International Journal of Scientific & Technical Development
(A Peer-Reviewed Bi-Annual Journal) ISSN: 2348-4047

SECUIRTY IN MOBILE ADHOC NETWORKS

Dr. Rajeev Dahiya
Department of Computer Science and Engineering
Desh Bhagat University, Mandi Gobindgarh, Punjab,India

Abstract
Mobile Ad Hoc Networks (MANETs) have received drastically increasing interest, partly owing to the potential applicability of MANETs to myriad applications. The deployment of such networks, however, poses several challenging issues, due to the dynamic nature of the nodes, the arbitrary topology, the limited wireless range of nodes, and transmission errors. Since all the nodes in the network collaborate to forward the data, the wireless channel is prone to active and passive attacks by malicious nodes, such as Denial of Service (DoS), eavesdropping, spoofing, etc. Implementing security is therefore of prime importance in such network , As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. we focus on the findings and future works which may be interesting for the researchers However, in short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms in MANET.
Keywords: [MANET, Prevention, Detection ,Reaction, GUI]

INTRODUCTION

MANET Introduction

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The

nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. it is a selfconfiguring network of mobile nodes connected by wireless links the union of which form an arbitrary topology. The nodes are free to move randomly and

organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. MANETs are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load).The following flowchart shows the working of any general ad-hoc network

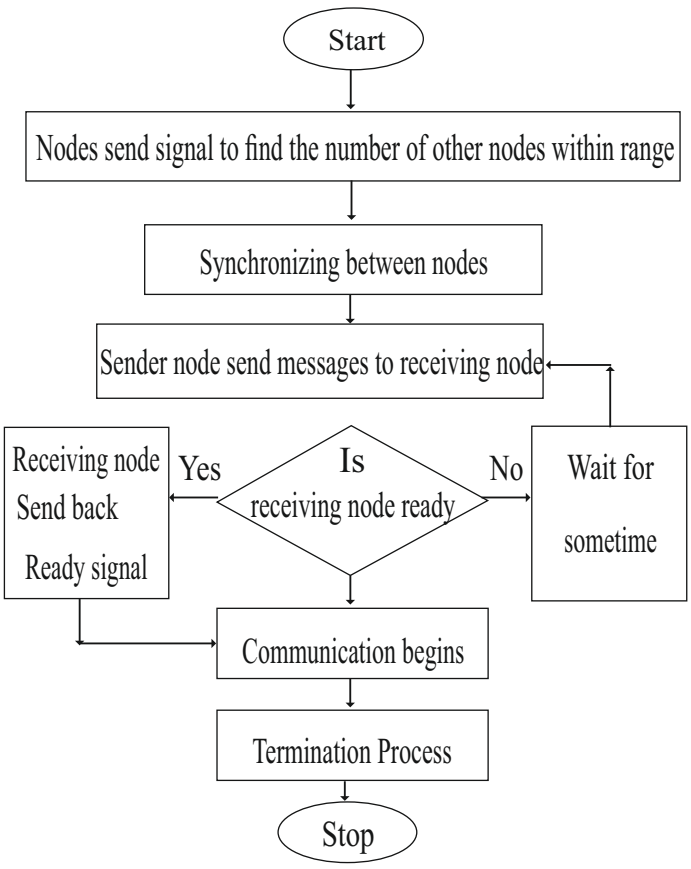

Fig1.1: Working of a general Ad-Hoc Network

MANET HISTORY

The whole life-cycle of ad-hoc networks could be categorized into the first, second, and the third generation ad-hoc networks systems. Present ad-hoc networks systems are considered the third generation. The first generation goes back to 1972. At that time, they were called PRNET (Packet Radio Networks). The history of ad-hoc networks can be dated back to the DoD1-sponsored Packet Radio Network (PRNET) research for military purpose in 1970s, which evolved into the Survivable Adaptive Radio Networks (SURAN) program in the early 1980s. In conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment. The second generation of ad-hoc networks emerged in 1980s, when the ad-hoc network systems were further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) program. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks.

In the 1990s, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences. Since mid 1990s, a lot of work has been done on the ad hoc standards. Within the IETF, the MANET working group was born, and made effort to standardize routing protocols for ad hoc networks. Meanwhile, the IEEE 802.11 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, for building mobile ad hoc network prototypes out of notebooks and 802.11 PCMCIA cards.

There are currently two kinds of Mobile wireless networks. The first is known as infrastructured networks with fixed and wired gateways. Typical applications of this type of "one-hop" wireless network include wireless local area networks
(WLANs).

The second type of mobile wireless network is the infrastructureless mobile network, commonly known as the MANET. MANET is usually a selforganizing and self configuring "multihop"network which does not require any fixed infrastructure. In such network, all nodes are dynamically and arbitrarily located, and are required to relay packets for other nodes in order to deliver data across the network

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[14]. 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. 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 infrastructured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include:

1) Military battlefield. Military equipment now routinely contains some sort of computer equipment. Ad hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarters.

