Introduction to Mobile Ad Hoc Network

Ms. Amita Pandey

Department of E. & c., Universal College of Engg. & Techno., Gujarat, India

Abstract- Wireless network consist of wireless node without any administration. Due to present of mobility of nodes, the network is easily personated by several attacks. In 1980's Mobile ad hoc network s have been widely researched ` for many years. Ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies .The infrastructure less and dynamic nature of these network demands new set of networking strategies to be implemented in order to provide efficient end to end communication. Wireless devices are constantly grooving in communication field having more computing speed and a number of features, while shrinking in weight and size. The ad hoc network is made up of multiple nodes connected by links since link can be connected as well as disconnected at any time. The ad hoc network inherits the some traditional problem of mobile communication as well as wireless. Routing in mobile ad hoc networks in challenges task due to its frequent changes in topology. We discuss in this paper routing protocol, challenges and security of ad hoc network

***Index Terms*-** Ad-hoc network, Routing Protocol, MANET Attacks, Challenges Application

I. Introduction

Mobile ad-hoc network is a collection of wireless mobile host without fixed infrastructure and centralized administration (figure1).Communication in MANET is done via multi hope paths. Lots of challenges are there in this area: MANET contains diverse resources the line of defence 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 hosts may vary in different applications, There is no stationary infrastructure. Each node in MANET acts as router those forward data packets to other nodes.

Higher flexibility and scalability in ad-hoc motivate many application. Nodes in ad hoc network are self –organized, these will require higher security over network. Due to limited communication and communication resources it becomes difficult to provide security for ad-hoc network. Group communication for is common for ad-hoc network which require data to be transmitted in a secure and trusted manner. To provide network security has to achieve security goals (1) Confidentially, to prevent unauthorized from reading transmitted dated, (2) Message authentication used to prevent tempering with transmitted packet. Source message authentication is the corroboration that message has not been changed and the sender of a message is as claimed to be, this can be done by(1) cryptographic digital signature(2) message authentication code, First involve asymmetric cryptography and often needs heavy computation at the sender and receiver. The MAC implicitly ensures message and source integrity. In unicast, a shared security system used for MAC generation. Many challenges are involved to provide group communication in ad hoc network; nodes in ad-hoc network have limited computing, bandwidth, and energy resources which make the overhead. Second due to unstable wireless links due to interference cause frequent packet loss error and require a security solution that includes retransmission and reply over the packet loss. Third use of same common key will make a problem of impersonating source by any receiver, so solution has to be made for using multiple authentications over the network without overhead. This paper propose a two tire authentication scheme

For multicast traffic for ad hoc network, the nodes are grouped into cluster in order to cut overhead and provide scalability. Multicast traffic with in the same cluster employ a one way has function to authenticate the message source. The message authentication code is appended to message and the authentication key is revealed after the message is delivered which is used to message authentication sources. Cluster would make it possible to keep the node synchronized and address the variance in forwarding delay issue of massage authentication within a cluster. Cross-cluster includes message authentication code (MACs) that are based on multiple keys. Each cluster has distinct combination of MACs in the message in order to authenticate the source.

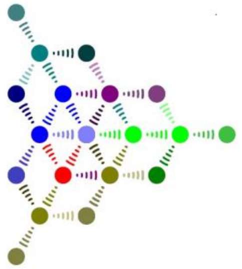


Figure 1: A mobile Ad Hoc Network

Network centric warfare broadly describe the combination of strategies ,emerging tactics, techniques procedures and organisations, which even partially networked force to gain a decisive war fighting advantage Network centric warfare should be supported with capabilities such as mobility, security, survivability, and is capable of supporting multimedia tactical information This require the importance of secure, integrated and efficient networking in digital battle field (DBFs) which may be comprised of various critical networking component including satellites ,terrestrial units and tactical operation centre. Among them military Mobile Ad-hoc networks (MANETS) gain a special importance for the future combat system.

