Secure Routing in Mobile Ad-hoc Networks

A Master's Project

Presented to

Department of Computer and Information Sciences

In Partial Fulfillment

Of the Requirements for the

Master of Science Degree

State University of New York Polytechnic Institute

by

Sumedh Jadhav

May 2016

Secure Routing in Mobile Ad-hoc Networks

DECLARATION

I declare that this project is my own work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

Sumedh Jadhav

05/21/2016

SUNY POLYTECHNIC INSTITUTE

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES

Approved and recommended for acceptance as a project in partial fulfillment of the requirements for the degree of Master of Science in Computer Systems Networking & Telecommunications.

7/19/16

DATE

Dr. Larry J. Hash

Project Advisor

ABSTRACT

The detailed study investigates the various problems faced by Mobile Ad hoc Networks because of their inherent characteristics. The characteristics make these networks vulnerable to various attacks. The attack known to be performed on MANETs were researched in order to gain better understanding and insight on how they can be defended against. The focus of this project was to secure the routing protocols, since routing plays a vital role in the operation of network and is the target of most attacks. Various research papers were referenced for collecting the information needed. The existing routing protocols were systematically categorized and compared. Additionally, advanced routing protocols that integrate cryptographic methods into them were studied to come to a conclusion that they are the most robust protocols that effectively protect the Mobile Ad hoc Networks against some dangerous attacks.

Securing the routing protocols is indeed the most important aspect for securing MANETs. However, there are other techniques that can be used as extensions for strengthening these networks, in addition to using a robust routing protocol. Recommendations have been made for the same.

PREFACE

The main purpose of writing this paper was to gain a better understanding on how the Mobile Ad hoc Networks can be made secure. These networks have a number of applications today, but are also more susceptible to attacks as compared to traditional wired or wireless networks. Research is still been going on this field. If we are able to protect the MANETs against attackers, these networks have proven to be very useful in scenarios where the traditional networks cannot be deployed.

ACKNOWLEDGEMENTS

I would like to thank my project advisor, Dr. Larry Hash, for always being sincere, supportive and encouraging me on this project from the very beginning. His insights and questions helped me collect information and study in depth, and thus gain a lot of knowledge in the area of security in MANETs. His expertise in research and writing assisted me greatly in writing the best paper of my career.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

The Mobile Ad-hoc Networks (MANETs) is a booming research area nowadays, mainly because we don't need a pre-installed network infrastructure such as base station or centralized management point in such networks. Also, the communicating mobile devices have become smaller, cheaper and more powerful. In the article "Mobile Ad hoc Networking: Imperatives and Challenges", Imrich Chlamtac, Marco Conti and Jennifer Liu have pointed out the importance of MANETs mainly because of their ability to provide network services for mobile users in places where a fixed pre-installed infrastructure is unaffordable, unreliable, not trusted or just not available [16]. Also, it is possible to connect the mobile ad hoc nodes to a fixed backbone network through a dedicated gateway device. In this way, IP networking services can be provided in places where the internet is not available.

Mobile Ad hoc Networking can be applied in large scale networks as well as in small-scale networks. For example, MANETs are efficiently used in military battlefields where planes, tanks, and soldiers on the ground can communicate with each other and relay information about situational awareness. Rescue missions and emergency disaster relief situations such as floods, fires or earthquakes use these networks as well. In such situations, quick deployment of a communications network is needed through which information can be exchanged between rescue team members. Sensor networks are used to take readings in places where it is difficult for people to reach physically. Temperature, pressure, toxins and similar properties of a place can be detected by such networks, thus proving helpful in various fields. For example, measurement of humidity in the ground for agricultural purposes, earthquake forecasts, etc. Also, MANETs are used by the students and teacher in classrooms or conferences for sharing data by setting up a network on the spot through mobile devices. VANET is a type to MANET which allows the vehicles on roads to communicate with the equipments fixed on roadside. MANETs are also used in commercial sectors, medical services, personal area networks, etc.

Over the years, one important concern about the Mobile Ad hoc Networks has been its security. The ultimate aim of the researchers is to make the MANETs efficient enough to provide protected communication between mobile nodes, in a hostile environment. As referenced in the paper "Routing Security in Wireless Ad Hoc Networks" by Hongmei Deng, Wei Li and Dharma P. Agrawal, published in IEEE Communications Magazine, wireless research indicates that the MANETs present a larger security problem as compared to conventional wired networks [21]. Basically, such networks are more vulnerable to attacks mainly because of the lack of centralized monitoring servers, wireless link and the dynamic nature of the network topology. Since the proper functioning of the mobile nodes cannot be managed by a centralized administration authority, a network layer protocol needs to be designed such that it will efficiently enforce connectivity and other requirements in the network. This will not only make sure that the network is secure but also allow the higher layer protocols to operate as needed. We cannot rely on the traditional methods of network security solutions in the case of MANETs.

Since this paper is mainly about "Secure Routing" in Mobile Ad Hoc Networks, it is important first of all to understand the aspects of routing. Routing, in general, is nothing but the act of moving information from a source to a destination within networks, occurring at the Network Layer (Layer 3) [24].

Furthermore, routing deals with – Routing Algorithms and Routing Protocols.
Routing Algorithms: These algorithms make decisions for the router to find out the best paths that packets in the network can take, to move from one node to another. The calculation of these best paths is done by using a variety of metrics like path length, reliability, delay, bandwidth, load, etc. Different types of routing algorithms can be used, which have a different impact on the network performance as well as routing resources. But, an algorithm to be used in the network cannot be selected manually. The routing protocol used in the network determines which algorithm to use. Usually different routing protocols use different algorithms. Also, the routing algorithm a certain routing protocol uses cannot be modified. The only way to change the algorithm utilized in a network is to change the routing protocol used. Routing algorithms can be classified into some types, e.g. static, dynamic, single-path, multi-path, link-state, distance vector, etc.
Routing Protocols: Routing protocols implement the routing algorithms and specify how routers in the network communicate with each other. They provide the information needed by the algorithm to perform its calculations. The protocol mainly collects the required information about the network and nodes in it, which is stored in a routing table in the router. The routing algorithm then uses this table to find out the best path to send data from one node to another. Routers in a network need to share route information with each other constantly so that their routing tables are updated. The Routing protocol also specifies how this information is exchanged between the routers. This paper will discuss in detail the different types of routing protocols that can be used in Mobile Ad hoc Networks, focusing on securing the network.

A number of IEEE papers and research papers were used for reference to get the information needed for this project. Most of them focus on the security issues in MANETs relating to the routing, whereas some focus on the solutions. In the rest of this theoretical paper, firstly I will discuss the background on Mobile Ad hoc Networks, giving the readers a basic idea on such kind of networks. These networks are very useful where a fixed infrastructure is not possible. MANETs have some security issues that will be addressed, especially related to the routing protocols. The background will also point out the extent to which routing affects security in MANETs.

Secondly, I will summarize a few research papers that have been published in the past few years, giving a general idea where MANETs stand currently and areas where research still needs to be done. Next, I will talk about the standard security goals for networks depending on which we can conclude whether Mobile Ad hoc Networks are secure or not.

Furthermore, I will be very specific to MANETs and point out the various vulnerabilities they have because of their inherent characteristics. Following it, the paper will evaluate in detail how an attacker can target the different vulnerabilities and perform a number of attacks to bring down the network or obtain important information. Most of those attacks take advantage of the vulnerable routing in Ad hoc Networks. I will also distinguish the attacks according to network layers. Most of the attacks take place on Physical (Layer 1), Data Link (layer 2), Network (Layer 3), Transport (Layer 4) and Application (Layer 7) of the Network OSI (Open Systems Interconnection) model.

Next, I will discuss various solutions to the issues faced by Mobile Ad hoc Networks. Focus will be how the routing protocols can be made more robust, which can help minimize most of the attacks and help secure the network. The existing secure routing protocols will be classified into different categories. Finally, I will conclude the paper with my thoughts and provide sources I used for my research.

2. METHODOLOGY

In this theoretical paper, the Security in Mobile Ad hoc Networks is being studied through referencing various IEEE papers and research papers. The basics of MANETs will be discussed, focusing on the security aspects by giving an overview of its current scenario. The report will discuss the history, distinct characteristics of MANETs and its applications, design constraints, security criteria to be achieved, susceptible nature of MANETs, the different types of security attacks and challenging issues. The current solutions and new approaches for securing the communication in such networks will be explored. The aim is to protect the multi-hop network connectivity between mobile nodes in the network. For full security, both data link and network layer should be considered. Also, mechanisms such as prevention, detection, and reaction, all should be given importance for complete security solutions. The area of focus for the security solutions has been mainly secure routing and data forwarding protocols [15]. Other than this, key management, nodal co-operation, mobility aspect, trust management, medium access, intrusion detection systems, etc. have also been in consideration to provide better security solutions.

The report will talk about the work that has been done over the years in the field of security in MANETs. We will learn how these networks play a vital role in the future of wireless communication technologies. I will survey the recent studies and mechanisms that have been done regarding the security issues in MANETs. The areas where more research needs to be done in the future will also be pointed out.

3. BACKGROUND

Mobile Ad hoc Network technology has been very promising since it is very efficient in scenarios where a fixed network infrastructure is unreliable, not needed or is unaffordable [14]. But there are challenges in implementing such networks, the most important of which is the security issue in MANETs. These networks have some limitations such as rapidly changing network topology, high power consumption, limited bandwidth, high error rates, limited physical security, etc. The network should be able to provide protected communication between the mobile nodes. First of all, it is necessary to determine the main goal of the security solutions for MANETs. It is indeed, to provide certain security services to the mobile users such as authentication, confidentiality, integrity, anonymity and availability. These goals are explained in detail in section 5 of this paper.

As mentioned in the article "Secure Routing for Mobile Ad Hoc Networks" by Patroklos G. Argyroudis and Donal O'Mahony, published in IEEE Communications Surveys & Tutorials, secure routing in MANETs is difficult as compared to the fixed networks, mainly because of the inherent characteristics of Ad Hoc Networks such as lack of infrastructure, rapidly changing topologies, high power consumption and high error rates, low bandwidth, etc. [6] These limitations make MANETs vulnerable to attacks, as compared to the traditional networks. An attacker will try to make use of the drawbacks of MANETs for his benefit as it is the easiest way for him to breach the network. In a fixed network that has a dedicated router and pre-defined infrastructure, additional layers of security are available such as access control lists in routers, firewalls, etc. This is not possible in MANETs because of its architecture, which makes securing such networks difficult.

New mechanisms, algorithms, protocols and fully secure schemes are being designed to overcome the security issues. Research has been going on the development of new security solutions for the Mobile Ad hoc Networks as well as modification of the current security solutions to apply to such networks. The solutions mainly use some hardware or cryptographic primitives. Usually, techniques applying preventive or reactive approaches help to protect the protocols and applications in most networks. The preventive defense line involves mechanisms that help to avoid attacks, whereas, in the reactive defense line, certain action is taken on demand with an aim to counter the attack.

Intrusion detection systems play an important role in making most traditional networks secure. Prevention of attack can never be guaranteed, making intrusion detection an important area of research. It is necessary to monitor the operations in a system, detect any suspicious behaviors and initiate a suitable response to secure the network. The aim of an intrusion detection system is to detect an attack as soon as possible, identify the attacker and block it before any damage is done to the network. However, since MANETs do not have a centralized management facility, it is difficult to detect an attack because of the difficulty in monitoring traffic [4].

Furthermore, key management mechanisms that are not based on the central point prove to be an important security solution for Mobile Ad hoc Networks. This is because MANETs do not have a fixed infrastructure or central points to place certification authorities. To be specific, management of the cryptographic keys is a major issue in such type of networks because of their architecture. [4]. To overcome this issue, modified Public Key Infrastructure (PKI) schemes can be used as a new security solution.

3.1. Secure Routing in MANETs

Routing in MANETs is challenging and vulnerable to attacks as compared to the fixed networks, mainly because of limitations such as rapidly changing topologies, high power consumption and high error rates, low bandwidth, etc [15]. In a fixed network, additional layers of security are available such as access control lists in routers, firewalls, etc. This is not possible in MANETs because of its architecture. Moreover, the co-operative nature of Mobile Ad Hoc Routing Protocols makes it easier for an attacker to tamper data, impersonate data or perform a Denial of Service attack. The attack on the routing protocols is hazardous as it can directly affect the performance and reliability of the network. Threats to Ad hoc Routing Protocols can either be from external attackers or faulty nodes within the network.

Some routing attacks directly target the route discovery or maintenance phase by not following the specifications of the routing protocols [23]. Unlike in fixed networks, a hacker can easily target the routing information in MANETs. He can introduce incorrect routing information, deform the correct one or simply replay old routing information. Any random mobile node in a MANET can selfishly compromise on the packet forwarding and routing operations just by interfering with the route discovery process or by sending wrong routing information to other nodes. Re-routing a packet is a huge security exposure. For example, a malicious node can send out incorrect information to other nodes in the network claiming that it is a neighbor of the destination where the packet is being sent through the network. This will cause all routes to the destination to pass through the malicious node. This node now has routing information for the entire network as well as the packet itself that was meant to be delivered to the destination. Thus, securing routing protocols is necessary.

