Routing Protocols and Security Issues in Mobile Ad-Hoc Network: A Review

Sandeep Dalal
Assistant Professor
Computer Science and application
DCSA, Maharshi Dayanand
University, Rohtak

Jyoti Mahendia
Student
Computer Science and Application
DCSA, Maharshi Dayanand
University, Rohtak

ABSTRACT
Mobile ad hoc networks(MANETs) is an infrastructure-less dynamic network consisting of collection of wireless mobile nodes that communicate with each other without using any centralized authority. MANETs are considered vulnerable to several kinds of security attacks like worm-hole attacks, black hole attacks, denial-of-service attacks and rushing attack etc. The routing protocol specifies a set of rules using which routers in network share information with each other and report updates to neighbourhood routers. The routing protocol enables a network to make dynamic adjustment to its conditions. Moreover, routing decisions need not to be predetermined and static. Different security mechanisms have been developed by numerous researchers so far in order to prevent such security threats in a network. In this regard, this paper discusses the existing security mechanisms and routing protocols in Mobile Ad-hoc Network in detail.

Keywords
Mobile ad-hoc network (MANET), Destination sequenced distance vector (DSDV), Ad-hoc On-demand Distance Vector routing (AODV), Dynamic Source Routing (DSR)

1. INTRODUCTION
Mobile Adhoc Network[7] is known as a group of multiple independent mobile nodes that are capable to communicate to each other via radio waves. Mobile nodes which are within range of radio of one other could directly communicate. Others nodes require aid of intermediate nodes within order to route packets. Every node has a wireless interface within order to communicate with one other. Such networks are considered fully distributed & could work at any place without any help of fixed infrastructure such as access points or base stations.

1.1 Characteristics of Mobile ad hoc Network

- *Distributed operation*: There is no background network for central control of network operations; control of network is distributed among nodes.
- *M*ulti hop routing[6]: When a node tries to send information to other nodes which is out of its communication range, packet should be forwarded via one or more intermediate nodes.
- Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host & a router.
- Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, network topology may change randomly & at unpredictable time.

1.2 Paper outline
The rest of paper is organized as follows:

In Section II, III, IV we stated Pros & Cons of MANET, its applications & how Routing Protocols[6] work within mobile Ad-hoc network & their classification of routing protocol.

In Sections V, VI present security threats issues within mobile ad hoc network & their remedies.

Finally Section VII concludes paper.

2. PROS AND CONS OF MANET
2.1 PROS
The advantages of an Ad-Hoc network[6] include following:

- They provide access to information & services regardless of geographic position.
- Independence from central network administration. Self-configuring network, nodes are also act as routers. Less expensive as compared to wired network.
- Scalable—accommodates addition of more nodes.
- Improvement in flexibility.
- Robust due to decentralize administration.
- The network could be set up at any place & time.

2.2 CONS
- Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, realized throughput of wireless communication after accounting for effect of multiple access, fading, noise, & interference conditions, etc., is often much less than a radio's maximum transmission rate.
- Dynamic topology: Dynamic topology membership may disturb trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.
- Routing Overhead: In wireless Adhoc networks[10], nodes often change their location within network.

So, some stale routes are generated within routing table which leads to unnecessary routing overhead.

- Hidden terminal problem: The hidden terminal problem refers to collision of packets at a receiving node due to simultaneous transmission [4]of those nodes that are not within direct transmission range of sender, but are within transmission range of receiver.
- Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes.
- Mobility-induced route changes: The network topology within an ad hoc wireless[5] network is highly dynamic due to movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.
- Battery constraints: Devices used within these networks have restrictions on power source within order to maintain portability, size & weight of device.
- Security threats: The wireless mobile ad hoc nature of MANET brings new security challenges to network design. As wireless medium is vulnerable to eavesdropping & ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

3. APPLICATIONS[1] OF MANET

Some of typical applications consist of:

- Military battlefield: Ad-Hoc networking would allow military to take advantage of commonplace network technology to maintain an information network between soldiers, vehicles, & military information head quarter.
- Collaborative work: For some business environments, need for collaborative computing might be more important outside office environments than inside & where people do need to have outside meetings to cooperate & exchange information on a given project.
- Local level: Ad-Hoc networks[6] could autonomously link an instant & temporary multimedia network using notebook computers to spread & share information among participants at a e.g. conference or classroom. Another appropriate local level application might be within home networks where devices could communicate directly to exchange information.
- Personal area network & Bluetooth: A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth could simplify inter communication between various mobile devices such as a laptop, & a mobile phone.
- Commercial Sector: Ad hoc could be used within emergency/rescue operations for disaster relief efforts, e.g. within fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure & rapid deployment of a communication network is needed.

4. ROUTING PROTOCOL[6] FOR MANET AND CLASSIFICATION

An ad hoc routing protocol is known as convention which controls how nodes decide within which way they have to route packets among computing devices within a mobile ad hoc network.

In ad hoc networks, nodes are not familiar with topology of their networks. Instead, they have to discover it: a new node announces its presence & listens for announcements broadcast by its neighbours. Each node learns about others nearby & how to reach them, & may announce that it too could reach them.

The following is a list of some ad hoc network routing protocols.

4.1 Table-driven (proactive) routing

This type of protocols maintains fresh lists of destinations & their routes by periodically distributing routing tables throughout network. The main disadvantages of such algorithms are:

- Respective amount of data for maintenance.
- Slow reaction on restructuring & failures.

4.2 On-demand (reactive) routing

This type of protocol finds a route on demand by flooding network with Route Request packets. The main disadvantages of such algorithms are:

- High latency time within route finding.
- Excessive flooding could lead to network clogging.

4.3 Hybrid (both proactive & reactive) routing

This type of protocol[7] combines advantages of proactive & reactive routing. The routing is initially established with some proactively prospected routes & then serves demand from additionally activated nodes through reactive flooding. The choice of one or other method requires predetermination for typical cases. The main disadvantages of such algorithms are:

- Advantage depends on number of other nodes activated.
- Reaction to traffic demand depends on gradient of traffic volume.

4.4 Hierarchical routing protocols[6]

With this type of protocol choice of proactive & of reactive routing depends on hierarchic level within which a node resides. The routing is initially established with some proactively prospected routes & then serves demand from additionally activated nodes through reactive flooding on lower levels. The choice for one or other method requires proper tribulation for respective levels. The main disadvantages of such algorithms are:

- Advantage depends on depth of nesting & addressing scheme.

- Reaction to traffic demand depends on meshing parameters.

5. SECURITY THREATS TO MOBILE AD-HOC NETWORK

The attacks could be categorized on basis of behaviour of attack i.e. Passive or Active attack [2].

- Passive attacks: A passive attack does not alter data transmitted within network. But it includes unauthorized "listening" to network traffic or accumulates data from it. Passive attacker does not disrupt operation of a routing protocol but attempts to discover important information from routed traffic.
- Active attacks[1]: Active attacks are very severe attacks on network that prevent message flow between nodes. However active attacks could be internal or external. Active external attacks could be carried out by outside sources that do not belong to network. Internal attacks are from malicious nodes which are part of network, internal attacks are more severe & hard to detect than external attacks.

These attacks[2] generate unauthorised access to network that helps attacker to make changes such as modification of packets, DoS, congestion etc. Active attacks are classified into four groups:

- Dropping Attacks: Compromised nodes or selfish nodes could drop all packets that are not destined for them. Dropping attacks could prevent end-to-end communications between nodes.
- Modification Attacks:. These attacks modify packets & disrupt overall communication between network nodes. Sinkhole attacks are example of modification attacks.
- Fabrication Attacks: In fabrication attack, attacker send fake message to neighbouring nodes without receiving any related message.

The characteristics of MANET make them susceptible to many new attacks. These attacks could occur within different layers of network protocol stack.