II. RELATED WORK

Many existing security solutions for conventional networks are ineffective and inefficient ad hoc networks. Consequently, researcher have been working for the last decade on developing new security solutions or changing current ones to be applicable to ad-hoc network. In literature several approaches have been developed Multicast security. Taxonomy and efficient construction, in this approach sources appends MACs for multicast keys so that a receiver verifies the authenticity of message without being able to forge the MACs the other nodes. The challenges in using this category of approaches are striking the balance between collision overheads and performance. Use of distinct MAC per node will create bandwidth overhead and if same key is used it will make risk over nodes collision. Efficient authentication and signing of multicast streams over loss channels TESLA is very popular example this category. One of the most distinct advantage of time asymmetry is the minimal per packet overhead that they impose. However, it requires clock synchronization among the communication parties in order to prevent accepting forged packet, or discarding authentic packet. But for large network forwarding delay will force the node to limit the packet transmission rates to avoid revealing next keys to intermediate nodes before all receivers get all previously transmitted packet.

Scalable Multicast rout is proposed, constructing a shared bi-directional multicast tree to avoid network partitioning. Protocol is based on the location information obtained employing relevant data structure. Two tired hierarchical strategy was proposed that combines both time and secret information asymmetry in order to achieve scalability and resource efficiency. Deliver multicast data reliably with minimal network overhead. No requirement of maintaining any tree or mesh likes structure for multicasting. Delivering data reliably in both sparse network and dense network efficient and scalable multicasting (ESM) was proposed.ESM used source to receiver expansion approach made a balance between multicast group and overhead. An Ad-hoc network is a network consist collection of nodes, which can communicate with each other with any Centralized infrastructure. Nodes within ad hoc are mobile. They can communicate with each within radio range through direct wireless links. They also communicate through other nodes

They are self-organizing. There is no infrastructure. They providing communication when a network is not available or not considered to be secure or safe to use an existing infrastructure and also providing a communication network when existing network is not available or destroyed they uses in personal are network like as Mobile phone, laptop etc.

In this study, in order to address the problem, we propose anew multi –tier adoptive military MANET security protocol using hybrid cryptography and sign crypt ion. In our protocol, we particularly focus on the secure multicast concept to provide secure and instant communication in digital battle field (DBF). In order to provide security and efficiency simultaneously, we make county buttons to the military MANETS for three main areas: Structural design of the military MANET a, cryptographic methods used in MANETs and integrated key management technique. These are particularly selected, since they are essential factors that determine security and performance characteristics of military MANETs, We use amulet-tired network structure, which provides advantage for structure organization of military MANETs. Two tired unmanned Ariel Vehicle- Mobile Backbone Networks (UAV-MBN) have been recently proposed for DBFs exploiting the heterogeneous structure of MANETs. In our protocol, as a new approach, we divide MBN tier into MBN1 and MBN2 tiers. This is significantly facilitating key management since it encapsulates effects of the rekeying operation in the restricted sub-theatres. It also utilizes some benefits of MBN1 type nodes and facilities certifications procedure in the MBN tier by reducing the threshold cryptography requirements.

III. APPLICATION AND LIMITATION OF MANET

It is easy to imagine a number of applications where this type of properties would bring benefits. One interesting research area id inter-vehicle communications. It is one area where the ad-hoc network could really change the way we communicate covering personal vehicle as well as professional mobile communication needs. Also, it is area where no conventional (i.e. wired) solutions would do because of high level of mobility. When considering demanding surrounding, say mines for example, then neither would the base station approach work but we must be able to accomplish routing via nodes that are part of the network i.e. we have to use ad-hoc network. Such network can be used to enable next generation of battlefield applications envisioned by the military including unmanned micro-sensor networks. Ad hoc networks can provide communication for civilian application, such as disaster recovery and message exchange among medical and security personal involved in rescue mission

Military sector**:** military equipment routinely contains some short of computer equipment. Ad-hoc networking would allow the military to take advantage of complete network technology to maintain an information network between the soldier vehicle and military information headquarters. The basic technique came from this field.

Commercial Sector**:** Ad hoc can be used in emergency/risqué operation for disaster relief efforts, e.g. in fire, flood and earth quake. This may be because all of equipment was destroyed, or perhaps because the region is too remote Rescuers must be able- to communicate in order to make the best use of their energy, but also to maintain to safety .By automatically establishing a data network with the communication equipment that the rescuer are already carrying, their job made easier. Other commercial scenarios include ship to ship ad hoc mobile communication, law enforcement, etc.

A. Low level:

Appropriate low level application might be in home networks where device can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium boat and small air craft, mobile ad hoc communication will have much application.