The most important security solution in MANETs is securing the routing protocols. External attacks can be avoided by using cryptographic schemes. By making the routing protocols more robust, the selfish activities of nodes can be countered by forcing the malicious nodes to co-operate in the network. Another way of securing the routing protocols is using trust-based multi-path routing. In this type of routing, the message is divided into many parts and then these parts are encrypted. Here, the less trusted mobile nodes are assigned a lesser number of self-encrypted parts of a message being transmitted in the network separately using different paths. This method makes it difficult for the faulty nodes to crack the encryption and thus, acquire important data. Non-trusted routes can also be prevented by using this method.

Existing routing protocols for MANETs can be classified as: Table-driven ad hoc routing protocols, Source-initiated on-demand ad hoc routing protocols and hybrid protocols. Routing protocols such as Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector (AODV) are widely used in MANETs. These and a few more routing protocols will be discussed in detail in later part of the paper. An important issue with DSR and AODV protocols is that they trust all nodes in the network and thus, are susceptible to attacks.

4. REVIEW OF RELATED LITERATURE AND RESEARCH

4.1. Security Issues in Mobile Ad Hoc Networks - A Survey

- Wenjia Li and Anupam Joshi

The 17th White House Papers Graduate Research In Informatics at Sussex, 2004

This research paper begins with discussing the current scenario and demand of Mobile Ad hoc Networks and defining it. A Mobile Ad hoc Network, in general, is a temporary network of wireless mobile nodes that dynamically organize on its own, in arbitrary network topologies. MANETs use multi-hop communication for the delivery of data. Some of the basic features of MANETs are:

- Unreliable nature of the wireless links between nodes, mainly because of their mobility and limited power supply.
- Because of the mobility of nodes in MANETs, the network topology changes constantly and unpredictably.
- Typically in routing protocols, it is necessary for the nodes to incorporate in a particular routing issue. But in the case of statically configured wireless routing protocols, this becomes difficult since the topology of MANETs keeps on changing.

Next part of the paper talks about the various vulnerabilities of the Mobile Ad-hoc Networks that will be discussed in detail in later. Further, the security criteria or the security goals are pointed out which are as follows: availability, integrity, confidentiality, authenticity, non-repudiation, authorization and anonymity. These are nothing but the basic requirements that should be reached by MANETs to make sure that the network is secured.

Moreover, the paper discusses the different types of attacks in Mobile Ad hoc Networks. The attacks can be classified into two types: external attacks and internal attacks. The various types of attacks will be discussed in detail later.

Finally, the paper points out various security schemes in MANETs to overcome the attacks. The different schemes are as follows:

- Intrusion Detection Techniques

There are different ways in which an intrusion can be detected.

(i) Architecture can be created in which every node in the network consists of an intrusion detection system agent. These agents have the capability to detect any kind of intrusion behavior, independently or by coordinating with each other.
(ii) Clusters of nodes that fall within the same radio range can be formed and only one node in a particular cluster monitors for an intrusion detection. This saves power supply in the MANET.
(iii) A cross-layer analysis can detect any misbehavior in the Mobile Ad-hoc Network.

- Secure Routing Techniques

There are a few mechanisms for defense against specific kinds of attacks such as wormhole attack, rushing attack, etc. Also, components such as watchdog and path rather are very useful. The main function of a watchdog is to copy packets to be forwarded into a buffer n then monitor how the adjacent nodes respond to these packets. Information about a detected malicious node is sent to the path rather.

This paper gives a detailed knowledge of how the Mobile Ad hoc Networks are more vulnerable than the traditional networks and the different types of attacks in it. It mainly focuses on how the attacks can be dealt, with using various security measures so that such types of networks can be used to its full potential.

4.2. Security Vulnerabilities in Ad Hoc Networks

- Po-Wah Yau and Chris J. Mitchell

Mobile VCE Research Group, Royal Holloway, University of London
The Seventh International Symposium on Communication Theory and Applications (ISCTA),
July 2003

This paper mainly focuses on security vulnerabilities in Mobile Ad hoc Networks by classifying them in detail. MANETs are prone to attacks from both, external nodes as well as internal nodes. Threats from internal nodes are more hazardous than the external nodes as they have the required authorization credentials for participating in the network and communicating with other mobile nodes.

We know that the main difference of the MANETs as compared to the conventional networks is the lack of pre-installed infrastructure. Due to this, such networks face problems regarding centrally controlled security. Also, we cannot rely on the security mechanisms that involve trusted third parties in case of Mobile Ad hoc Networks. Since

MANETs have a dynamically changing topology, it's necessary that the security has to be scalable. Because of the bandwidth and energy constraints in such networks, there are problems with heterogeneous networking. In this paper, the authors also describe a general threat model for MANETs. This model classifies the different behaviors of mobile nodes in case of both, external and internal threats. An important area of research in Mobile Ad hoc Networks has been the setting up and maintenance of ad hoc infrastructure by using new routing protocols, since most of the existing routing protocols are resource intensive. This paper also talks about some routing protocols that have been proposed to suit MANETs. They are classified as reactive protocols and proactive protocol, which will be discussed in detail later. Some hybrid routing protocols have been proposed as well which use both, pro-active and reactive techniques. Also, some scenarios for simulations of MANETs have been pointed out in this research paper.

Furthermore, the paper talks about a "Routing Threat Model" where first of all the security requirements or goals are stated, followed by the different threats to Mobile Ad hoc Networks.

There are two types of threats to Mobile Ad hoc Networks: External threats and internal threats: External Threats and Internal Threats. These threats will be discussed in detail later, including their sub-divisions. The external threats can be sub-divided as passive eavesdropping and active interference. On the other hand, internal threats can be sub-divided as failed nodes, badly failed nodes, selfish nodes, and malicious nodes. It's the malicious nodes that deliberately perform many attacks on the Mobile Ad-hoc Network.

The goal of the paper is to come up with simulations to test the security mechanisms in MANETs, considering the four types of node misbehaviors discussed earlier. Some properties of network topology need to be taken into consideration while designing secure protocols and simulations since they directly affect the possible threats to Mobile Ad hoc Networks. The properties are as follows:

- <u>Size</u>: The network size should be variable. It can be large or small depending on the nodes entering and leaving the network.
- <u>The density of Nodes</u>: It's better to have many nodes in the network to minimize the denial of service attacks. But, the threats to network integrity can be more hazardous to the network in this case.
- <u>The position of Nodes</u>: Since some nodes can drift in and out of the range of network at the perimeter, we can make the perimeter of the network physical or use a logical perimeter consisting of a group of mobile nodes co-operating with each other.
- <u>Grouping</u>: It can be useful to simulate the grouping of nodes since the mobile nodes tend to communicate with a common group of nodes, e.g. a group closest to it.

- Mobility: It’s not necessary for all the nodes in an ad hoc network to be mobile. Thus, it can be helpful if protocols and their simulations also consider fixed nodes in the network.
- Relationships: We should consider the relationship of a node to another node when it sends a random data packet to that other node. The relationship can be either short term or long term.

4.3. Survey of security issues in mobile ad hoc and sensor networks

- D. Djenouri , L. Khelladi and A. N. Badache

IEEE Commun. Surveys & Tutorials, vol. 7, 2005

This paper talks about how the Mobile Ad hoc Networking have gained importance these days because of various wireless devices being produced. Sometimes it’s not possible to have a fixed infrastructure for the network. This is where the MANET technology proves to be very efficient. For example, in a situation of emergency disaster relief in a damaged place, digital sensors to work efficiently in unreachable areas, military purposes and information shared by students in a classroom lecture. A MANET can be defined as a temporary network of mobile nodes which does not have a fixed pre-installed infrastructure or a central administration authority.

There are various challenges in MANETs such as limited resources for mobile devices, rapid topology changes as a result of mobility of nodes, unreliability and limited bandwidth of the wireless channel, etc. Also, the mobile nodes hardly have any physical protection, and there is no certification authority or centralized monitoring agent in these networks. This makes securing the Mobile Ad hoc Networks a difficult task to achieve.

Earlier, researchers mainly focused on the routing protocols in MANETs, but since they considered only trusted nodes, security couldn’t be achieved fully. The paper, in general, is a survey of the recent studies that have paid more attention to the security problems in MANETs. Various mechanisms have been designed to provide security to the basic protocols and applications. The authors point out different security problems in MANETs and its current solutions, taking into consideration the different network layers. The main security issues that are mentioned in this paper are routing and data forwarding, secure key management, medium access, etc. Intrusion detection techniques are also important for the security of these types of networks.

First of all, some basic concepts about Mobile Ad hoc Networks have been discussed such as the security requirements and the unique characteristics that make them more vulnerable to attacks compared to the traditional networks. Then the paper talks about threats in MANETs, which can be classified as attacks and misbehaviors. Attacks can be classified according to their origin as external attacks and internal attacks. They can also be classified according to their nature as passive attacks and active attacks. Misbehavior is nothing but a faulty behavior of an internal node that can cause damage to the network.

Further, the authors focus on security issues regarding routing and the different attacks on the routing protocols. The intruder can perform these attacks by modifying the routing information or generating false routing messages in the network. Spoofing and rushing attacks have also been discussed. Later, some current solutions to these attacks have been pointed out. Next, security issues regarding data forwarding are noted, and some solutions are proposed to them as well. Then the security issues in MAC-layer protocol are discussed with its current solution that is difficult to achieve. Moreover, the paper talks about key management in MANETs. Key management has been an important area of research as it is the first step to secure applications and underlying protocols in MANETs. After that, the intrusion detection systems have been explained in detail. Problems in the traditional intrusion detection techniques and their solutions have been shown. The paper ends by discussing a type of Mobile Ad hoc Networks, the wireless sensor networks, and the security issues in it.

Various aspects of the Mobile Ad-hoc Networks have been surveyed in detail by the authors in this paper. This article mainly helps in getting information about the current solutions to MANETs to tackle the security issues.

4.4. Secure Routing Protocol: Affection on MANETs Performance

- Shervin Ehrampoosh and Ali Mahani

International Journal of Communications and Information Technology (IJCIT),
Vol.1,
December 2011

Since Mobile Ad hoc Networks are infrastructure-less and lack centralized management as in fixed networks, it is difficult to find out whether a node in the network is trusted or not. Drawbacks such as open resource constraints, wireless medium, dynamic network topology, lack of centralized monitoring and management and no clear line of defense, make it, even more, difficult to protect such network from attackers. Securing MANETs is essential especially because of the areas in which such networks are used, e.g. military applications, battlefields, emergency disaster situations. In such networks, any user can access the network and leave it anytime, making it easier for an attacker to perform attacks such as passive eavesdropping, active signal interface, network jamming, etc. Moreover, the co-operative nature of Mobile Ad Hoc Routing Protocols makes it easier for an attacker to tamper data, impersonate data or perform a Denial of Service attack. Attacks on MANETs can be classified into different types based on behavior or source of attack, processing capacity of the attacker and number of attackers. A very popular attack is the Black Hole Attack. Here, the malicious node replies to the sender of RREQ packet with a false RREP packet making the sender think that it has the latest route to the destination and thus, ignoring RREP packets from other nodes in the network. The sender now sends the data packets to the malicious node, which does not forward the data packets to the destination but keeps them to itself.

Conventional security solutions such as using cryptographic schemes, especially Public Key Infrastructure (PKI) and intrusion detection systems prove to be useful for most of the networks. But these mechanisms are not very efficient in case of Mobile Ad hoc Networks because of their architecture. Since MANETs do not have a centralized management facility, it is difficult to detect an attack because of the difficulty in monitoring traffic. Also, it hinders trust management for the mobile nodes. All the mobile nodes in a MANET act as a router for forwarding information. Thus, it is important to secure the routing protocols to secure the network itself. This paper focuses on evaluating and comparing the performance metrics of routing protocols in MANETs such as AODV, OLSR, and MAODV. MAODV is a much secure routing protocol compared to the former two, because, in this protocol, the neighbors of a node help it to recognize trusted and untrusted nodes.

Furthermore, the paper points out how routing protocols in MANETs can be distinguished. They can be classified into four different types: i) Single Phase routing, ii) Two Phase routing, iii) Proactive /Table-driven routing protocols and iv) Reactive/Source-initiated routing protocols. These types will be elaborated in detail later.

The paper also discusses some techniques by which the Black Hole Attack can be tackled. For example, digital signatures, message authentication codes (MAC) and hashed MAC can be very useful. Authenticated Routing for Ad-Hoc Networks (ARAN) and SAODV are effective routing protocol that can be used to avoid the Black Hole Attack. Modified AODV is discussed in detail and is considered as a secure routing protocol for MANETs because, in this protocol, the neighbors of a node help it to recognize trusted and untrusted nodes in the network. To prove that MAODV is much secure than the conventional routing protocols: AODV and OLSR, various simulations are performed further in the paper. The simulations show that when these three protocols are under Black Hole Attack, the packet delivery ratio of MAODV is better than that of AODV and OLSR under different scenarios like increasing traffic load, mobility, network size, etc.

4.5. Secure Routing for Mobile Ad Hoc Networks

- Patroklos G. Argyroudis and Donal O'mahony

University Of Dublin, Trinity College
IEEE Communications Surveys, vol. 7, no. 3,
2005

The nodes in MANETs communicate with each other through a wireless medium, forming dynamic topologies. Since there is no fixed infrastructure in such networks, there are no dedicated nodes to provide network management operations. For maintaining proper communication in the network, all the nodes in MANETs need to perform routing. Hence, a reliable and secure ad hoc routing protocol is needed. This paper talks about some traditional routing protocols and how they are susceptible to different types of attacks on ad hoc networks. The possible attacks that a malicious node can perform to disrupt the operation of a routing protocol in a MANET are discussed. Further, secure ad hoc routing protocols are classified and presented. Next, a detailed comparison is made between these secure protocols.

