International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-2, Issue-8)

Research Article | **August 2013**

Survey of Challenges and Solution in MANET

Er. Sukhvir Boora[1], Asst. Prof. in Dept. of Computer Science & Engg., NCCE Israna, Haryana, India

Er. Shayog Sharma[2] Research Scholar at NCCE, Israna, Haryana, India

Dr. Seema
Assistant Professor
KITM, Karnal
Haryana, India

Abstract:

In this paper the authors present a survey of secure ad hoc routing protocols for wireless networks. Ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. Attacks on ad hoc network routing protocols disrupt network performance and reliability with their solution. They briefly present the most popular protocols that follow the table-driven and the source-initiated on-demand approaches. The comparison between the proposed solutions and parameters of ad hoc network shows the performance according to secure protocols. The authors discuss in this paper routing protocol and challenges and also discuss authentication in ad hoc network

Keywords: Security, Ad hoc Networks, Routing Protocols, Key Management.

1. INTRODUCTION

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. No fixed infrastructure such as base stations as mobile switching .Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology.

1.1 Security Goals

1) **Availability:** Ensures survivability despite Denial Of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

2) **Confidentiality:** Ensures certain information is never disclosed to unauthorized entities.

3) **Integrity:** Message being transmitted is never corrupted.

4) **Authentication:** Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

5) **Non-repudiation** Ensures that the origin of a message cannot deny having sent the message

1.2 Challenges

The salient features of ad hoc networks pose both challenges and opportunities in achieving these security goals. First, 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 [1,2,3], 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.

1.3 Criteria for Protecting Ad-hoc Networks

It necessary to find out how to judge a mobile ad-hoc network that it is secure or not, or in other words, what should be covered in the security criteria for the mobile ad-hoc network when to inspect the security state of the mobile ad-hoc network. Some important factors that are used to evaluate the security of a MANET protocol are:

1.3.1 Physical Security

In ad-hoc network especially mobile nodes are typically significantly more susceptible to physical attacks than wired nodes in traditional networks. However, the significance of the physical security in the overall protection of the network is highly dependent on the ad-hoc networking approach and the environment in which the nodes operate. For instance in ad-hoc network that consist of independent nodes and work in a hostile battlefield the physical security of single nodes may be severely threatened. Therefore in such scenarios the protection of nodes cannot rely on physical security. Physical security of a node is an important issue to the owner of the node, perhaps for privacy reasons, but the breaking of the physical security does not affect the security of the system as such.

1.3.2 Security of Network Operations

The security of ad-hoc network can be based on protection in the link or network layer. Security of network operations includes the confidentiality and authenticity of data.

• **Confidentiality:** Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Confiden- tiality can be achieved by using different encryption techniques so that only the legitimate communicating nodes can analyze and understand the transmission. The content disclosure attack and location disclo- sure attack reveals the contents of the message being transmitted and physical information about a particular node respectively.

• **Authenticity:** Authenticity is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

1.3.3 Access Control

Access control is often related to the identification and authentication of data.

• **Integrity:** Integrity guarantees that information passed on between nodes has not been tempered in the transmission. Data can be altered both intentionally and accidentally (for example through hardware glitches, or in case of ad hoc wireless connections through interference).

• **Non-repudiation:** Non-repudiation ensures that the information orig- inator can not deny having sent the information. This service is useful for detection and isolation of compromised nodes in the network. Many authentication and secure routing algorithms implemented in ad hoc networks rely on trust-based concepts. The fact that a message can be attributed to a specific node helps making these algorithms more secure. Designing a secure ad hoc wireless networks communication is a challeng- ing task due to (1) insecure wireless communication links, (2) absence of a fixed infrastructure, (3) resource constraints (e.g. battery power, bandwidth, memory, CPU processing capacity), and (4) node mobility that triggers a dynamic network topology. The majority of traditional routing protocols design fail to provide se- curity. The main requirements of a secure routing protocol are: (1) detection of malicious nodes; such nodes should be avoided in the routing process, (2) guarantee of correct route discovery, (3) confidentiality of net- work topology; if an attacker learns the network topology, he can attack the bottleneck nodes, detected by studying the traffic patters. This will result in disturbing the routing process and DoS, and (4) stability against attacks; the routing protocol must be able to resume the normal operation within a finite amount of time after an attack.

1.3.4 Service Aspects

Ad-hoc network may apply either hierarchical or flat infrastructure both in logical and physical layers independently. As in some flat ad-hoc network the connectivity is maintained directly by the nodes themselves, the network cannot rely on any kind of centralized services. In such networks the necessary services such as the routing of packets and key management have to be distributed so that all nodes have responsibility in providing the service. As there are no dedicated server nodes, any node may be able to provide the necessary service to another. Moreover, if a tolerable amount of nodes in the ad-hoc network crash or leave the network, this does not break the availability of the services

II. Availability

The term availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. Availability is a central issue in ad-hoc network that must operate in dynamic and unpredictable conditions. The network nodes may be idle or even be shut down once for a while. Thus the ad-hoc network cannot make any assumptions about availability of specific nodes at any given time. For commercial applications using ad-hoc network availability is often the most important issue from the viewpoint of the clients. The routing protocol must guarantee the robustness of the routing fabric so that the connectivity of the network is maintained even when threatened by rapid changes in topology or attackers.

2.1 Classification of MANET Routing Protocols

2.1.1 Flat Routing

Flat routing protocols are divided mainly into two classes; the first one is Proactive (Table-Driven) routing protocols and other is Reactive (On-Demand) routing protocols. One thing general for both protocol classes is that every node participating in routing plays an equal role. Proactive routing is mostly based on LS (Link-State) while On-Demand routing is based on DV (Distance-Vector).