*B. Data Network***:**

A commercial application for MANETs includes ubiquitous computing. By allowing computers to forward data for others, data network may be extended for beyond the usual reach of installed infrastructure. Network may be made more widely available and easier to use.

***C. Sensor Network*:**

This technology is a network composed of a very large number of small sensors. These can be used to detect any number of properties of an area. Examples include temperature, pressure, toxin, pollution, etc. The capabilities of each sensor are very limited, and each must rely on other in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile ad hoc networks could be the key to future homeland security.

D. Temporal dependency:

Due to physical constrains of the mobile entity itself, the velocity of mobile node will change continuously and gently instead of abruptly, i.e. the current velocity is dependent on the previous velocity. However, intuitively, the velocity at two different time slots is independent in random waypoint model.

E. Spatial dependency:

The movement pattern of mobile node may be influenced by and correlated with nodes in its neighbour-hood. In random waypoint, each mobile node moves independently of order.

F. Geographic restriction*:*

In many cases, the movement of a mobile node may be restricted along the street or a freeway. A geo-graphic map may define these boundaries.

IV. SECURITY PROBLEM IN MANET

MANETS are much more vulnerable to attack than wired network. This is because of the following reason:

A. Open medium-

Eavesdropping is easier than in wired network.

B. Lack of centralized Monitoring*-*

Absence of any centralized prohibits any monitoring agent in the system.

C. Lack of clear line of defence

The only use of line of defense attack prevention may not use, Experience of security research in wired world has taught us that we need to deploy layered security mechanism because security is a process that is as secure as its weakest link. In addition to prevention, we need II line of defense detection and response.

D. Cooperative Algorithm*-*

The algorithm of MANET requires mutual trust between nodes which violates the principle of Network

V. ADVANTAGE

The following are the advantage of MANETs; they provide access to information and service regardless of geographic position. This network can be setup at any place and time. These networks work without any preexisting infrastructure.

VI. DISADVANTAGE

Some of the disadvantage of MANETs are; limited resources, limited physical security, and intrinsic mutual trust vulnerable to attacks. Lack of authorization facilities volatile network topology makes it hard to detect malicious nodes Security protocols for wired networks cannot work for ad hoc networks.

VII. CHALLENGE IN MANET

***A.* Autonomous-**

No centralized administration entity is available to manage the operation of the different mobile nodes

B. Dynamically a Changing Network Topology

Mobile node come and goes from the network there by allowing any malicious node to join the network without being detected.

C. Device discovery*-*

Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

D. Bandwidth optimization:

Wireless linked has lower capacity than the wired network. Routing protocols in wireless network always use the bandwidth in an optimal manner by keeping the overhead as low as possible. The limited transmission range also imposes constrained on routing protocols in maintaining the topological information. Especially in MANETs due to frequent change topological information at all nodes involves more control overhead which, in turn, more bandwidth wastage.

E. Limited Resources :

Mobile nodes rely on battery power, which is a scare resource; also storage capacity and power are severely limited.

F. *Scalability:*

Scalability can broadly define as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes

G. Infrastructure less and self-operated:

Ad-hoc networks are supposed to operate independently of any fixed infrastructure.

H. Poor transmission quality:

This is an inherent problem of wireless communication caused by several error source that result in degradation of received signal.

I. Ad-hoc addressing:

Challenges in standard addressing schema to be implemented.

J. Network configuration*:*

The whole MANET infrastructure is dynamic and is the reason for dynamic connection and dis connection of the variable links.

