongoing packets.

6.11 Byzantine Attack

Byzantine attack can be launched by a single malicious node or a group of nodes that work in cooperation. A compromised intermediate node works alone or set of compromised intermediate nodes works in collusion to form attacks. The compromised nodes may create routing loops, forwarding packets in a long route instead of optimal one, even may drop packets. This attack degrades the routing performance and also disrupts the routing services.

6.12 Rushing Attack

In wormhole attack, two colluded attackers form a tunnel to falsify the original route. If luckily the transmission path is fast enough (e.g. a dedicated channel) then the tunneled packets can propagate faster than those through a normal multi-hop route, and result in the rushing attack. Basically, it is another form of denial of service (DoS) attack that can be launched against all currently proposed on-demand MANET routing protocols such as ARAN and ARIADNE.

6.13 Resource Consumption Attack

Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. The target of resource consumption attack isto send request of excessive route discovery or unnecessary.

7. THRESHOLD CRYPTOGRAPHY

Threshold cryptography (TC) involves sharing of a key by multiple individuals called shareholders engaged in encryption or decryption. The objective is to have distributed architecture in a hostile environment. Other than sharing keys or working in distributed manner, TC can be implemented to redundantly split the message into n pieces such that with t or more pieces the original message can be recovered. This ensures secure message transmission between two nodes over n multiple paths.
Threshold schemes generally involve key generation, encryption, share generation, share verification, and share combining algorithms. Share generation, for data confidentiality and integrity, is the basic requirement of any TC scheme. Threshold models can be broadly divided into single secret sharing threshold e.g. Shamir's t-out-of-n scheme based on Lagrange's interpolation and threshold sharing functions e.g. geometric based threshold. These schemes are being used to implement threshold variants of RSA, Elgamal, and Diffie-Hellman cryptographic algorithms that have characteristic, E (x + y) = E (x) * E (y), called homomorphism. TC finds its application in document authorization/signing or verification in organizations, a voting system for allowing access to system resources, e-commerce transactions, distributed online certification authority, and key distribution , in computer networks. TC can be implemented in various applications in a MANET. Applications such as coordinating efforts of military attacks using wireless devices in the battlefield or in disaster-struck area, wireless connectivity of various home appliances, and establishing communication among laptops, PDA sand other wireless devices at conferences, are ideal grounds for adopting TC. When compared with computer networks, it is easy to deduce that to implement TC in MANETs is a challenging task due to its dynamic and distributed nature and constrained resources at each network node.

8. SECURITY

In recent years, infrastructure-less ad hoc networking technologies such as MANET and Bluetooth have received critical attention in both academia and industry. This emerging technology seeks to provide users "anytime, anywhere" networking services in a potentially large-scale ad hoc wireless network. Mobile users are expected to exchange secure data communications among one another and with the rest of the Internet, at any time, and at any place. The growing commercial and military deployments of these networks have made security design increasingly important. Providing security support for ad hoc wireless networks is challenging for a number of reasons:

- Wireless networks are susceptible to security attacks ranging from passive eavesdropping to active interfering and denial-of-service (DoS) attacking;
- Occasional break-ins in a large-scale mobile network are inevitable over a large time interval;
- Ad hoc networks provide no infrastructure support;
- Mobile nodes may constantly leave or join the network;
- Mobility-induced wireless link breakage/reconnection and wireless channel errors make timely communications over multihop highly unreliable; and
- A scalable solution is a must for a large scale network. Therefore, adequate security support for authentication, confidentiality, integrity, non-repudiation, access control and availability is critical to deploying this wireless networking technology in commercial environments.

This work describes the efforts on providing ubiquitous, robust, and scalable security services for mobile ad hoc wireless networks. Our design has been driven by the following four main goals:

8.1 Ubiquitous service availability

Mobile users may freely roam inside the network. Our security service must be available everywhere and be robust against potential DoS attacks.

8.2 Robustness against break-ins

Complete intrusion-free systems are expected to be costly and unrealistic. Our design seeks to work in the presence of break-ins. Our overall system security should not be compromised if the break-ins are under a certain threshold.

8.3 Scalability

A wireless mobile network may consist of a large number of networking nodes. The network size may constantly change as nodes leave and new nodes join. Our design should scale to the network size.

8.4 Communication efficiency

Wireless channel is bandwidth constrained and error-prone. Routing in infrastructure-less ad hoc wireless networks is unreliable due to the node mobility and link breakage/reconnection. Our design should be communication efficient to conserve the mobility-based d-hop Algorithm. Mobility-based d-hop Algorithm [15] a clustering scheme based on the real distance between nodes. to calculate an estimate value of the distance between nodes by measuring the received signal strength taken from periodic beaconing used in some routing protocols. According to this estimated value they can determine the stability of every node. Then they elect the

most stable node as cluster-head. This algorithm is based on stability of node But stability of node not fixed. Therefore, the main design goals of this clustering algorithm are as follows:

- The algorithm minimizes the number of clusters by considering group mobility pattern.
- The algorithm must be distributed and executed asynchronously.
- The algorithm must incur minimal clustering overhead, be it cluster formation or maintenance overhead.