2.1.2 Geographical Routing Protocols

Geographic routing protocols prevent network-wide searches for destinations. If the recent geographical coordinates are known then control and data packets can be sent in the general direction of the destination. This trim downs control overhead in the network.

There are two approaches to geographic mobile ad-hoc networks: (1) Actual geographic coordinates (as obtained through GPS – the Global Positioning System) (2) Reference points in some fixed coordinate system. Some of these routing protocols are:

- Distance Routing Effect Algorithm for Mobility (DREAM).
- GPS Ant-Like (GPSAL) .
- Greedy Perimeter Stateless Routing (GPSR).

There is another category of routing protocols; known as Power Aware routing protocols . This type of routing protocols take into consideration the energy required to transmit a signal, because the energy required is proportional to the square of the distance and transmitting a signal half the distance requires one fourth of the energy. Power Aware Multi Access Protocol with Signaling Ad-hoc Network (PAMAS) is an example of these types of routing protocol .

III. Security Attacks

The nature of attacks [4,5] vary greatly from one set of circumstances to another. In general, there is flow of information from a source to a destination. We have listed below the generic types of attack that might be encountered. They have also been pictorially depicted.

_ **Interruption:** An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.

_ **Interception:** An unauthorized party gains access to an asset. This is an attack on confi-
dentiality. The unauthorized party could be a person, a program or a computer. Examples
include wiretapping to capture data in a network and the illicit copying of files or programs.

_ **Modification:** An unauthorized party not only gains access to but tampers with an asset.**2**
This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.

_ **Fabrication:** An unauthorized party inserts counterfeit objects into the system. This is an
attack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.

IV. Possible Solutions

In this section, some possible ways of protecting routing information, integrity from malicious nodes has been discussed. Also the disclosure threat and location privacy is considered.

a) Redundant Paths

Another solution for increasing route robustness that is mentioned in [6] is the use of redundant paths. Some current routing algorithms such as AODV could easily be modified to produce several routes to one node. If one of the routes fails, possibly due to a malicious node in the path, another one of the discovered routes could be used instead. The usefulness of this protection is also limited, since an attack cannot always be detected by the route endpoints, which would be necessary in order to switch to another route.

b) Virtual Private Networks (VPN) This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP (Internet Protocol) data grams. Software are available to implement VPNs on just about every platform. Authentication depends upon three factors as password, Fingerprints and a security Token. Using two factors is desirable and using all three is most secured. VPN only support IP suite so it cannot be solution for all environments.

c) Encryption: Encryption is a technique used for many years for passing information from one place to other in a secured manner. A message in its original shape is referred to as a plaintext (or Text) and a message used to conceal original message is called Ciphertext (or Cipher). The process of changing plaintext into ciphertext is called Encryption and the reverse process is called decryption. There are many algorithms available for these processes. Some of them are Data Encryption Standard (DES), International Data Encryption algorithm (IDEA) and Public key algorithm (RSA) These are based on key based

algorithms. There is one popular key algorithm as Digital signature algorithm. In Digital signature, Signer encrypts the message with key, this is sent to recipient, the message is then decrypted with sender's public key. In case of ad hoc networks this may not be the best method as it uses a lot of space and is also slow.

d) One Way Hash Function: There is another algorithm called One way hash Function: it is like checksum of a block of text and is secure in that it is impossible to generate the same hash function value without knowing the correct algorithm and key. It accepts a variable size message and produces a affixed size tag as output. This algorithm can be combined with encryption to provide an efficient and effective digital signature.

e) Digital Signature: External attacks can be checked using Confidentiality of the routing information and also by authentication and integrity assurance features. Encryption can be solution to this. Digital signatures and one way functions can be applied [12]. Permian[18] used complex robustness to protect routing data from compromised nodes. It is ability to continue correct operation in presence of arbitrary nodes with complex failures.

V. Conclusions

Currently, ad hoc routing protocols are vulnerable to several kinds of attacks. Also, existing security enhancement techniques such as the Non-Disclosure Method and IPsec can be considered but these are either too expensive or ineffective to be of value. Unless protection against routing attacks can be provided by the applications that are used in the network, current routing protocols should not be used in areas of applications where the threats of denial-of-service attacks, forged routes, or location disclosure are of any significant importance. Ad hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. Several protocols for secured routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The current security mechanisms, each defeats one or few routing attacks. It is still a challenging task to design routing protocols resistant to multiple attacks.

Acknowledgement:

I wish to express my heartiest thanks to Er. Sukhvir Boora, Head Dept. of Computer Science,NCCE, Israna for his valuable suggestions.

References

[1] J. Ioannidis, D. Duchamp, and J. M. Gerald Q. IP based protocols for mobile ternetworking. ACM SIGCOMM Computer Communication Review (SIGCOMM'91), 21(4):235–245, September 1991.

[2] F. Teraoka, Y. Yokore, and M. Tokoro. A network architecture providing host migration transparency. ACM SIGCOMM Computer Communication Review (SIGCOMM'91), 21(4):209–220, September 1991.

[3] C. E. Perkins. IP mobility support. Request for Comments: 2002, October 1996.

[4] A.Kush, C.Hwang, P.Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE). May 2009, Volume 3. pp 1793-179

[5] A.Kush, C.Hwang, "Proposed Protocol For Hash-Secured Routing in Ad hoc Networks", MASAUM JOURNAL OF COMPUTING (MJC) Volume: 1 Issue: 2 Month: September 2009 , pp 221-226.

[6] Krishna Ramachandran. Aodv-st. Technical report, University of California, Santa arbara, USA. http://www.cs.ucsb.edu/ krishna/aodv-st/(visited 2006-04-15). [7]Bassam Halabi. Internet Routing Architectures. Cisco Press, 2000.