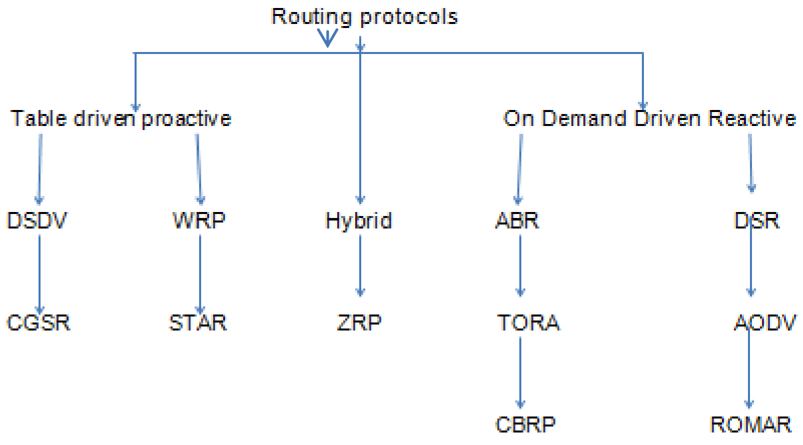
K. Topology maintenance

Updating information of dynamic links among nodes in MANETs is a major challenge

VIII. ROUTING PROTOCOLES

Routing protocols define a set of rules which governs the journey of message packets from source to destination in a network. In MANET there are three types of routing protocols each of them is applied according to the network circumstances.

Figure 1shows the basic classification of the routing protocols in MANETs



1. Proactive Routing Protocols-

Proactive protocols are also called as table driven protocols. In this each node maintain routing table which contains information about the network topology even without requiring it. The routing table are updated periodically whenever the network topology changes. Proactive protocols are not appropriate for large network as they need to maintain node entries for each and every node.

There various proactive routing protocols. Example: DSDV, OLSR. WRP etc.

2. Reactive Routing Protocols-

Reactive protocol is also known as on demand routing protocol. In type of protocol, rout is discovered whenever it is needed. Node initiates rout discovery when demanded. A rout is acquired by the initiation of a rout discovery process by the source node. This routing protocol has two major components

A. Rout discovery-In this phase source node initiate rout discovery on demand basis. Source node consult its rout cache for the available route from source to destination otherwise if the rout is not present it initiate rout discovery. The packet of source node includes the address of the destination node as well as address of the intermediate node to the destination.

B. Route maintenance-Due to dynamic topology go the network cases of the rout failure between the nodes arises due to link breakage etc, so rout maintenance is required. Reactive protocol has more acknowledgement mechanism due to which route maintenance is possible.

There are various reactive protocols. Example: DSR, AODV, TORA AND LMR.

3. Hybrid protocol-

This type of routing protocol is trade –off between proactive and reactive protocols. Proactive protocols have more overhead and less latency while reactive protocols overhead and more latency. Thus a hybrid protocols needed to overcome the shouting of both proactive and reactive routing protocols. This protocol is a combination of both proactive and reactive routing protocol. Its uses the on demand mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problem in the network. Hybrid protocol is appropriate for large networks where large numbers of nodes are present. In this, large network is divided into a set of zones where routing inside the zone is done by using proactive approach and the zone routing is done routing using reactive approach.

There are various hybrid routing protocols for MANET, like ZRP, SHRP etc.

IX. COMPARISON OF PROTOCOLS

Protocol	Advantage	Disadvantage
Proactive	Information is always available. Latency is reduced in the network	Overhead is high, routing information is flooded in the whole network
Reactive	Path available when needed overhead is low and free from loops	Latency is increased in the Network
Hybrid	Suitable for large networks and up to date information Available	Complexity increases

X. ATTACKS ON MANET

There are various kinds of attacks on ad hoc network which are following:

A .Location Disclosure-

Location disclosure is an attack that targets the privacy requirements of an ad-hoc network. By using traffic analysis techniques, simpler probing and monitoring approaches, an attacker is able to detect the location of node or the structure of the whole network.

B. Black Hole-

In a black hole a malicious node injects false route replies to route requests, announcing it as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for simply to attract all the traffic towards it in order to perform a denial of service attack by discarding the received packets.

C. Replay-

A replay attack is one of the attacks that degrade severely the performance of MANET. a reply attacker does this attack by interception and retransmission of valid signed messages

D. Wormhole-

The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, capture routing traffic at one point of the network and tunnel them to another point in the network ,to node B, for example that share a private communication link with a. Node B then selectively injects tunneled traffic into the network. The connection between the nodes that have established route over the wormhole link is completely under the control of the two conspiring attackers. The packet leashes are the solution to this attack.

E. Blackmail-

These attacks are relevant against routing protocols that use mechanism for the identification of malicious nodes and propagates messages and try to isolate legitimate node from the network. The non-repudiation security criteria can prove to be usefully in such cases since it binds a node to the message it generated.