Network-wide flooding must be avoided.
Optimal clustering may not be achieved, but the algorithm must be able to form stable clusters should any exists.

8.5 Secured Clustering Algorithm

The main basic concepts used to derive the needed parameters are given below:

1. The Max Value: represents the upper bound of the number of nodes that can simultaneously be supported by a cluster-head. Since mobile nodes have limited resources, therefore they can't handle a great number of nodes. This value is defined according to the remainder of resources of the cluster-head.

2. The Min Value: represents the lower bound of the number of nodes that belong to a given cluster before proceeding to the extension or merging mechanisms. This value is global and the same for the entire network. The Min Value may avoid the complexity due to the management of great number of clusters.

3. D hops Cluster: as we have said, one hop clusters are too small for large ad hoc networks, therefore SCA creates D hops clusters where D is defined by the underlying protocol or according to the cluster-head state (busy or not). By the way, the diameter of the cluster can be extended in some situations.

4. Identity (ID): is a unique identifier for each node in the network to avoid any spoofing attacks or perturbation in the election procedure. We propose to use certificate as identity , therefore we suppose the existence of an online or offline Public Key Infrastructure managing the certificate distribution.

5. Weight: each node is elected cluster-head according to its weight which is computed from a set of system parameters. The node having the greatest weight is elected as cluster-head.

8.6 Identity based cryptosystem

An Identity-based cryptosystem is a novel type of cryptographic scheme proposed by Shamir [11], which enables any pair of users to communicate securely, and to verify each other's signatures without exchanging public or private keys, without keeping any key directories and without using the services of any third party. Problems with the traditional Public key cryptosystems (PKCs) are the high cost of the infrastructure needed to manage and authenticate public keys, and the difficulty in managing multiple communities. Whilst ID-based PKCs will not replace the conventional Public Key infrastructures, it might prove to be a complementary technology. In an ID-based PKC, everyone's public keys are predetermined by information that uniquely identifies them, such as their email address.

8.7 Cluster-Based Security Architecture for Ad Hoc Networks

A Cluster-Based Security Architecture for Ad Hoc Networks Secure communication, is very important in computer networks and authentication is one of the most eminent preconditions. However, common authentication schemes are not applicable in ad hoc networks because public key infrastructures with a centralized certification authority are hard to deploy there. This work proposes and evaluates a security concept based on a distributed certification facility. A network is divided into clusters with one special head node each. These cluster head nodes execute administrative functions and hold shares of a network key used for certification. New nodes start to participate in the network as guests; they can only become full members with a network signed certificate after their authenticity has been warranted by some other members.
In a security concept, typically striving for goals like authenticity, integrity, confidentiality, non-repudiation and availability, authentication of communicating entities is of particular importance as it forms the basis for achieving the other security goals: e.g., encryption is worthless if the communication partners have not verified their identities before.

9. CONCLUSION

As we can see from the above studies that there are policies to manage MANET using clustering with different set of advantages and application capabilities. On the other hand at Transport layer, so many methods are available for encryption. At application layer, Multi agent system to handle data retrieval. There is no such security architecture which can lead to all these requirements right from management of MANET through security and in turn information retrieval.

9.1 SOLUTIONS TO PROBLEMS IN AD-HOC-ROUTING

Here we assume existence of certain amount of security infrastructure. The type of Ad-hoc environment that we are dealing with here is called managed clusters.

- Concealing Network topology or structure
- Using independent Security Agents (SA)

9.2 SECURITY-AWARE AD-HOC ROUTING (SAR)

Wireless ad-hoc networks don't have fixed infrastructure,

since almost all of current network based IDS sit on the network gateways and routers and analyze the network packets passing through them, these type of network based IDS are rendered ineffective for the wireless ad-hoc networks. In case of wireless ad-hoc networks the only available audit data is restricted to the communication activities taking place within the radio range, and any IDS meant for these types of networks should be made to work with this partial and localized kind of audit data.