The existing routing protocols are distinguished on two approaches: the table-driven approach and the source-initiated on-demand approach. The table-driven ad hoc routing protocols are also called as proactive protocols and are less adaptable to MANETs. They periodically update the routing information and makes sure that every node has up-to-date routing tables. Thus, all the nodes in the network can make immediate forwarding decisions. Protocols such as Destination-Sequenced Distance-Vector (DSDV) protocol and Optimized Link State Routing (OLSR) protocol follow this approach. In DSDV protocol, every node in the network maintains a periodically updated routing table, consisting of all the possible destinations. Each table entry also has a sequence number to avoid routing loops. The OLSR protocol first senses the neighbors by periodically transmitting "hello" messages. Then every mode distributes the signaling traffic by forwarding a flooded message that it has not forwarded previously. Finally, the topological information is distributed among the nodes.

The source-initiated on-demand ad-hoc routing protocols are also called as reactive protocols and are more adaptable to MANETs. They do not periodically update the routing information. Routes are forwarded to a node only when necessary. A route is acquired by the initiation of a “route discovery” function by the source node. Examples of protocols following this approach are Dynamic Source Routing (DSR) protocol and Ad hoc On-demand Distance Vector (AODV) routing protocol. DSR is a reactive protocol in which the complete route is chosen by the source and is forwarded by each packet. Every node stores the source routes learned, in its cache. Before sending a packet, the node first checks in its cache if it has the route to the destination. If it doesn’t have one, it broadcasts a request packet (RREQ) in the network for route discovery. When a node receives this request packet, it first looks in its cache if it has the route to RREQ’s destination. If it does, it sends a route reply packet (RREP) to the source. If it doesn’t, then the node adds its address to the RREQ and broadcasts it again. If a node detects route failure, it sends route error packet (RER) to the source that uses this link. AODV is a hop-by-hop routing protocol. In this protocol, the source does not put the complete route in the packets being forwarded. Instead, the next hop decision is made separately after each hop. If a node has a route to the destination or is the destination itself, it sends RREP packet through the same path until it reaches the source. Each node within the path then updates its routing table.

But an important issue with these traditional routing protocols is that they do not consider the possibility of a threat targeting the disruption of the protocol itself. They trust all the nodes in a network to forward the traffic correctly, and thus, are very susceptible to attacks. Also, features of MANETs such as rapidly changing topologies, low bandwidth, high power consumption and high error rates worsen the situation. The routing operation can be disturbed by either internal attacker or external attacker. The possible attacks that can disrupt the operation of a routing protocol in a MANET are as follows: Location disclosure, Blackhole, Replay, Wormhole, Blackmail, Denial of service and Routing table poisoning.

Researchers have come up with some secure and robust ad hoc routing protocols that can protect the network against these attacks. Some solutions are completely new stand-alone protocols while some are modifications to the existing protocols. The secure ad hoc routing protocols will be discussed in detail later.

5. SECURITY GOALS

To evaluate whether a Mobile Ad hoc Network is secure or not, first of all, it is necessary to determine a security criteria or security goals for protecting the network. These goals are more generic, rather than specific to MANETs. Other than these, more specialized and application-oriented security goals exist such as location privacy, self-stabilization, Byzantine Robustness, etc. Similar to the traditional networks, security of the ad hoc networks can be judged by the basic security goals. Various research papers were studied regarding security goals in both, traditional networks as well as MANETs. Some papers gave information on only the first four security goals since they are the most important ones. Few papers pointed out the rest as well [2]. Thus, a complete list of basic security goals is as follows:

5.1. Availability

Availability means that the network services or data should be available to authorized users whenever they want, despite an attack on the network. To be specific, the network should be able to tackle attacks such as Denial of Service attack, energy starvation attack or simply node misbehavior. In other words, if a route exists to a certain node in MANET, then any node in the network should be able to get that route when needed.

5.2. Confidentiality

Confidentiality makes sure that particular information cannot be accessible to anyone other than authorized users or the desired recipient of that information. Data encryption techniques usually achieve this goal. In MANETs, it is also necessary that the routing information must be secure at all times.

5.3. Integrity

This security goal ensures that the data being transmitted from one node to another in a network is never modified by anybody except authorized nodes. The information could be corrupted in two ways: Malicious altering, where a hacker intentionally attacks the network, and Accidental altering, where the modification or loss of information is caused because of some failure in the network such as transmission or hardware issue. The integrity of a MANET is directly dependent on the nodes following correct routing methods and transmitting proper routing information.

5.4. Authentication

Authentication makes sure that the communicating nodes in a network are trusted, and not impersonator. The nodes need to prove their identities to start communication. This ensures that a malicious node cannot pretend to be a genuine one, and thus, cannot acquire critical information or transmit incorrect information within the network. If this security goal is compromised, an attacker can gain access to the network by posing as a genuine node and manipulate the route that traffic takes to reach a particular destination. An effective way to prevent this is configuring passwords to use within the routing protocol configuration, thus ensuring that every node in the network is authentic.

5.5. Authorization

This is a security goal that assigns different access rights to different users. Here, a user is given a certain credential, which determines what level of privileges he will have for communication within the network. For example, some users can only have read access while others can have read/write as well as network management capabilities. The advantage of this goal is that we can be safe by giving write permissions only to the most trusted nodes in the network. The nodes that are less trusted or new in the network can be given only read permissions so that they are not able to make any configuration or algorithm changes, primarily related to routing.

5.6. Non-Repudiation

Non-repudiation is nothing but ensuring that the sender of a certain message cannot deny having sent that message. Similarly, receiver of a message cannot deny having received it. This security goal is very important for detecting a compromised node in the network and then isolating it. It means that even after false routing information is injected into the network, the attacking node cannot deny the malicious behavior. Thus, once the origin of false routing information is traced, the compromised node can be detected and banned from the network.

5.7. Anonymity

This security goal states that any information that can identify the user of a node in the network must be kept confidential by default and not be distributed among other nodes. Anonymity makes sure that the privacy of users in the network in maintained. It proves to be useful in cases where an attacker wants to target a particular person. This goal is not relevant to routing in MANETs.

5.8. Accountability

This requirement is essential so that actions affecting the network security can be systematically logged and protected. By default, actions of every node in the network are logged. Hence, suspicious activities can be marked and nodes posing a threat can be detected so that measures can be taken against them. This security goal is not specifically related to routing. But, any malicious behavior in the network, including false routing, can be found out in the logs.

6. VULNERABILITIES

6.1. Lack of centralized management/monitoring and infrastructure

Mobile ad hoc networks do not have a centralized management or monitoring server. Each node acts as an independent router and operates in distributed a peer-to-peer mode. Because of this, it is very difficult to detect attacks, path breakages, packet drops or transmission issues. The main reason for the difficulty, as discussed in “Security Issues in Mobile Ad Hoc Networks - A Survey” by Wenjia Li and Anupam Joshi, is that it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network [2]. It also hinders trust management of nodes within the network as anybody can join the network at any time without any security requirement, thus making it difficult to distinguish between trustworthy nodes and malicious nodes.

6.2. Lack of predefined boundary

In general, a network can be secured from the outside attackers in a more efficient way if its boundaries are predefined so that we can distinguish between internal users and external users. This helps to narrow down and avoid attacks coming from outside the network. Typically, firewalls are placed right at the boundary of a network to filter out malicious traffic originating from outside the network. But in the case of MANETs, do not have a clear line of defense or a predefined boundary that separates the inside network from outside one. This is because any node can join, leave or move within the network at any time, regardless of being a legitimate user or an attacker. So there is no secure boundary to protect an internal network from outside adversaries. As long as the attacker is in the radio frequency range of just one node in the network, he can communicate with that node, and then target and perform an attack on any other node in the entire network. On the other hand, a traditional wireless network has a predefined boundary, i.e. the radio frequency range of wireless access point.

6.3. Cooperativeness

As pointed out in “Security Threats in Mobile Ad Hoc Networks” by Sevil Şen, John A. Clark and Juan E. Tapiador, the routing algorithms for MANETs usually assume that nodes are cooperative and non-malicious [22]. Since the routing algorithms rely on mutual trust and cooperative participation of all nodes in the network, an attacker can easily take advantage of this vulnerability. He can perform an attack that intentionally disrupts the cooperative nature of operation of the network. A malicious node can simply pose as a neighbor to other nodes in the network and participate in important routing decisions, thus affecting the network operation. This vulnerability doesn't exist in traditional wireless networks since the nodes in it do not need to cooperate with each other for routing decisions.

6.4. Restricted power supply

As the mobile nodes in a MANET use batteries as their power supply, its restrictiveness is a major vulnerability. The limited processing power of each node adversely affects the services and routing decisions performed by it. Various attacks can be performed by a hacker to take advantage of this. He can perform a denial-of-service attack by continuously sending unnecessary packets to a node, causing the node to waste its battery, and thus go out of service. Also, a node in a mobile ad-hoc network may behave selfishly, avoiding the routing decisions or cooperative algorithms to save its battery. In the case of traditional wireless networks, this vulnerability is limited only to the mobile nodes, but not to the wireless access points and routers/switches in the network, and hence is not that critical.

6.5. Dynamic network topology

Since the nodes in a mobile ad hoc network can move independently and join or leave the network whenever they want, the topology of the network changes constantly. It is very unpredictable and random, which frequently causes route changes, network partitions, and packet/data losses. It also disturbs the trust relationship among nodes. For example, nodes that are in the network for a longer period of time, develop trust with each other and carry most of the routing decisions for the entire network. If suddenly a couple of these important nodes leave the network, the trust relationship they had with their adjoining nodes will be lost. The nodes still in the network will again have to develop mutual trust with new nodes, thus slowing down the network operation to some extent. Furthermore, the dynamic nature of the network makes it difficult to differentiate between a legitimate behavior and malicious behavior. A node sending suspicious routing information to its adjacent nodes might be a malicious node or a genuine one, simply forwarding outdated routing information because it didn't receive any latest information yet.

6.6. Scalability

The scale of MANETs keeps changing continuously because any number of mobile nodes can join and leave the network anytime [2]. It cannot be predicted how many numbers of nodes will be there in a network in a certain time. Therefore, the security mechanisms, interoperability of nodes and routing protocols in mobile ad hoc networks need to be flexible with the scale of the network. They should work efficiently for a small number of nodes in the network as well as a large number, and they should adapt quickly to the continuously changing scale. In a scenario where the protocols and services fail to scale up and down as needed, a hacker can easily take advantage of the situation. It will be like a free pass for the hacker if the security mechanism in a MANET fails on its own, simply because of not being able to adapt to the continuously changing scale of the network. Scalability in traditional wireless networks is fixed. It can only have a certain number of nodes that the wireless access point or router can handle routing for.

6.7. Multi-hop Routing

As mobile ad hoc networks do not have a default router or gateway, each node in the network acts as a router by forwarding packets, as well as an end user. All the packets in a MANET follow multi-hop routes, i.e. mobile nodes in the network forward packets to each other until the packets reach their final destination. This type of routing is a major vulnerability because a malicious node can take advantage of the packets forwarded to it and bring down the network. This vulnerability is very specific to MANETs because, in the case of traditional wireless networks, the mobile nodes can only communicate with a central wireless access point, which then forwards packets to the destination node.

6.8. Compromised nodes within the network

Attacks caused by a node within a MANET are more dangerous than those caused by a malicious node outside the network [2]. Since such networks assume that the nodes in it are trustworthy and the fact that anybody can join or leave the network spontaneously, it is difficult to detect and prevent the attacks. For example, a legitimate node in the network will have no idea that its adjoining node that it is trusting and sharing information with is an attacker eavesdropping on the network. Also, because the nodes can move freely within the network, the attacker can change its target whenever he wants, or a compromised node can easily perform attacks on multiple nodes in the network. The mobility of the nodes makes it, even more, difficult to detect attacks and especially source of the attack. A compromised node in MANET can act like a legitimate node, but could take advantage of the access to forwarded packets or drawbacks in routing algorithm, eventually disrupting the network communications.

6.9. Variation in link/node capabilities

The mobile nodes in a MANET usually have varying transmitting, receiving and processing capabilities [16]. Their operating frequencies, channel capacities, and bandwidth may also be different. These variations might lead to asymmetric links. Also, it is difficult to design routing protocols and security mechanisms for such networks because they need to be able to adapt to asymmetric links and dynamically changing network. For a network that has a weak security mechanism simply because it is not adaptable to asymmetrical links, this would be an ideal opportunity for an attacker to explore the weakness. The nodes in a traditional wireless network, on the other hand, usually have similar link/node capabilities, to be able to communicate with the wireless access point efficiently.

7. ATTACKS ON MANETS

The attack, in general, is a planned activity that aims to disrupt a network. This section describes various attacks that are knows to be performed on MANETs. It should be noted that most of the attacks apply to other types of networks like the traditional wired and wireless networks as well. However, the MANETs are much more vulnerable to them because of their inherent characteristic pointed out earlier. The attacks can be divided into two main types: origin-based attacks and nature-based attacks. Origin-based attacks are those attacks that are categorized with respect to where they are originated from. An attack can either be originated from a node within the internal network or from a node outside the Mobile Ad-hoc Network. In other words, origin-based attacks can be further classified as - internal attacks and external attacks.