5.1 Attacks at Physical Layer

Some of attacks identified at physical layer include eavesdropping, interference, & jamming etc.

- Eavesdropping: It could also be defined as interception & reading of messages & conversations by unintended receivers. The main aim of such attacks is to obtain confidential information that should be kept secret during communication.
- Jamming: Jamming is a special class of DoS attacks[1] which are initiated by malicious node after determining frequency of communication. Jamming attacks also prevents reception of legitimate packets.
- Active Interference: An active interference is a denial of service attack which blocks wireless communication channel, or distorting communications.

5.2 Attacks at Data link layer[1]

The data link layer could classify attacks as to what effect it has on state of network as a whole.

- Selfish Misbehaviour of Nodes: The selfish nodes may refuse to take part within forwarding process or drops packets intentionally within order to conserve resources & to conserve of battery power.
- Malicious Behaviour of nodes The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when communication takes place between neighbouring nodes. Attacks of such type are fall into following categories.
- Denial of Service (DoS): The prevention of authorized access to resources or delaying of time-critical operations. A denial of service (DoS) attack is characterized by an attempt by an attacker to prevent legitimate users of a service from using desired resources & attempts to "flood" a network, thereby preventing legitimate network traffic.
- Misdirecting traffic: A malicious node advertises wrong routing information within order to get secure data before actual route.
- Attacking neighbour sensing protocols: malicious nodes advertise fake error messages so that important links interface are marked as broken.

5.3 Attacks at Network Layer[4]

The basic idea behind network layer attacks is to inject itself within active path from source to destination or to absorb network traffic.

- Black hole Attack: In this type of attacks, malicious node claims having an optimum route to node whenever it receives RREQ packets, & sends REPP with highest destination sequence number & minimum hop count value to originator node .whose RREQ packets it wants to intercept.
- Rushing Attack: In rushing attacks when compromised node receives a route request packet from source node, it floods packet quickly throughout network before other nodes, which also receive same route request packet.
- Wormhole Attack: In wormhole attack, malicious node receive data packet at one point within network & tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole.

5.4 Attacks at Transport Layer

Session Hijacking: Attacker within session hijacking takes advantage to exploits unprotected session after its initial setup. In this attack, attacker spoofs victim node's IP address, finds correct sequence number i.e. expected by target & then launches various DoS attacks.

5.5 Attacks at Application Layer[1]

Malicious code attacks: Malicious code attacks include, Viruses, Worms could attack both operating system & user application.

6. REMEDIES OF SECURITY THREATS

There are several security[1] mechanisms that could be used to provide security. The Mechanism to secure MANET from external attacks are as follow:

6.1 Firewalls

In order to provide some level of separation between an organization's intranet & Internet, *firewalls* have been employed. A firewall is simply a group of components that collectively form a barrier between two networks.

6.1.1 Bastion host

A general-purpose computer used to control access between internal (private) network (intranet) & Internet (or any other un trusted network). Typically, these are hosts running a flavour of Unix operating system that has been customized within order to reduce its functionality to only what is necessary within order to support its functions. Many of general-purpose features have been turned off, & within many cases, completely removed, within order to improve security of machine.

6.1.2 Router

A special purpose computer for connecting networks together. Routers also handle certain functions, such as *routing*, or managing traffic on networks they connect.

6.1.3 Access Control List (ACL)

Many routers now have ability to selectively perform their duties, based on a number of facts about a packet that comes to it. This includes things like origination address, destination address, destination service[10] port, & so on. These could be employed to limit sorts of packets that are allowed to come within & go out of a given network.

6.1.4 Demilitarized Zone (DMZ).

The DMZ is a critical part of a firewall: it is a network that is neither part of un trusted network, nor part of trusted network. But, this is a network that connects un trusted to trusted.

6.1.5 Proxy

This is process of having one host act within behalf of another. A host that has ability to fetch documents from Internet might be configured as a *proxy server*, & host on intranet might be configured to be *proxy clients* .