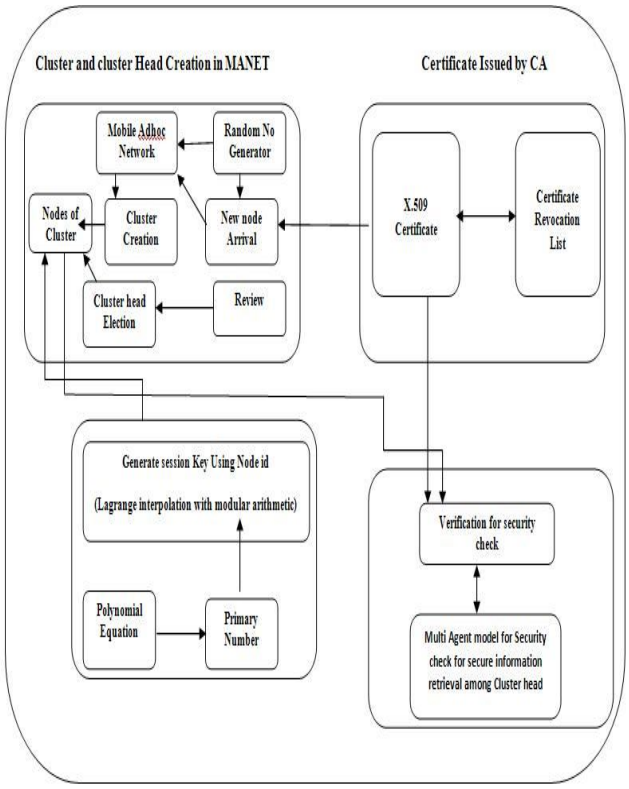
Anomaly Detection models of IDS cannot be used for wireless ad-hoc networks, since the separating line between normalcy and anomaly is obscure. A node that transmits erroneous routing information (fabrication) can be either a compromised or is currently out of sync due to volatile physical movement. Hence in wireless ad-hoc networks it is difficult to distinguish between false alarms and real intrusions.

10. PROPOSED SOLUTION

Architecture and Mechanism for Identity Based Information Retrieval system. Figure below illustrates the working architecture for Identity Based Information Retrieval System based on clustering, threshold cryptography and Lagrange interpolation. The proposed architecture is divided in to four modules like Clustering and cluster head election criteria, Generate session key using node id and threshold cryptography, Multi Agent model for secure information retrieval among cluster head, Last part explains about the X.509 certificate which we are using for authentication of node. The proposed architecture is divided in to three modules :-

- Clustering
- Generate session key
- Information retrieval using Multi Agent Model and CertificateX.509 for authentication Clustering consists of cluster formation, cluster head election criteria, cluster management etc.

Second module generates session key using node id and threshold cryptography with Lagrange interpolation. In the third module we explained about the Multiagent model for information retrival among cluster head.which is explained in next section. And in the last Module we are using X.509 certificate for authentication of node.



11. OTHER FACTORS

11.1 The Min Value

Represents the lower bound of the number of nodes that belong to a given cluster before proceeding to the extension or merging mechanisms. This value is global and the same for the entire network. The Min Value may avoid the complexity due to the management of great number of clusters.

11.2 D hops Cluster

As we have said, one hop clusters are too small for large ad hoc networks, therefore SCA creates D hops clusters where D is defined by the underlying protocol or according to the cluster-head state (busy or not). By the way, the diameter of the cluster can be extended in some situations.

11.3 Identity (ID)

Identity (ID) is a unique identifier for each node in the network to avoid any spoofing attacks or perturbation in the election procedure. We propose to use certificate as identity, therefore we suppose the existence of an online or offline Public Key Infrastructure managing the certificate distribution. The Certificate Issue by Certificate Authority and Cluster Head Certificate structure is shown below:-

VERSION
CERTIFICATE SERIAL NO.
ALGORITHM
CA NAME
TIME STAMP
NODE PUBLIC KEY
CA-ID
VALIDITY PERIOD
ACCESS POLICY
SIGNATURE

Fig. 5.7(a): Certificate issued by CA

CH-ID
SECRET-KEY
MOBILITY
STABILITY
GLOBAL
ISSUE DATE
EXPIRE DATE
BATTRY

Fig. 5.7(b): Cluster Head Certificate

12. CONCLUSION

Security has become a prime concern in the field of Networking and while communication between mobile nodes in Mobile Ad Hoc networks (MANETs) because of its unique characteristics like, rapid movement of node in infrastructure less network. It changes its topology also. This paper propose a security architecture for homogeneous as well as heterogeneous nodes. A technique based on Identity-Based information retrieval system in MANET that uses Citification authority for the purpose of accessing of nodes by using corresponding session key which is based on threshold cryptography. To generate the session key langrage's polynomial is used because it works for non uniform distribution of weights. It is required because Node identity is not always uniform in case of mobile nodes. It is also helpful to provide a safe strategy for authentication over Mobile Ad hoc Network.

13. FUTURE ASPECTS

The proposed architecture and mechanism for an identity based security system will provide efficient and effective security to nodes in MANET but as number of nodes over network increases beyond certain limit then performance might be reduced. Further advancements can be done to improve the performance of clustering by minimizing the inter node communication messages. This architecture can also be used in combination with different security algorithms at different layers.