The basic techniques of ad hoc network came from this field.

2) Commercial sector. Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where nonexisting or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

3) Local level. Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

4) Personal Area Network (PAN). Shortrange MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context

PROPERTIES OF MOBILE ADHOC NETWORKS

MANETs have the following special features that should be considered in designing solutions for this kind of networks.

Dynamic Topology

Due to the node mobility, the topology of mobile multi-hop ad hoc networks changes continuously and unpredictably. The link connectivity among the terminals of the network dynamically varies in an arbitrary manner and is based on the proximity of one node to another node. It is also subjected to frequent disconnection during node's mobility. MANET should adapt to the traffic and propagation conditions as well as to 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.

Bandwidth

MANETs have significantly lower bandwidth capacity in comparison with fixed networks.The used air interface has higher bit error rates, which aggravates the expected link quality.Current technologies suitable for the realization of MANETs are IEEE 802.11(b,a) with bandwidth up to 54Mbps and Bluetooth providing bandwidth of 1Mbps. 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 subjected 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 links themselves can be heterogeneous.

Energy

All mobile devices will get their energy from batteries, which is a scarce resource. Therefore the energy conservation plays an important role in MANETs. This important resource has to be used very efficiently. One of the most important system design criteria for optimization may be energy conservation.

Security

The nodes and the information in MANETs are exposed to the same threats like in other networks. Additionally to these classical threats, in MANETs there are special threats, e.g. denial of service attacks. Also mobility implies higher security risks than static operation because portable devices may be stolen or their traffic may insecurely cross wireless links. Eavesdropping, spoofing and denial of service attacks should be considered.

Autonomous

No centralized administration entity is required to manage the operation of the different mobile nodes. In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. So usually endpoints and switches are indistinguishable in MANET.

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 among themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

Multi-hop Routing

Basic types of ad hoc routing algorithms can be single-hop and multi-hop, based on different link layer attributes and routing protocols. Single-hop MANET is simple in comparison with multi-hop MANET in terms of structures and implementation. 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.

Light-Weight Terminals

In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size and low power storage.Infrastructure-less and Self Operated A mobile ad hoc network includes several advantages over traditional wireless networks, including: ease of deployment, speed of deployment and decreased dependence on a fixed infrastructure. MANET is attractive because it provides an instant network formation without the presence of fixed base stations and system administrators.

SECUIRTY GOALS

The Goals of security mechanism of MANETs are similar to that of other networks. They can be briefly summarized as follow

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.

Confidentiality

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

Integrity

Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted. As with confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message. But, the most useful and straightforward approach is total stream protection. A connectionoriented 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.

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.

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, nonrepudiation allows A to accuse B using this message and to convince other nodes that B is compromised

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

CHALLENGES AND OPPORTUTNITIES

The salient features of ad hoc networks pose both challenges and opportunities in achieving these security goals. First of all, the use of wireless link renders an mobile ad hoc network susceptible to link attacks ranging from passive eaves dropping to active interfering. Unlike fixed hardwired networks with physical defense at firewalls and gateways, attacks on an mobile ad hoc network can come from all directions and target at any node. Damage includes leaking secret information, interfering message and impersonating nodes, thus violating the basic security requirements. All these mean that every node must be prepared for encounter with an adversary directly or indirectly.

Secondly, autonomous nodes in an mobile ad hoc network have inadequate physical protection, and therefore more easily to be captured, compromised, and hijacked. Malicious attacks could be launched from both outside and inside the network. Because it is difficult to track down a particular mobile node in a large scale of mobile ad hoc network, attacks from a compromised node are more dangerous and much harder to detect. All these indicate that any node must be prepared to operate in a mode that should not immediately trust on any peer.

Thirdly, any security solution with static configuration would not be sufficient because of the dynamic topology of the networks. In order to achieve high availability, distributed architecture without central entities should be applied. This is because introducing any central entity

into security solution may cause fatal attack on the entire network once the centralized entity is compromised. Generally, decision making in the mobile ad hoc networks is decentralized

TECHNIQUES USED TO SECURE MOBILE AD-HOC NETWORKS

In order to provide solutions to the security issues involved in mobile adhoc networks, we must elaborate on the two of the most commonly used approaches in use today:

- Prevention
- Detection and Reaction

Prevention dictates solutions that are designed such that malicious nodes are thwarted from actively initiating attacks. Prevention mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. Among the existing preventive approaches, some proposals use symmetric algorithms, some use asymmetric algorithms, while the others use one-way hashing, each having different trade-offs and goals. Prevention mechanisms, by themselves cannot ensure complete cooperation among nodes in the network. Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. A node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish or malicious. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets.