6.2 Cryptography

Cryptography has been process of altering plaintext (ordinary text, just as letter) using process encryption into cipher text using procedure decryption. This procedure has been used for secure communication btw two parties within occurrence of third party. There are four goals for Modern cryptography:

- **Confidentiality:** It identifies that only participants (Sender & Receiver) should be able to access message.
- **Integrity:** Content of message should not be changed. If this has been altered, then this has been called type of modification attack.
- **Non-repudiation:** There has been situation where sender converts content of message & after that he refuses that he had not sent message.
- **Authentication**: Both sender & receiver have to prove credentials to each other.

In current times, cryptography has been basic requirement of computer experts for security purposes so that two parties could send data to each other without any modification & confidently. So both sender & receiver could validate to each other for secure communication so that material could be safely send to each other.

Cryptography has been process of changing plaintext (ordinary text, just as message) using process encryption into cipher text using procedure decryption. Encryption has been method of transforming real data, called clear text or plaintext, into form that appears to be random & unreadable, that has been called cipher text. That text could be understood by individual by computer. Executable code has been called clear text or plain text. After conversion into cipher text, then this has been impossible to understand this text by individuals as well as machine until this has been decrypted. So we could say this process has been very secure due to encryption & decryption technique. To protect message from attack[1] i.e. public & private attack, cryptography has been basic prerequisite.

7. CONCLUSION

Due to dynamic topology, distributed operation & limited bandwidth MANET is more vulnerable to many attacks. In this paper, we discuss MANET & its characteristics, Routing protocols for Adhoc network. We also discussed challenges, advantages, application, security goals, various types of security attacks within its routing protocols.

Security attack could classify as a active or passive attacks[1]. Different security mechanisms are introduced within order to prevent such network. We have also discussed existing security mechanism & proposed work to enhance security using one time password & internet protocol[6] filter.

8. REFERENCES

[1] Priyanka Goyal, Vinti Parmar & Rahul Rishi, "MANET: Vulnerabilities, hallenges,Attacks, Application",IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[2] Gagandeep, Aashima & Pawan Kumar "Analysis of Different Security Attacks within MANETs on Protocol Stack".

[3] International Journal of Engineering & Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012

[4] Mohammad Wazid , Rajesh Kumar Singh & R. H. Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques " International Journal of Computer Applications® (IJCA) International Conference on Computer Communication & Networks CSI- COMNET-2011.

[5] Fan-Hsun Tseng, Li-Der Chou & Han-Chieh Chao " A survey of black hole attacks within wireless mobile ad hoc networks" Human-centric Computing & Information Sciences 2011

[6] Sunil Taneja & Ashwani Kush, " A Survey of Routing Protocols within Mobile Ad-Hoc Networks", International Journal of Innovation, Management & Technology, Vol. 1, No. 3, 279-285, August 2010.

[7] Gary Breed Editorial Director, "Wireless Ad-Hoc Networks: Basic Concepts", High Frequency Electronics,March 2007.

[8] Hongmei Deng, Wei Li, & Dharma P. Agrawal, "Routing Security within Wireless Ad Hoc Networks" IEEE Communications Magazine • October 2002

[9] Mohseni, S.; Hassan, R.; Patel, A.; Razali, R, "Comparative review study of reactive & proactive routing protocols within MANETs", 4th IEEE International Conference on Digital Ecosystems & Technologies, 304-309, 2010.

[10] Humayun Bakht, " Survey of Routing Protocols for Mobile Ad-hoc Network", International Journal ofvInformation & Communication Technology Research, 258-270, October 2011.

[11] Mohit Kumar & Rashmi Mishra "An Overview of MANET: History, Challenges & Applications" , Indian Journal of Computer Science & Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[12] C. Perkins, E. Belding-Royer & S. Das, "Ad-Hoc On-Demand Distance Vector (AODV) Routing", RFC3561, July 003.