On the other hand, nature-based attacks are those attacks that are categorized with respect to their nature. There are two ways in which the hacker can breach a network, either by being a part of the network and only gaining critical information which can later be used adversely, or by interrupting communications in the network in some way. Nature-based attacks are sub-divided into – passive attacks and active attacks. [4] Furthermore, attacks can also be categorized according to the network protocol stacks they target. This paper will discuss each type of attack that is known to be performed on Mobile Ad-hoc Networks in detail, giving their examples.

7.1. Origin-based Attacks

7.1.1. External Attacks

These attacks are caused by the external unauthorized nodes i.e. the nodes that do not belong to the logical ad hoc network or are banned from accessing the network. Attacks performed by external nodes can be easily detected by using traditional security methods like membership authentication techniques and firewalls. The targets of these threats are mainly physical layer and data link layer of the network. Usually, the goal of the hacker is to cause traffic congestion, propagate faulty routing information into the network or prevent the nodes from providing services. [2]

7.1.2. Internal Attacks

These attacks are caused by the nodes within the network and are difficult to detect since they arise from trusted nodes that have the required authorization credentials for participating in the network activities and communicating with other mobile nodes.

Internal attacks are much more hazardous to the network as compared to external attacks because of the pervasive communication nature, open network media in MANETs and the fact that hijacked nodes already belong to the network as authorized entities. [2] The goal of an attacker, in this case, is to gain access to the ad hoc network and participate in the network activities, either by acting as a genuine new node or by compromising an authorized node in the network to use it for conducting the malicious behaviors. Also, the defense mechanisms used against external attacks are not effective against the internal ones.

The unreliable internal nodes can be classified by their misbehavior as follows:

i) *Failed nodes*: These nodes merely refrain from performing certain protocol-specified operations because of some unforeseen failure in the network or environmental conditions. It can be a big issue for routing in MANETs if nodes are unable to update data structures or forward data packets to other mobile nodes. Inability to forward authentication data, routing information, route error messages can be harmful for the network. Failed nodes in a network are the most hazardous if they are part of an emergency or secure route.

ii) *Badly failed nodes*: In addition to not forwarding messages, these nodes usually perform faulty operations such as sending false routing information, in turn, introducing misleading information into the network. This affects the network integrity adversely. Also, resources and bandwidth are wasted because of these nodes, especially in cases where they send false route requests for a node that does not exist or where they unnecessarily request routes which they already have. A badly failed node can also reply a source’s genuine route request with a false route, resulting in false routing being forwarded throughout the MANET. A false route error message will cause a working link to be marked as failed one, thus resulting in alternative route discovery process.

iii) *Selfish nodes*: These nodes are similar to failed nodes as they do not perform certain protocol-specified operations like packet forwarding, but it’s because of some selfishness, i.e. to enhance their performance or save resources. They exploit the routing protocol such that it acts as an advantage for them, but not for the network. Packet dropping is an attack caused by such nodes. This attack is serious because most routing protocols currently used in Mobile Ad-hoc Networks do not have a mechanism to detect whether a data packet is properly forwarded to the destination or is dropped in the way.

iv) *Malicious nodes*: These nodes have the ability to attack the network and interrupt the communication or services deliberately. They can directly disturb the network integrity, misdirect traffic or exploit the route maintenance capabilities. Such nodes can be hazardous when an attack is performed on routing protocol specific optimizations. Malicious nodes are most dangerous nodes as they can directly disrupt the normal operation of routing protocols. These nodes cause many attacks, Denial of Service attack being the most common one. [3]

7.2. Nature-based Attacks

7.2.1. Passive Attacks

The goal of passive attacks is to analyze and collect valuable information about the network and nodes in it by unauthorized listening to information from traffic routed in the network. The information could be node hierarchy, network topology or something specific to the nodes like their location. This information can be used later to perform a harmful active attack. Passive attacks do not disrupt the communications in MANET or operation of routing protocols directly, which makes them difficult to be detected. These attacks are usually internal ones and are easy to perform in MANETs compared to traditional wired networks because of the shared nature of wireless communication medium. Eavesdropping, traffic analysis and traffic monitoring are the most common examples of passive attacks, which will be elaborated in the later part of the paper. Even though these are described as “attacks”, it should be noted that passive attacks do not harm the network directly, but only gain access to critical information propagating within the network.

7.2.2. Active Attacks

An active attack is an attempt to modify the data transmitted within the network, gain authentication, prevent communications between the mobile nodes or cause traffic congestion. The attacker can also send some malicious data into the network with an intention of disrupting the network. These attacks can be internal – carried out by the attacker via a malicious node that is part of the network or external – performed by the attacker via an outside source. There are various kinds of active attacks known, e.g. sleep deprivation torture attack, hijacking, jamming, spoofing, replay, etc., most of which result in and can be generalized as a Denial of Service attack. Each of these attacks will be discussed in detail later. In these attacks, the hacker blocks the wireless communication channel or causes some problems in communications within the network. The effects of these attacks on the MANET usually vary depending on their duration and the routing protocol used. For example, if the network uses a reactive routing protocol, a Denial-of-Service attack may be assumed as a link failure, resulting in the discovery of alternate routes to the destination. If the network uses a proactive routing protocol, the route having link failure will be timed out and deleted after a certain time.

Furthermore, active attacks can be grouped into four major categories:

7.2.2.1. Dropping Attacks*:*

In these types of attacks, compromised nodes in a Mobile Ad hoc Network intentionally drop all the packets that are not destined for them, thus preventing end-to-end communications. They are mainly caused by selfish nodes and malicious nodes, both having different aims for the attack. A selfish node performs this attack to preserve its resources since the mobile nodes have restricted power supply. On the other hand, malicious nodes perform it to disrupt the network performance. To be specific, network performance is affected by data packet drops because it may unnecessarily lead to retransmission of packets from the source node or new alternative routes to the destination being discovered in the network. If the dropping node is at a critical point, dropping attacks can prevent end-to-end communications between the mobile nodes. Dropping attacks are difficult to detect since most routing protocols currently used in MANETs do not have a mechanism to detect whether packets have been forwarded to the destination or not. [22] An alternative solution to this drawback of routing protocols is that the neighboring mobile nodes can detect packet drops through passive acknowledgment or hop-by-hop acknowledgment.

- *Selective Dropping Attack*: This is a smarter way of performing dropping attacks. Here, the attacker chooses to drop only a few data packets via a malicious node, instead of dropping all of them. This strategy helps the attacker to avoid being detected. The attacker can also choose to drop a particular type of data packets, for example, he can only drop route error packets. Because of this, the source nodes will be unaware of failed links in the network and continue to try to use them. This will create bottlenecks and new alternative route discovery will be prevented.

7.2.2.2. Modification Attacks:

Modification attacks can be very harmful to MANETs since a malicious node directly modifies original data packets in the network, affecting data integrity. These attacks can target routing by modifying route sequence numbers, hop counts, source route, etc. A sinkhole attack is an example of modification attack that will be discussed in detail further in this paper.

7.2.2.3. Fabrication Attacks:

In these attacks, fake messages are generated and advertised in the Mobile Ad-hoc Network. Fabrication attacks are usually concerned with routing in the network and are difficult to detect because the false routing messages seem to be genuine. Some typical scenarios of such attacks are:

- *Fabricated routing error message*: Here false routing error messages are advertised in the network. A malicious node sends a message that a particular neighboring link is failed, and thus no messages should be forwarded to the concerned node. Hence, that node will be cut out of all the communications happening in the network.
- *Active forge*: In this attack, the attacker sends out any fake message, ensuring that any related messages will not be received back. Active forge can easily cause misdirection of network traffic, if the malicious node advertises wrong routing information with an intention to capture secure data that was meant for the destination node.
- *Forge reply*: Here the adversary node sends out false route replies in response to genuine route request messages. The malicious node will falsely reply that it has the best route to a certain destination node. Thus, once the attacker receives the data packet, he will not forward it to its real destination, but instead use it to gain valuable information. [22]

7.2.2.4. Timing Attacks:

Timing attacks are attacks where a malicious node in MANET attracts other nodes by falsely causing itself to appear closer to them than it actually is. Since the genuine nodes tend to forward packets to nodes that are nearest, the malicious node receives most of the network traffic. Typical examples of such attacks are Denial of Service attacks, rushing attacks and hello flood attacks. These attacks will be discussed in detail further. [22]

7.3. Classification of Attacks based on the Network Protocol Stacks

Attacks on MANETs can also be classified according to the network protocol stacks of the OSI (Open Systems Interconnection) model. Most of the attacks are performed specifically on:

- Physical layer (Layer 1)
- Data Link layer (Layer 2)
- Network layer (Layer 3)
- Transport layer (Layer 4)
- Application layer (Layer 7)

Some attacks affect multiple layers, which will be described as Multi-layer attacks.

This is a comprehensive list of all the well known attacks that are performed on Mobile Ad-hoc Networks. A number of research papers were referred to describe the attacks. Most of the research papers focused primarily on the attacks that target the operation of routing protocols in MANETs [6], while some briefly pointed out the attacks on each of the above mentioned network layers.

7.3.1. Physical Layer Attacks

- Eavesdropping:

Eavesdropping is a very common attack performed on Mobile Ad-hoc Networks. The primary aim of the attacker is to capture confidential information either about the network or the mobile nodes in it. If the information is about the network, it could be the routes to certain nodes. If the information is about the nodes, it could be the location of the node, public/private keys or passwords used by the node, etc. Typically this is an internal attack, i.e. the attacker somehow gains access to be part of the network or uses a compromised node which is already an authorized entity of the MANET. The attacker does not directly interfere with the network traffic, but only places itself near the target node physically in order to listen to its ongoing communications. He uses powerful receivers tuned to proper frequency for listening to the broadcasted signals, thus taking advantage of the wireless medium. The information collected can later be used to perform an active attack or simply leak it to everybody. [2] Even though eavesdropping is called an "attack," it is not a traditional attack since it does not directly disrupt the communications in the network.

- Jamming:

Jamming, in general, causes a channel to become unavailable because of it being overused. This is an active attack which can be generalized as one of the types of Denial of Service attacks. Here the attacker uses a powerful transmitter to generate continuously spurious signals targeted towards the entire network or a specific node, once the radio frequency of communication in the network is determined. This leads to disrupted communications in MANET since the real signals propagating within the network become corrupted or are lost. Random noise and pulse are common examples of this bogus signals used intentionally for jamming a network. [23] If the attacker is targeting a particular node in the network, he physically places himself near that node and transmits bogus signals towards it to interfere with its communications effectively.

- Active Interference:

Active interference is also a type of Denial of Service attack. Here the hacker's intention is to block the wireless communication channel or interrupt communications happening in the network by fabricating the order of messages or simply replaying old messages again and again. Forwarding old routes causes false routing messages to be propagated throughout the network, thus disrupting communications between the mobile nodes. [3]

7.3.2. Data Link Layer Attacks

- Traffic Analysis:

This is typically a passive attack where the attacker aims to identify important information such as the existence and location of mobile nodes, the topology of the Mobile Ad-hoc network, functionalities or roles played by the nodes, sources, and destinations of ongoing communications in the network, etc. In addition, the attacker intends to find out what type of communication is going on in the network. This critical information can later be used to perform harmful attacks on the network. By using methods like RF direction finding, traffic rate analysis and time-correlation monitoring, the attacker can find out even more details about the traffic propagating within the network. This attack is similar to an eavesdropping attack but much advanced because the attacker can gain more critical and detailed information by analyzing and monitoring the traffic, instead of just listening to ongoing communications in the network. [22]

- Disruption on MAC Protocol:

In wireless communications, the Medium Access Control (MAC) protocols play a vital role as they coordinate the transmission of nodes on the common transmission medium. IEEE 802.11 is the MAC protocol specifically dedicated to the wireless LANs, which uses distributed contention resolution mechanisms for sharing the wireless channel. The two algorithms used for this purpose are Distributed Coordination Function (DCF) and Point Coordination Function (PCF). PCF relies on a centralized base station, whereas DCF uses the CSMA/CD protocol for resolving channel contention among multiple wireless hosts. In Mobile Ad-hoc Networks, the IEEE 802.11 MAC protocol uses the DCF algorithm, which assumes the cooperative behavior among all nodes in the network. A malicious node can simply not follow the MAC protocol specifications which cause issues with the sharing of the wireless channel among mobile nodes. The malicious node can easily corrupt the ongoing transmission of a genuine neighboring node or prevent other nodes from channel access. [23]

7.3.3. Network Layer Attacks

Most of the attacks on the network layer are targeted directly on the routing protocols. In these attacks, the aim of the adversary is to block the network traffic or control the flow of traffic in some way. The attacker usually forwards the packets to a wrong path to cause a delay in communication, or even worse to a non-existing path causing the packet to be dropped. Other common methods of attack on the network layer are to create routing loops or cause network congestion. It is dangerous when the attacker tries to prevent the source node from finding any route to the desired destination node as it leads to network partition. This also results in unnecessary network control traffic, thus amplifying congestion in the network. [23]

7.3.3.1. Attacks on the Routing Process

Attacks on the routing protocols can be divided with respect to the phases of the routing process: route discovery, route maintenance, and data forwarding.