A selfish nodeis unwilling to spend battery life, CPU cycles or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. All protocols defined in this category detect and react to such misbehavior. Using this as the basis, we describe the following broad classifications:

1.Prevention

using symmetric cryptography

using one-way hash chains

2. Detection and Reaction

1.0 Prevention using asymmetric cryptography Asymmetric cryptographic techniques specify the underlined basic methodology of operation for protocols under this category. A secure wired networks or a similar network is required to distribute public keys or digital certificates in the ad-hoc network. Mathematically speaking a network with in nodes would require n public keys stored in the network. SAODV(an extension to AODV routing protocol) and ARAN are two of the protocols defined in this category.

1.1 Prevention using symmetric cryptography

Symmetric cryptographic techniques are used to avoid attacks on routing protocols in this section. We assume that symmetric keys are pre-negotiated via a secured wired connection. Taking a mathematical approach we see that a network with 'n' nodes would require n * (n + 1) / 2 pair wise keys stored in the network. SAR and SRP are the two protocols that belong to this category.

1.2 Prevention using one way hash Chains

This category defines a one-way hash chain to prevent attacks on routing protocols. They protect modification of routing information such as metric, sequence number and source route. SEAD and Ariadne fall into this category.

2.0 Detection and Reaction

Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes.All protocols in this category are designed such that they are able to detect malicious activates and react to the threat as needed. Byzantine , CONFIDANT , DSR, CORE and a protocol that uses Watchdog and Pathrater are the few protocols specified in this section

Conclusion :

Mobile Ad-Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Whether ad-hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of
MANET.

In this paper we have presented introduction to Manets, History of these networks, Goals of security mechanism, Various types of challenges in Manets, Various techniques to secure these network. As it is much clear that the complete security solution requires the prevention, detection and reaction mechanisms.

Preventive mechanism: In preventive mechanism, the conventional approaches such as authentication, access control, encryption and digital signature are used to provide first line of defense. Some security modules, such as tokens or smart card that is accessible through PIN, passphrases or biometrics verification are also used in addition.

Detection mechanism: In Detection mechanism ,It specifics solutions that attempt to identify clues of any malicious activity and the malicious node that is responsible for the malicious activity in the network.

Reaction mechanism: In Reaction
mechanism,it take punitive actions
against malicious node that is
responsible for the malicious activity in
the network.

Hence we can say that the
complete security solution requires the
prevention, detection and reaction
mechanisms for in MANET

FUTURE WORK:

Significant research in MANET
has been ongoing for many years, but still in an early Stage. In this paper our main motive is give the direction to the researchers in the area of security in mobile ad hoc network.

At present, we have to use the different tools/technique to provide the security at each different level. In future the researchers can develop the one tool/technique which will able to provide the security at each level ,where there is the security breach ,To achieve this goal it is necessary that the developed technique should include the functionality of prevention, detection and reaction mechanisms under one command line/ or GUI.

REFERENCES:

[1] Lecture Notes, "Broadband Computer Networks," by Prof. Zhisheng Niu, Tsinghua University, 2003.

[2] L. Tao. Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications. Ph.D. thesis in Computer Engineering, Virginia Polytechnic Institute and State University, 2004.

[3] L. Zhou and Z. Haas, Securing ad hoc networks," IEEE Network Magazine, vol. 13, November/December 1999.

[4] Sonja Buchegger & Jean-Yves Le Boudec. The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks. IBM Research Report RR 3354, May 2001

[5] S. Yi, P. Naldurg, and R. Kravets Security-Aware Ad hoc Routing for Wireless Networks The Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01), 2001.(another version Security- Aware Ad Hoc Routing Protocol for Wireless Networks, Report, August, 2001)

[6] Manel Guerrero Zapata. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing INTERNET-DRAFT draftguerrero- manet-saodv-00.txt, August 2002. First published in the IETF MANET Mailing List (October 8th 2001).

[7] Panagiotis Papadimitratos and Zygmunt J. Haas Secure Routing for Mobile Ad hoc Networks SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[8] Yih-Chun Hu, David B. Johnson, and Adrian Perrig.

SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.

[9] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad-hoc NeTworks In Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, June 2002. IEEE [10] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru and Herbert Rubens An On-Demand Secure Routing Protocol Resilent to Byzantine Failures In ACM Workshop on Wireless Security (WiSe), Atlanta, Georgia, September 28 2002

[11] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad-hoc NeTworks In Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, June 2002. IEEE

[12] Pietro Michiardi, Refik Molva Core: A Collaborative REputation mechanism to enforrce node cooperation in Mobile Ad Hoc Networks in Communication and Multimedia Security 2002 Conference

[13] Sergio Marti and T. J. Giuli and Kevin Lai and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. Mobile Computing and Networking (2000)