F .Denial of Service-

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. In a routing tangle overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of participating nodes and disrupt the establishment of legal route.

G. Routing –

Table poisoning-Routing protocol maintain table that hold information regarding route of the network. In this type of attack, the malicious node generate and send fabricated signaling traffic or modify legitimate message from the other nodes ,in order to add false entries in the tables of the participating nodes.

H. Breaking the neighbour relationship-

An intelligent filter is placed by an intruder on a communication link between two ISs (information system) could modify or change information in the routing update or even interrupt traffic belonging to any data session.

I. Masquerading-

During the neighbor acquisition process, an outside intruder could masquerade a nonexistence or existing IS by attacking itself to communication link and illegally joining in the routing protocols domain by comprising authentication system .The threat of masquerading is almost the same as that of a compromised IS.J.

J.Impersonation-

Impersonation attacks are a severe threat to the attacker can capture some nodes in the network and make them look like friendly nodes. Thus, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information

K. Eavesdropping-

It is another kind of attack that usually happens in the mobile ad hoc networks.Eavesdroping means to obtain some confidential information that should be kept secret during the communication. The confidential information may include the public key, private key, location and passwords of the nodes. Because such data are very confidential to the nodes, they should be kept secret so that unauthorized can't access this.

XI. CONCLUSION

In this paper, we describe the infrastructure less Mobile Ad Hoc networks. Firstly the brief introduction was discussed, including the basic idea of MANET. Then the characteristic and application of MANETWERE discussed that helps us to understand more about MANET. Routing protocols were discussed, including its types, example and pros and cons comparison among them .We describe the challenges of MANET, through which we can know the issue in MANET which leads to some problem in this type of networks. Security of MANET is discussed having the brief description of security criteria and then the attack on MANET.

The solution of these issues is necessary to fulfill the requirement of wide commercial deployment of MANET.

Mobile Ad hoc networking is one of the most important and essential technologies that support future computing scheme the characteristic of MANET bring this technology as a great opportunity together with many challenges. Now a day. MANET is becoming an interesting research topic and there are many research projects employed by academic and companies all over the world.

MANETs can be exploited in a wide are of application like military battlefield, emergency search and rescue, law enforcement, commercial, local and personal contexts. The most important thing for the networks is security. It is also important for wireless Ad hoc network because its application is military.

REFERENCES

[1] Jagtar Singh & Natasha Dhiman, Department of computer Science& Engineering HCTM Technical Campuses, Kaithal, India Vol.2 Issue 4 July 2013.ISSN 2278-621X.

[2] Ankur Bang, Prabhakar L. Ramteke. MANET: History, Challenges and Applications. Volume 2, issue9, September2013.ISSN2319-4847

[3] Ms.Ruchica A. Kale and Prof.Dr.S.R. Gupta Department of Computer Science & Engineering PRMIT & R, Bandera vol. 6, No.2, Apr 2013 (IJCSA) ISSN: 0974-1011 (Open Access).

[4] Malik N. Ahmed, Department of Computer science & Information. System, University Technology Malaysia. Johor, Malaysia. Abdul Hanan Abdullah, Ayman El –Sayed Department of Computer science and

Engineering. Menouf, Egypt. VOL. IJCNSS, 2013, 6,176-185

[5] Mr. Raja, Capt. Department of Computer application, Pachaiyappa ‘college, Chfnni30. Dr . S Santosh Baboo. Department of Computer Science, D.G.Vaishnav College, Chennai s106.IJCSMC, Vol.3, Issue.1, January 2014, pg. 408-417.ISSN 2320-088X.

[6] Stephen Mueller, Department of Computer science, University of California, Davis, CA95616 Rose P. Tsang.and Deepak Ghosal Department of Computer science, University of California, live more, Ca94551 Multipath Routing in Mobile Ad Hoc Network: Issues and Challenge

[7] H. yang, et al.. Security in mobile Ad-hoc wireless network: Challenges and solutions. IEEE wireless commun.Mag. Vol.11 no.1, pp. 1536-1284 feb 2004

[8] Turk J Elect Eng. & Comp Sci, Vol.18, No.1, 2010

AUTHORS

First Author – Ms. Amita Pandey, Department of E. & c., Universal College of Engg. & Techno, Gujarat, India, apamitapandey@gmail.com