➢ *Attacks on Route Discovery Phase*:

There are many malicious attacks known that target the route discovery phase in the protocols. Some simply do not follow the routing protocol specification or refuse to participate in the route discovery process, while some do more harm than that. Some attacks aim to change the contents of a route or modify a route reply message. An attacker can also advertise faulty routes, thus invalidating the route cache in other mobile nodes in the network. Examples of attacks on the route discovery phase are as follows:-

- <u>Routing Message Flooding Attacks</u>:

These are attacks that result in a Denial of Service. They are also called as resource consumption attacks, where the hacker's main goal is to disrupt the routing operations by unnecessarily consuming the bandwidth and resources of other nodes in the network. This is done by unregulated forwarding of packets in the entire network. The attacker uses a malicious node to flood the network with a large number of route request packets for a non-existing destination node or simply with a bunch of useless data packets. This consumes a lot of bandwidths and causes network congestion. Also, the genuine nodes tend to waste their resources by receiving and processing the useless data packets forwarded to them by the malicious node. A common example of flooding attack is the "hello flooding". In some routing protocols, the mobile nodes broadcast hello packets to detect the neighboring nodes. These messages are received by all one-hop neighbor nodes but are not forwarded to further nodes in the MANET. The attacker broadcasts many hello packets throughout the network with a large enough transmission power. Thus, each mobile node receiving hello packets assumes the adversary node to be its neighbor and forwards most of the routes to it. Similarly, "RREQ flooding" and "ACK flooding" are also popular flooding attacks. Route Request (RREQ) flooding is nothing but broadcasting a lot of route request messages to a node that is not in the network, whereas Acknowledgement (ACK) flooding is where the malicious node sends out an acknowledgment message again and again. [2]

- Routing Table Overflow:

In this attack, the attacker uses a malicious node to advertise routes for nodes that do not exist in the network. Routing table overflow attack is mostly performed on proactive routing protocols. In proactive routing protocols, the routing information in mobile nodes is updated periodically, which makes it easier for the attacker to cause the routing table to overflow. The goal of the attacker is to flood the routing tables of target nodes and prevent new routes from being created by simply advertising useless routing information throughout the Mobile Ad-hoc Network. The routing table overflow attack often results into a Denial of Service since communications are hindered. [22]

- Routing Table/Cache Poisoning:

Routing table poisoning is another harmful fabrication attack where the attacker targets the functionality of routing table updating. In this attack, the malicious node in MANET either generates and propagates faulty routing information in the network or modifies the genuine routes received from mobile nodes before forwarding them ahead. This results in false routes to be created in the routing tables of the communicating nodes. The malicious node can modify and broadcast routes to a certain destination via itself so that the neighboring nodes will update their routing cache with the same and forward any packets to that destination to be sent via the malicious node. Moreover, a mobile node overhearing a data packet being propagated tends to add the routing information contained in that packet header to its routing cache, which makes this attack easier to perform. Routing table poisoning attack results in many issues like routing loops, bottlenecks, and network partitions being created or resources being wasted because of the packets following non-optimal routes. [6]

- Rushing Attacks:

These attacks are usually performed on the route discovery phase of routing process in MANETs and lead to a Denial of Service attack against the routing protocols. Rushing attacks are known to penetrate even the most secure routing protocols like ARAN and Ariadne. In these attacks as seen in the figure below, when am attacker receives a route request message from a genuine source node S, it immediately broadcasts the same route request message throughout the network before the other mobile nodes receive the route request message from the original source node. The compromised node makes sure that the route request packets forwarded by it are received by other nodes in the network before the actual route request packet sent by the source. Thus, the nodes tend to discard the original route request message from the source node as it is received too late and consider the route request message from the malicious node as the legitimate one as it was received first. Because of this, any routes discovered to the destination D will always involve the compromised node. In general, a rushing attack can be performed by an attacker if he can forward the RREQ packets faster than the genuine source node. The attacker can rush the route request packets in many ways such as removing MAC and network delays in packet transmission, broadcasting the packets at a higher power, using the wormhole attack as a basis and tunneling the RREQ packets instead of the usual routing process, etc. [25]

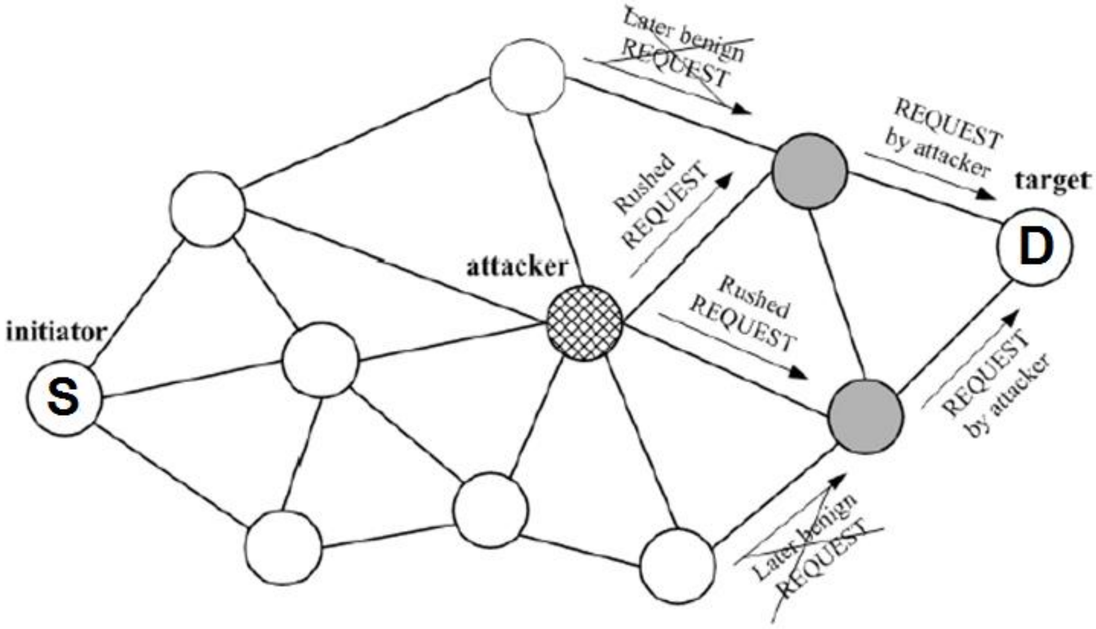


Fig. 1. Rushing Attacks

- *Attacks on route maintenance phase*:

These attacks target the route maintenance phase in the routing process usually by broadcasting false control messages through the network. In routing protocols like AODV and DSR, path maintenance procedures are followed to recover broken paths when the nodes move within the network. The broken links caused by node movements are detected by the neighboring nodes, which broadcast genuine route error messages. These neighboring nodes also invalidate the broken route in their routing table. An attacker can easily take advantage of this mechanism at the route maintenance phase of protocols by propagating false route error messages. A common scenario is where a malicious node broadcasts false link failure messages, resulting in the discovery of alternate non-optimal routes and unnecessary processing for the repairing operations. Attacks on route maintenance phase are typically fabrication attacks. [3]

- *Attacks on data forwarding phase*:

In these attacks, the malicious node refrains from forwarding data packets consistently and drops them. In addition to dropping, attacks on this phase of routing process can also modify the routes or contents of legitimate data packets being propagated in the Mobile Ad-hoc Network. Modification of source route can lead to a Denial-of-Service attack. They can also introduce junk packets in the network. An attacker can perform a replay attack or flooding attacks on this phase. The malicious node can pretend to be a genuine node by behaving normally during the route discovery and route maintenance phases. Once it gains the trust, it can then perform an active attack on the data forwarding phase. Furthermore, the attacker can redirect network traffic by modifying the route sequence numbers. The malicious node can divert traffic through itself by claiming a route with a sequence number higher than the original sequence number. The traffic can also be redirected by modifying the hop-count in routing protocols like AODV that use hop-count for determining the best path. Thus, attacks on this phase of routing protocols can be very critical [4].

- Replay:

In a replay attack, the attacker retransmits the genuine routing information or network data repeatedly. This can easily lead to network congestion and often a Denial of Service attack. [6]

7.3.3.2. Advanced Network Layer Attacks

There are more advanced and sophisticated attacks known to be performed on the network layer that does not target any specific phase of the routing process in Mobile Ad-hoc Networks and are usually routing protocol-independent. Some of them are as follows:

- Wormhole Attack:

Wormhole attack is a very hazardous attack that is performed on the network layer of the protocol stack and involves cooperation between two malicious nodes in the MANET. It can be either one attacker simply operating two malicious nodes or two different attackers working together towards disrupting the network. In this attack as seen in the diagram below, one malicious node (node M1) captures the data packets or routing information at one point in the network and tunnels them to another location in the network, which is received by the other malicious node (node M2). Then node M2 replays that tunneled traffic back into the Mobile Ad-hoc Network. The tunnel between the two malicious nodes, which is nothing but a private communication link invisible to other nodes is called as a "wormhole." This attack is sometimes also referred to as a tunneling attack. Routing process in the network is interrupted when the routing control messages are tunneled in a network [23]. Wormhole attack affects the authenticity and confidentiality of communications. For example, genuine nodes in the network that are connected via routes through the wormhole are completely dependent on the two malicious nodes. Also, in routing protocols like DSR and AODV, a wormhole attack can easily prevent the discovery of any routes other than routes through the wormhole. The data packets tunneled from one point of a network to another arrive at the destination much quicker than normal routing and data forwarding, causing the two malicious nodes to be included in almost all the routes. Thus, they can intercept all the data traffic and drop any packets whenever they want. It is difficult to detect a wormhole attack because the data packets transmitted through the wormhole appear to be the same as those forwarded by the genuine nodes. [3]

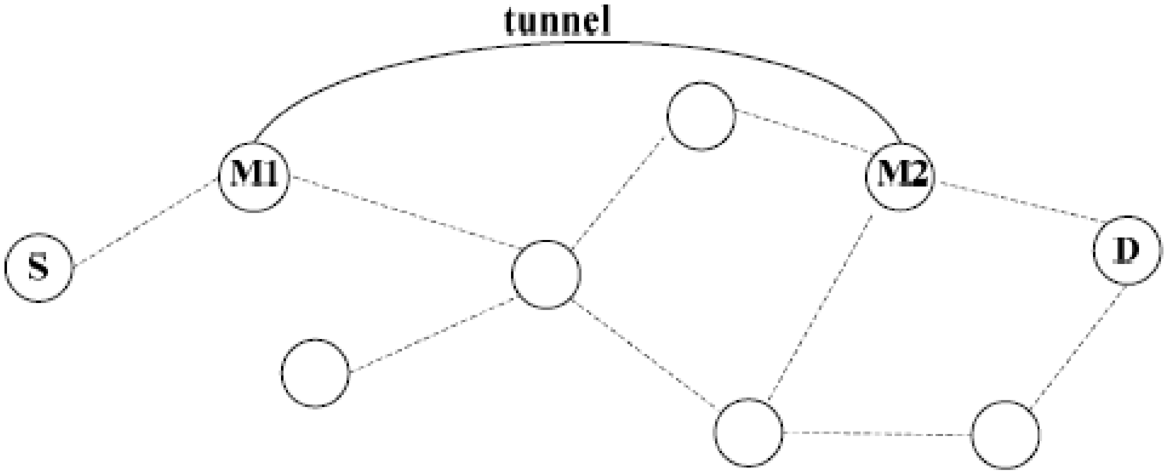


Fig. 2. Wormhole Attack

- Blackhole Attack:

In a blackhole attack, the attacker uses a malicious node to send fake routing information and attract all the network traffic towards itself. In this attack, the malicious node advertises a zero metric for all the destinations so that all the genuine nodes in the MANET forward data packets towards it thinking that it has the shortest path to the destination node. Every time a legitimate source node initiates the route discovery process to send data to a certain destination node, as soon as the malicious node receives the route request, it immediately replies back with false routing information claiming that it has the highest destination sequence number and minimum hop count value to the source node. Thus, the source node has an impression that the malicious node has the most optimum route to the destination. It routes the data packets through the malicious node and ignores all other reply messages from the genuine nodes. This leads to all the data packets in the network to be dropped at the malicious node and never being forwarded to their destinations. The attacker's aim is to perform a Denial of Service attack by consuming the network traffic, by dropping all of it and not forwarding any of it ahead. [27]

- Sinkhole Attack:

Sinkhole attack is a classic example of modification attack and is very similar to a blackhole attack. The difference is that in this case, the malicious node drops the data packets selectively or modifies and forwards them selectively, instead of dropping them all. The hacker’s primary goal is to attract all the network traffic towards a compromised node in the network. Once all the network traffic is received after sending false routing information in the network, the malicious node then modifies and forwards the data packets or simply drops them selectively. He can modify the packets by maximizing the route sequence numbers or minimizing the hop counts. It can be very difficult to detect this attack. [27]

- Greyhole Attack:

This attack is similar to a blackhole attack, but in this case, the attacker targets a particular node in the Mobile Ad-hoc Network. When the malicious node M receives route request message from the target node S, it immediately claims to have an optimum route. Thus, the target node S forwards the traffic to the malicious node M, which is then dropped and never forwarded to the actual destination. In this attack, the adversary doesn't usually care to attract all the network traffic towards itself, but only wants to intercept one particular node's traffic, making it unable to communicate with other mobile nodes, in this case the node D. [23]