REFERENCES

[1.] R. Murugun, S. Shanmugam "Cluster based authentication techniques for mitigation of internal attacks in MANET". ISSN 1450-216X VOL-51 No-3 (2011) PP.433-441.

[2.] Nevadita Chateerjee,Anupama Potluri and Atul negi, "Self organizing approach to MANET Clustering "

[3.] Atef Z. Ghalwash, Aliaa A. A. Youssif, Sherif M. Hashad and †Robin Doss Helwan "Self Adjusted Security Architecture for Mobile Ad Hoc Networks (MANETs)" University, Melbourne, Australia 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)

[4.] A. Shajin Nargunam, N.I. College of Engineering, Thuckalay, Tamil Nadu, India; E. P. Sebastian "Dynamic Security Scheme for MANET", Naitonal Institute of Technology Calicut, India

[5.] Li Wang, Jiu Hui Zhang " Security Strategy of MANET Based on Identity- Based Cryptosystems" 978-1-4244-5143-2/10/$26.00 ©2010 IEEE

[6.] S.Muthuramalingam and R.Rajaram Department of Information Technology, Thiagarajar College of Engineering, Madurai "A Transmission based clustering algorithm for topology control MANET", India International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.2, No.3, September 2010

[7.] Dang Nguyen1, Pascale Minet2, Thomas Kunz3 and Louise Lamont1 "On the Selection of Cluster Heads in MANETs" Communications Research Centre Ottawa, ON K2H 8S2, Canada INRIA Rocquencourt Rocquencourt, Le Chesney Cedex 78153, France 3 Dept. of Systems and Computer Engineering, Carleton UniversityOttawa, ON K1S 5B6, Canada IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814

[8.] Kadri, A. M'hamed, M. Feham "Secured Clustering Algorithm for Mobile Ad Hoc Networks" National Institute of Telecommunications, Evry, France IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007.

[9.] XU Xiao-long XIONG Jing-Yi, CHENG Chun-Ling "The Model and the Security Mechanism of the Information Retrieval System based on Mobile Multi-Agent" 978-1-4244-6871-3/10/$26.00 ©2010 IEEE.

[10.] Pradeep Rai Asst. Prof., CSE Department, Asst. Shubha Singh Prof., MCA Department, "A Review of 'MANET's Security Aspects and Challenges" IJCA Special Issue on "Mobile Ad-hoc Networks"MANETs, 2010

[11.] Shamir A, "Identity-Based Cryptosystems and Signature Schemes (LNCS196)[M]," Heidelberg: Springer-Verlag ,2009.

[12.] M. Gerla and J.T.C. Tsai. Multicluster, "mobile, multimedia radio network, Wireless Networks". Vol. 1, No. 3, 1995, PP. 255–265.

[13.] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks". Technical Report 200030, UCLA Computer ScienceDepartment 2000.
[14.] M. Chatterjee, S. K. Das and D. Turgut. WCA: "A WeightedClustering Algorithm for Mobile Ad hoc Network"s. Journal of Cluster Computing (Special Issue on Mobile Ad hocNetworks), Vol. 5, No. 2, April 2002, pp. 193-204.
[15.] I.I. ER, and Winston K. G. Seah, "Mobility-based D-hop Clustering Algorithm for Mobile Ad hoc Networks". IEEE WCNC, Atlanta, USA, March 2004
[16.] X. Xu, R. Wany, "The Agent-based information retrieval model with multi-weight ranking algorithm", Journal of Electronics & Information Technology, vol. 30 no.2, pp. 482-485, February 2008.
[17.] S.Muthuramalingam, R.RajaRam, Kothai Pethaperumal and V.Karthiga Devi "A Dynamic Clustering Algorithm for MANETs by modifying Weighted Clustering Algorithm with Mobility Prediction" International Journal of Computer and Electrical Engineering, Vol. 2, No. 4, August, 2010
[18.] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless Network Security, Springer Book, ISBN: 978-0-387-28040-0, pp. 103--135, 2007.
[19.] Gerla M., Tsai J. T. C., "Multi-cluster Mobile Multimedia Radio Network", ACM/Baltzer Wireless Networks Journal 95, vol. 1, (PP. 255- 265), Oct. 1995.
[20.] D.J. Baker and A. Ephremides. "The Architectural Organization of a Mobile Radio Ntwork Via a Distributed Algorithm", IEEE Transactions on Communications(PP. 1694– 1701), COM- 29- 11 (1996).
[21.] Basagni S., "Distributed Clustering for Ad Hoc Networks", Proceedings of International Symposium on Parallel Architectures, Algorithms and Networks, (PP. 310- 315), Jun. 1999.