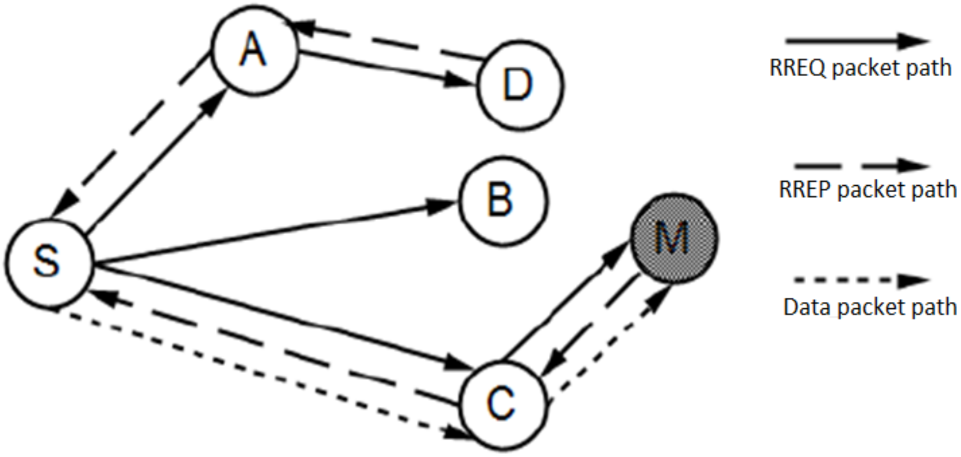


Fig. 3. Greyhole Attack

- Blackmail Attack:

A blackmail attack takes advantage of the mechanism of some distributed routing protocols that once a malicious node is identified; it is blacklisted and isolated from further communications in the MANET. An attacker fabricates a message that a particular legitimate node is harmful and propagates that message throughout the network. Hence, the genuine victim node is cut out of all the communications in the network. [6]

- Byzantine Attacks:

Byzantine attacks are a generalized type of attacks that are usually performed by a group of compromised nodes in the network. The malicious behavior is difficult to detect because of the cooperation among them. In this attack, the main goal of the attacker is to disrupt the communications in MANET by degrading the routing services. There are many ways this is done, for example, creating routing loops, forwarding the data packets via non-optimal paths in the network, advertising fake routing information or dropping packets. The compromised nodes can also pretend to be genuine nodes and simply gain information about the network. Such attacks are common today and can prove to be severe on the network. [6] A common example is a Colluding Misrelay Attack.

- *Colluding Misrelay Attack*: In a colluding misrelay attack, multiple attackers perform an attack together to interrupt the routing process in Mobile Ad-hoc Networks by modifying or dropping the routing packets. A typical scenario is where one malicious node sends false hello messages to the target node such that all the messages generated by the target node are forwarded to it. The first malicious node then transmits the packets, as usual, to avoid being noticed of any malicious activity. However, it forwards the packets to the second malicious node, which then drops or modifies the data packets. Thus, a combination of two attackers performing an attack can be very dangerous. [28]

- Sleep Deprivation Torture Attack:

This is a well-known attack in Mobile Ad-hoc Networks, which results in a Denial of Service attack. In sleep deprivation torture attack, the attacker typically targets specific nodes in the network and causes them to exhaust their resources. The malicious node causes other mobile nodes in the network to do unnecessary processing by continuously making excessive service requests and route discoveries or by forwarding useless data packets, which usually leads to them running out of batteries and become unavailable to operate. This attack is a huge issue in MANETs because the mobile nodes already have power constraints, and targeting this vulnerability makes it even worse. Unavailability of nodes and the services provided by them also causes network partition. This attack is sometimes also referred as energy starvation attack or resource/energy consumption attack. A common example of sleep deprivation torture attack is where a malicious node continuously advertises topology updates with false routes and wrong IP addresses of source and destination. Because of this, the genuine nodes take longer time and more processing power for calculating the routing tables, thus eventually running out of batteries. [22]

- Location Disclosure Attack:

The main aim of the hacker to perform a location disclosure attack is to capture and reveal information about the nodes in Mobile Ad-hoc network, specifically their location or structure of the network. The attacker does this by using various probing, traffic analysis, and monitoring techniques. Revealing the confidential information about the mobile nodes like their location in the network can be very critical because the attacker can then target that particular node for further attacks. [6]

- Sybil Attack:

Sybil attack is an advanced attack where the malicious node impersonates not only one but multiple nodes in the network. It shows multiple IP addresses, making the genuine nodes think that it is a group of nodes, thus undermining the redundancy of routing protocols. This attack usually tends to demean the integrity of data, network security, and resource utilization. The malicious node performing this attack is called as a Sybil node. The malicious node usually pretends to be a group of nodes large enough to outnumber the genuine nodes in MANET, which also protects it from being detected. As seen in the diagram below, the Sybil node can impersonate other nodes (B and C) by taking over their original identities or simply by creating new false identities, in an attempt to acquire the network traffic destined for them. This type of attack can be destructive towards not only the routing mechanisms and node localization but also the storage, resource allocation, and misbehavior detection schemes. [23]

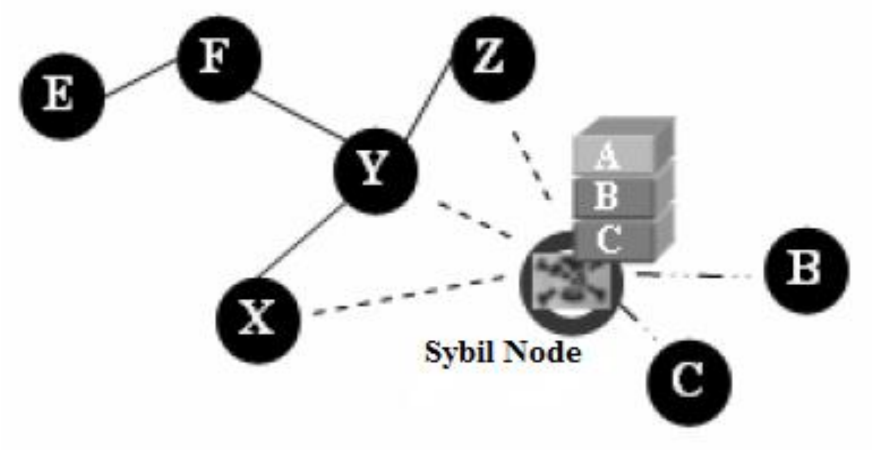
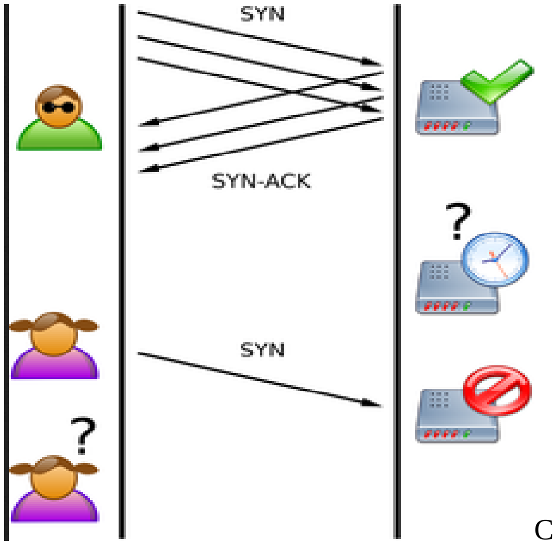


Fig. 4. Sybil Attack

7.3.4. Transport Layer Attacks

- SYN Flooding Attack:

This is another attack that can be generalized as a Denial of Service attack. In a SYN flooding attack, the adversary uses a malicious node to create many half-opened TCP connections with the target node but never completes the three-way handshake needed to establish the connection. A three-way handshake is nothing but a standard for using the Transmission Control Protocol (TCP) in which two mobile nodes in the network must first exchange three messages for setting up a TCP connection for further communications. This handshake is important as it allows a node to ensure that the other node it is willing to communicate with, is ready for the conversation. The three messages in the handshake are: a SYN packet sent by the source node to the destination node which is a request for establishing a TCP connection, a SYN/ACK packet which is a reply from the destination node to the source node that it received the SYN packet, and an ACK packet back from the source node to the destination which means that it received the reply, and a TCP connection is confirmed for further communications. In a SYN flooding attack, the attacker takes advantage of this initial process of setting up the TCP connection. The malicious node sends a large number of SYN packets to the target node and spoofs the return addresses of the SYN packets. Once the target node receives a SYN packet, it replies back with a SYN/ACK packet and waits for an ACK packet, i.e. confirmation of the TCP connection, back from the source node. However, the malicious source node never sends an ACK packet, and the TCP connection is never fully established between the two nodes. Thus, the victim node tends to store the half-opened connections in its buffer, waiting for an ACK packet for all of those initiated connections. This quickly leads to the buffer of the target node to overflow, and it is not able to accept any more requests for establishing the TCP connection, not even the legitimate requests from other genuine nodes in MANET. SYN flooding attack is very dangerous since it can completely make a node unavailable for communications, causing a Denial of Service. [23]



Credit: Wikipedia

Fig. 5. SYN Flooding Attack

- Session Hijacking:

Session Hijacking is an attack where the attacker takes control of an ongoing communication between two legitimate nodes and disguises as one of them to continue that communication. Most of the authentication processes for communication are performed in the beginning when a session starts. However, after the initial setup, the session or the communication is unprotected. A session hijacking attack takes advantage of this adversely. In this attack, the hacker spoofs the victim node's IP address, determines the correct sequence number that is expected by the target node and then performs the attack on the victim node [23]. This attack is often generalized as a Denial of Service attack since it hinders communication between the victim node and the target node. The attacker impersonates the victim node and continues the session initiated by it to communicate with the target node. A TCP session hijacking attack usually leads to the TCP ACK storm in Mobile Ad hoc Networks, where ACK packets are transmitted back and forth between the victim node and the target node, creating the TCP ACK storm in the network. In the case of a UDP session hijacking attack, it is easier for the attacker to perform the attack without being detected because UDP is a connectionless protocol. [23]

7.3.5. Application Layer Attacks

- Malicious Code Attacks:

These attacks include the attacks performed by a virus, worm, spyware, Trojan horse, etc. They can attack both, the operating systems as well as the user applications. An attacker can perform a malicious code attack on Mobile Ad-hoc Networks specifically to cause a node to slow down, make it unavailable for communication or gain critical information about the network or nodes in it. A virus attaches itself to a program or file, with an intention of propagating itself from one node to another infecting each one, throughout the MANET. It requires human action to spread, for example, genuine users sharing infected files not knowing that it is infected. A worm is similar to a virus, the only difference being that it does not require human action for spreading from one node to another. A worm is more dangerous than a virus because it can also replicate itself. Instead of sending one infected file to a node, it can send multiple copies of it, which usually results in the receiving node to become unavailable for communication. An attacker uses spyware which is installed on a target node without the knowledge of the user, for gathering private information about the user. A Trojan horse is used by an attacker to damage the target node. The target node's user is tricked into installing it as it appears to be useful and legitimate software or file. [26]

- Repudiation Attacks:

These attacks directly violate the security goal of non-repudiation. In these attacks, the attacker or the malicious node denies having sent a message or having participated in communications. The attacking node can inject false routing information into the network and simply deny sending it. Thus, it is important that the routing protocols have a mechanism to detect a malicious node and prove that it did perform a malicious activity which cannot be denied. [23]

7.3.6. Multi-layer Attacks

- Denial of Service (DoS) Attack:

Denial of Service is a type of attack in which the goal of the attacker is to block the wireless communication channel and cause some interruption or complete halt in communications between the mobile nodes. In other words, this attack leads to prevention of authorized access to services or delaying critical operations in the network. A DoS attack can be performed on various layers of the protocol stack. For example, jamming takes place on the physical layer, disruption on MAC protocol takes place on the data link layer, routing process can be disrupted through various methods on the network layer, SYN flooding and session hijacking is performed on the transport layer and the malicious code attacks are performed on the application layer. The attacker usually prevents genuine users in the MANET from using the desired resources by flooding the network with route requests or irrelevant information via a malicious node, thus consuming bandwidth and blocking the legitimate traffic. He can also target a specific node with an intention to consume its resources so that it will not be able to participate in the network communications anymore, making the services provided by it unavailable to other genuine nodes in the network. Usually, battery exhaustion or radio jamming is performed by the attacker to conduct this attack. The attacker can also spoof its IP address and send a large number of route requests with fake IDs to a target destination node. [2] The most common examples of Denial of Service attacks are sleep deprivation torture attack, routing table overflow attack, flooding attacks, rushing attack, spoofing, session hijacking, etc.

- Impersonation Attacks:

Impersonation attacks are multi-layer attacks where the attacker introduces a malicious node in the MANET, which pretends to be a legitimate node and then conducts malicious behaviors. The malicious node can propagate false routing information in the network or gain critical information about the network. Impersonation attacks are often a first step for launching further destructive attacks on the network. Thus, to avoid such attacks, it is necessary to have a proper authentication mechanism among the mobile nodes every time a node is introduced in the network. A typical example of an impersonation is Spoofing. [2]

- Spoofing Attack: In a spoofing attack, the malicious node misrepresents its identity by altering its MAC address or IP address in the outgoing packets. A spoofing attack is often performed in combination with modification attacks, which results in network issues like routing loops. It can also allow routing loops to be formed which results in network partitioning. [4]

- Man-in-the-middle Attack:

A man-in-the-middle attack is one of the most frequent attacks on MANETs. In this attack, the adversary node places itself between the source node and the destination node, with an intention to sniff the messages exchanged between them. Typically, the attacker does not harm the network directly, but only tries to gain information through the ongoing communication between two nodes in the network. [23]

8. ROUTING PROTOCOLS

Routing in Mobile Ad-hoc Networks is more complicated and as compared to wired networks because of the inherent characteristics of such networks, such as lack of fixed infrastructure, rapidly changing topologies, high power consumption and high error rates, low bandwidth, etc. In a wired network, additional layers of security are available such as access control lists in routers and firewalls. This is not possible in MANETs because of its architecture. Moreover, the co-operative nature of Mobile Ad Hoc Routing Protocols makes it easier for an attacker to tamper data, impersonate data or perform a Denial of Service attack.

This paper presents a list of popular routing protocols currently used in Mobile Ad-hoc Networks. Because so many routing protocols have been proposed for mobile ad hoc networks, it is impossible to cover all of them [30]. Most of the advanced routing protocols covered in this paper are typically based on the traditional ones and try to have some modifications or add-ons for securing the network. They intend to overcome the drawbacks faced by traditional routing protocols because of the inherent characteristics of MANETs, which made them susceptible to attacks. The newer protocols are more robust and operate on different types of approaches like using location services, clustering of mobile nodes, etc. The hybrid routing protocols have proven to be more effective than the proactive or reactive ones. Furthermore, the paper will discuss some protocols that use cryptographic solutions to the existing routing protocols, thus making them secure. It should be noted that this paper focuses only on the unicast routing protocols, and not the multicast routing protocols.

The existing unicast routing protocols for MANETs can be classified based on how the routing information is acquired and maintained by the mobile nodes in network. They can be distinguished into three main types:

i) Proactive (table-driven) routing protocols
ii) Reactive (source-initiated on-demand) routing protocols
iii) Hybrid routing protocols

8.1. Proactive Routing Protocols

Proactive routing protocols are also called as table-driven Ad-hoc routing protocols. These protocols maintain the routing information at all times, by periodically updating it, thus ensuring that every node in the network has up-to-date routing tables. The routing information is usually stored in a number of different tables, for example, routing table, distance table, link-cost table, Message Retransmission List table, cluster member table, etc. The tables are periodically updated or on each instance the network topology changes, or both. Each node has a clear and consistent view of the network topology since it maintains the routing information to every other node in the MANET. Hence, all the mobile nodes in network are able to make the routing decisions for forwarding a data packet instantly. The nodes continuously evaluate and maintain routes to other nodes and proactively update the network state, regardless of whether the data traffic exists or not. This results in a constant high amount of signaling traffic in the network, even if there is no ongoing data traffic or topology change. The proactive routing protocols vary in the way how the routing information is updated in the network, the different tables maintained and the type of information stored in the routing table.

8.1.1. Destination Sequenced Distance Vector (DSDV)

The Destination Sequenced Distance Vector (DSDV) is a table-driven Ad-hoc routing protocol that is based on the Bellman-Ford algorithm. In this protocol, each node in the MANET maintains a routing table containing all of the possible destinations in the network and the number of hops to reach them. Every entry in the routing table is marked with a sequence number assigned to the destination node, which enables the nodes to differentiate new routes from the old ones, thus avoiding routing loops to be formed. A route having the most recent sequence number is always preferred. In case of two routes having the same sequence number, the route with smaller metric is used. Each node maintains its routing tables by periodically transmitting updates to all the neighboring mobile nodes. To reduce the constant high amount of signaling traffic, two types of packets are used to update the routes: ‘full dump’ packets and ‘incremental’ packets. A full dump packet contains the entire routing table in the update, whereas an incremental packet contains only the routing information that changed since the last full dump. The incremental packets are transmitted more often than the full dump packets. However, even with the use of these two types of routing update packets for reducing the amount of overhead, DSDV protocol still utilizes a significant amount of network bandwidth for route updating procedures especially in large Mobile Ad-hoc Networks, making the protocol effective only in small networks. [6]

8.1.2. Optimized Link State Routing (OLSR)

The Optimized Link State Routing (OLSR) is a proactive routing protocol based on the traditional link-state algorithm in which each node propagates its link-state information throughout the network for maintaining the network topology. This routing protocol uses multipoint relay (MPR) selection strategy where the overhead is reduced and the number of re-broadcasting nodes is minimized. In this strategy, each mobile node in the network selects a set of neighboring nodes to re-transmit its packets, called the MPRs. Each of these MPRs maintains the list of nodes selected as a multipoint relay. To select the MPRs, each node periodically broadcasts ‘hello’ messages which contain a list of its one-hop neighbors, its address identifier and the type of link it has with each node. When a node broadcasts a message, all of its neighbors receive it, but only the MPR nodes can re-transmit it forward. Hence, the overhead for message flooding is significantly reduced. Also, only the MPRs advertise ‘topology change’ messages periodically. After receiving the topology change messages from all the MPRs, a particular node can learn the partial network topology and thus, has a route to every mobile node in the network. In this way, each node obtains the network topology information and builds its routing table through link-state messages. [6]

8.1.3. Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) uses an improvised Bellman-Ford Distance Vector routing algorithm to ensure the reliable exchange of update messages between the mobiles nodes. This protocol reduces routing loops in the network significantly by using predecessor information. As per the protocol, each mobile node in the Mobile Ad-hoc Network has to maintain four types of tables: distance table, routing table, link-cost table and Message Retransmission List (MRL) table. The link changes are propagated in the network using update messages that are exchanged between the neighboring nodes. MRL table contains information about which neighboring node has not acknowledged an update message. If needed, the update message is re-transmitted to that neighboring node. WRP avoids the count-to-infinity problem by enforcing each mobile node to perform consistency checks of predecessor information reported by all its neighboring nodes. This is done by storing the predecessor and successor information in the routing table. The routing tables are exchanged between the neighboring nodes using update messages. Also, if there is no change in the routing table since last update, the mobile nodes need to send a ‘hello’ message to maintain the connectivity. After receiving an update message, the nodes modify their distance tables and look for better routes. The link-cost table contains entry for each neighboring node, which includes the cost of the connecting link and the number of timeouts since an error-free message was received by a particular neighboring node. A major disadvantage of this protocol is that each node needs a large amount of memory for maintaining four tables and high processing power since each node has to stay active at all times and maintain connectivity through ‘hello’ messages. Hence, it has a limited scale and is not suitable for large MANETs. [30]

8.1.4. Fisheye State Routing (FSR)

The Fisheye State Routing (FSR) is another proactive routing protocol used in Mobile Ad-hoc Networks that is based on the link-state routing algorithm. This algorithm is helpful in reducing the overhead to maintain the network topology information. In this protocol, each node maintains an accurate distance and path quality information about its immediate neighbors, and gradually reduces the details of such information about the mobile nodes that are far away. In other words, the link-state information for nearest nodes is updated at a higher frequency compared to that for nodes located farther. FSR protocol does not require each node in the network to have the same level of accuracy about link-states. The accuracy of the topology information is reverse proportional to the distance. Thus, an advantage of this protocol is its larger scalability, but a disadvantage is that the accuracy of routes to remote destination is reduced. [29]

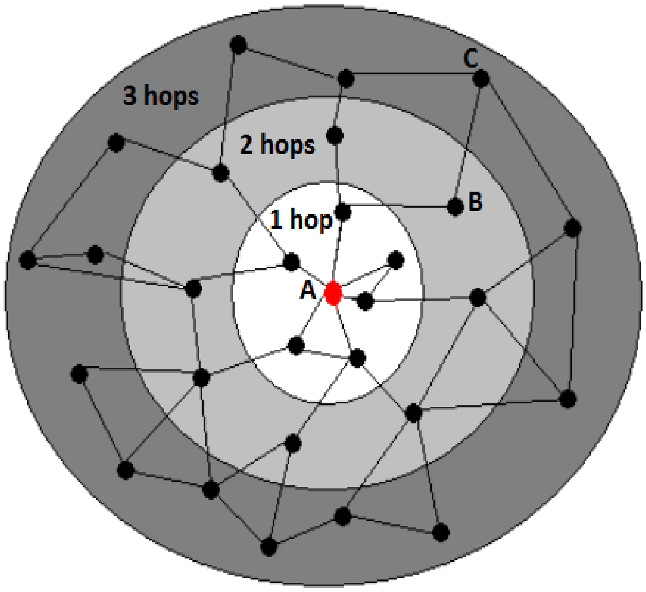


Fig. 6. Fisheye State Routing

8.1.5. Distance Routing Effect Algorithm for Mobility (DREAM)

This proactive routing protocol routes data packets based on the location and mobility of nodes in MANET. Each node in the network knows its geographical location coordinates via a GPS, which are periodically exchanged with other mobiles nodes and stored in the routing table. In DREAM, the nodes in network do not need to exchange the link-state or distance vector information, which conserves the bandwidth considerably. Thus, this protocol is more scalable than most other proactive routing protocols. Before sending a data packet, the source node first determines the location of the destination node through its routing table and then forwards the data packet to a neighboring node that is in the direction of the destination. Furthermore, the frequency of the location update messages is also determined by the distance and mobility of a node, which reduces the routing overhead even more. The stable nodes, especially the ones far away from a particular node that will relatively seem more stable than the nearby nodes, update their location information less frequently. DREAM is an effective routing protocol in larger networks. [29]

8.1.6. Clustered Gateway Switch Routing (CGSR)

The Clustered Gateway Switch Routing (CGSR) protocol uses the DSDV routing protocol as its underlying routing scheme. The difference and modification to DSDV is that it uses a hierarchical cluster multi-hop approach for routing traffic, channel access and bandwidth allocation. In this protocol, the mobile nodes are grouped into a cluster which is maintained by an elected cluster-head node. This cluster-head node manages all other nodes within the cluster and also controls the transmission medium. All inter-cluster communications must include this node. Each node maintains a cluster member table which includes mapping of each node in the network to its cluster-head. This table is broadcasted periodically. An important advantage of this protocol is that each node only maintains routes to its cluster-head and does not need to flood the routing information throughout the network, thus reducing the routing overhead. Also, the cluster structure provides effective membership and traffic management. However, if a cluster-head is changed frequently, it can adversely affect the routing process since the cluster-head election process would take a lot of bandwidth. To avoid frequent cluster-head changes, a Least Cluster Change (LCC) clustering algorithm is used, according to which a cluster-head will change only when two cluster-heads in the network come in contact with each other or when a mobile node moves out of coverage of all current cluster-heads in the network. A data packet sent by a source node is first forwarded to its own cluster-head, which is then routed to a gateway node and then to another cluster-head. A gateway node is nothing but a node that lies within the communication range of two or more cluster-heads in the MANET. The data packet is routed between gateway nodes and cluster-heads until it reaches the cluster-head of destination node, which is then forwarded to the destination node. [30]

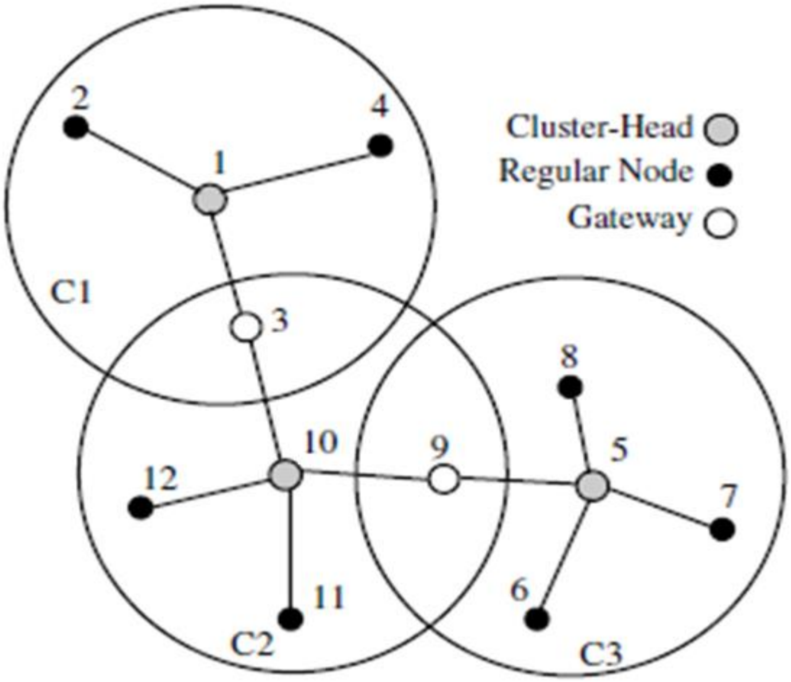


Fig. 7. Clustered Gateway Switch Routing

8.1.7. Hierarchical State Routing (HSR)

The Hierarchical State Routing (HSR) is a multi-level cluster-based routing protocol. It is similar to the CGSR protocol in terms of organizing the mobile nodes with close proximity into clusters and the routing mechanism. Additionally, the cluster-heads of low level clusters further organize themselves into upper level clusters. Nodes in the upper level hierarchical clusters flood the network topology information to the nodes the lower level clusters. The HSR protocol also uses hierarchical addressing for each node and a topology map. The hierarchical address reflects the physical locations of mobile nodes and provides enough information for routing the data packets. Each node also has a logical address that reflects the cluster property of nodes. Combination of these two addressing improves the adaptability of routing algorithm. A location management mechanism is used in this protocol for mapping the logical address to physical address. An advantage of HSR protocol is that it separates the mobility management from the physical hierarchy. However, this protocol causes additional overheads in the MANET from multi-level cluster formations and their maintenance. [30]

The table below compares the 6 proactive routing protocols discussed according to the tables used for routing, frequency of the update messages, ‘Hello’ message for maintaining the neighbor relationships, features and advantages/disadvantages.

Protocol	Tables	Frequency of Updates	‘Hello’	Features and Advantages / Disadvantages
DSDV	- routing	periodic and on topology change	yes	- distance-vector routing - loop free - high overhead
OLSR	- routing - neighbor - topology	periodic	yes	- link-state routing - low overhead - 2-hop neighbor knowledge required
WRP	- distance - routing - link-cost - MRL	periodic	yes	- distance-vector routing - uses predecessor info - loop free - large memory required
FSR	- link-state - topology - next-hop - distance	periodic and local	no	- link-state routing - low overhead - large memory required - low accuracy
DREAM	- location (routing)	mobility based	no	- location-based routing - low overhead - GPS required
CGSR	- routing - cluster-member	periodic	no	- cluster-based, distance-vector - low overhead - cluster maintenance

Table 1. Comparison between Proactive Routing Protocols

8.2. Reactive Routing Protocols

Reactive routing protocols are also called as source-initiated on-demand routing protocols. These protocols were designed mainly to reduce the overheads by maintaining the routing information in the network only for active routes. To be specific, a routing path is searched, created or maintained only when a source mobile node requires it for communicating with the destination node. The routing information is not updated periodically via tables as seen in proactive routing protocols, thus minimizing the control overhead significantly. This makes the reactive routing protocols more scalable as compared to the proactive routing protocols. The operation of this type of protocol is divided into route discovery and route maintenance. Route discovery takes place when a node has to send some data to a destination whose route information is not known. The source node acquires the required route by the initiating the 'route discovery' mechanism. In this mechanism, route request packets are broadcasted throughout the Mobile Ad-hoc Network. When the destination node or the node having a route to the destination receives this route request packet, it immediately responds back to the source node with a route reply packet. Once the path is established, the source node then transmits the data packets to the destination node. This established route is maintained in the MANET until it is no longer required or the destination becomes inaccessible via every path from the source, which is done through a 'route maintenance' mechanism. Also, when there is a link break between two nodes, one or both of the nodes send error information about it to all the affected nodes. Overall, in a reactive routing protocol, the source node may have to deal with long delays for finding a route to the destination, before it can transmit data packets to it.

The routing process in reactive protocols can be categorized into two types: source routing and hop-by-hop routing. In *source routing*, the data packets contain the entire path i.e. every hop in the route, for forwarding the packet from source to destination. Hence, other mobile nodes neither need to maintain up-to-date routing information for each active route for forwarding the data packets, nor do they need to maintain the neighbor connectivity through periodic exchange of 'hello' messages. However, a drawback of this routing approach is that it does not perform well in large networks because larger the network, higher is the probability of a link failure while the data packet is being forwarded. Route recalculations are needed every time a route fails during data transmission. Also, larger the network, the overhead carried in the data packet header with information about the entire path from source to destination will be higher. On the other hand, in *hop-by-hop routing*, the data packet only contains the destination address and the next hop address. Each intermediate mobile node in the path to destination node has to use its routing table to forward the data packets towards destination. This approach is very effective in adapting to the dynamically changing network topology as each node can update its routing table when they receive fresh routes and forward the data packets accordingly. However, a disadvantage of hop-by hop routing is that each node in the network has to maintain up-to-date routing information for each active route and also need to maintain the neighbor connectivity. [30]

8.2.1. Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) is a source-initiated on-demand routing protocol that is based on the concept of source routing process discussed earlier. Each data packet transmitted contains the entire address i.e. the every hop in the path from source node to destination node. Also, each node maintains a route cache that contains routing information. The entries in route caches are frequently updated as new route is learnt by a mobile node. When a source node has to send a data packet to a destination node, it first checks its route cache to find whether it already has a route to it. If it does, then it uses that route to forward the packet, and if it doesn’t, then it initiates the route discovery process. The broadcasted route request packet contains addresses of source and destination, as well as a unique identification number. Each node receiving it checks its own route cache to find whether it knows a route to the destination. If it doesn’t know it, then it appends its own address to the route request record field of the route request packet and forwards it to its neighbors. A route reply message is sent by the destination itself or an intermediate node having a route to the destination in its route cache. In the route maintenance process, each node generates a confirmation through acknowledgements when it can verify that the next hop node has successfully received the packet. When a mobile node is not able to verify, it re-transmits the packet. After a certain number of failed re-transmissions or when a link disconnection is detected, the node generates a ‘route-error’ packet specifying the failed link and sends it to the source node. Additionally, route containing the failed link is removed from the route caches of each node in the path. On receiving the route error message, the source node initiates the route discovery process again.

The DSR protocol is not very effective in large MANETs since the overhead carried in the data packet header keeps on increasing as the network increases. In small networks, DSR proves to be advantageous as the nodes can store multiple routes in their route caches, minimizing the need for route discoveries especially in MANETs with low mobility of nodes. Also, since the dynamic source routing protocol does not require periodic ‘hello’ messages to be exchanged between neighbors, the nodes can conserve their power by going into a sleep node if needed. [6]

8.2.2. Ad-hoc On-demand Distance Vector (AODV)

The Ad-hoc On-demand Distance Vector (AODV) is a hop-by-hop reactive routing protocol for Mobile Ad-hoc Networks, i.e. the source node does not put the entire path address in the data packets being transmitted. Instead, the packets carry only the destination address and the next hop decision is made separately after each hop. Thus, AODV has less routing overhead as compared to the DSR protocol. The source node broadcasts route request (RREQ) messages throughout the network to discover the paths required. When the destination node or an intermediate node having a route to the destination receives this route request packet, it immediately responds back to the source node with a route reply (RREP) message. Also, the intermediate node replies only if it has a fresh route to the destination, which is determined by sequence numbers. If it does not have it, then it broadcasts the RREQ packet further in the network. When the destination node sends the RREP packet to the source, all the intermediate mobile nodes between them set up forward route entries in their routing tables. Once the path is established, the source node then transmits the data packets to the destination node. In the route maintenance process, the neighboring nodes of a failed link transmit link-layer notifications throughout the MANET. These notifications are nothing but route error (RERR) messages. On receiving a RERR packet, each node then initiates a route discovery to replace the broken link path. An advantage of AODV protocol is that it is adaptable to highly dynamic networks. However, the route discovery process may introduce large delays and consume more resources in larger networks. [6]

8.2.3. Temporally Ordered Routing Algorithm (TORA)

The Temporally Ordered Routing Algorithm (TORA) is a reactive routing protocol that is based on link reversal. A Directed Acyclic Graph (DAG) is maintained, which is rooted at the destination. There is no need for the source node to find a path to destination node through route request messages. Instead, a flooding technique is used to determine routes. TORA is very useful in highly dynamic Mobile Ad-hoc Networks and provides loop-free distributed routing. The basic functions of TORA include route creation, route maintenance and route erasure. The main concept of the design of TORA is that it utilizes localization of control messages to a small set of neighboring nodes where a change in topology has occurred. Each node in the network maintains routing information only to its one-hop neighbors, thus reducing overheads. Also, in case of 'route maintenance', when a node loses its last downstream link, it generates a new reference level and broadcasts the reference to its neighbors. Thus, links are reversed to reflect the topology change and adapt to the new reference level. In the 'route erasure' process, Clear (CLR) packets are broadcasted throughout the network to erase invalid routes. Another advantage of this protocol is that it also supports multicasting when used in conjunction with the Lightweight Adaptive Multicast (LAM) algorithm. [30]

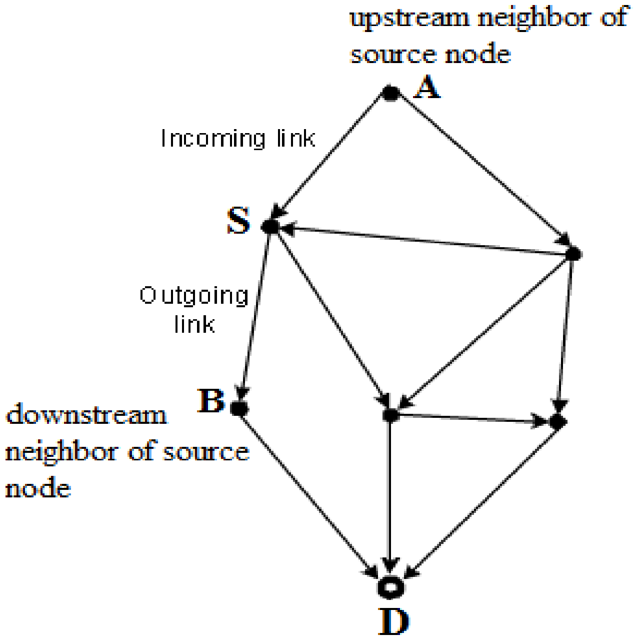

upstream neighbor of source node
A
Incoming link
S
Outgoing link
B
downstream neighbor of source node
D

Fig.8. Temporally Ordered Routing Algorithm

8.2.4. Associativity Based Routing (ABR)

The Associativity Based Routing (ABR) is another source-initiated reactive routing protocol that utilizes the typical route discovery process discussed previously. However, in this protocol, the route selection is mainly based on stability of the mobile nodes as it finds routes that are expected to last longer in the network. Each node maintains an ‘associativity’ table, which contains the connection stability between itself and its neighbors. After receiving a ‘hello’ packet to maintain the neighbor connectivity, each node increases the associativity tick with respect to the neighbor sending the hello packet. When a neighbor is disconnected from the network, the respective associativity tick for it is reset. Thus, the link with higher associativity tick is more stable and always preferred for routing traffic. ABR protocol has three main functions: route discovery, route reconstruction and route erasure. The ‘route reconstruction’ mechanism may consist of partial route discovery, invalid route erasure, valid route update or new route discovery. A major advantage of this protocol is that since the routes last long, fewer route reconstructions are needed and hence, more network bandwidth is available for data transmission. A disadvantage is that each node is required to send the periodic hello packets to maintain neighbor connectivity and the associativity table. Thus, the nodes have to stay active all the times consuming its power continuously. [29]

8.2.5. Location Aided Routing (LAR)

The Location Aided Routing (LAR) protocol improves the efficiency of route discovery process and reduces the routing overheads by using location information through a GPS and limiting the scope of route request flooding. This protocol has two different schemes for operation. In the first scheme, a request zone is calculated and defined in the request packets, which is nothing but an area near the destination node where the route request packets should be transmitted. Any intermediate node outside the request zone will discard the request. The destination node replies back with a route reply message containing its current location, time and average speed. In the second scheme, the coordinates of the destination node are stored in the route request packets. The packets travel only in the direction where the relative distance to destination node becomes smaller with each hop, finally reaching the destination. Both these schemes reduce the control overhead and usually also determine the shortest path to the destination. However, one disadvantage of this protocol is that each mobile node in the network must have a GPS. [30]

8.2.6. Cluster Based Routing protocol (CBRP)

The Cluster Based Routing protocol (CBRP) is reactive routing protocol based on the clustering algorithm where the mobile nodes in network are divided into clusters. Each cluster has a cluster-head node which coordinates communications within the cluster and to other clusters in the MANET. The source node sends the route request packet to its own cluster-head. If the destination node is in the same cluster, then the cluster-head forwards the data packets to the destination node, otherwise it floods the route request packet to neighboring cluster-heads via the gateway nodes, which further check if the destination belongs to their respective clusters. If next hop is not reachable, the nodes also perform a ‘local route repair’, where they check the routing information in packet. If the next-hop or the hop after next-hop is reachable through one of its neighbors, the packet is then forwarded through the new route. An advantage of CBRP is that since only the cluster-heads exchange routing information, the control overheads is lesser. However, cluster formation and maintenance has its own overhead. Furthermore, route discovery process may take long delays. [30]

8.2.7. Signal Stability-based Adaptive (SSA)

The Signal Stability-based Adaptive (SSA) routing protocol is very similar to ABR. The difference is that in case of SSA, the routing mechanism is based on signal strength and location stability, instead of using an associativity tick. Similar to ABR, the routes selected in SSA reactive routing protocol last longer in the network, thus needing fewer route reconstructions. A 'signal stability' table and routing table are maintained by each node in the MANET. The signal stability table contains the signal strength of neighboring nodes that is received through the periodic hello messages. The route request packets transmitted by the source node are forwarded only through the strong channels. Thus, the routing paths in this protocol have the strongest stability as the route request packets going through weak channels are dropped at intermediate nodes. However, a disadvantage of SSA is that the route discovery process may take long delays because sometimes it is impossible to compose a route solely by strong stable links. Also, when an intermediate mobile node detects a link failure, it sends an error message to the source with information about the failed link. The source node then broadcasts an erase message throughout the network to notify all the nodes about the failed link and a new route discovery is initiated if needed. [29]

The table below compares the 7 reactive routing protocols discussed so far according to the route metric used in the routing process, 'Hello' message for maintaining the neighbor relationships, route maintenance, route re-configuration, features and advantages/disadvantages.

Protocol	**Route Metric**	**'Hello'**	**Route Maintenance**	**Route Re-configuration**	**Features and Advantages / Disadvantages**
DSR	shortest path/next available in route cache	no	route cache	erase route, notify source	- source routing - multiple routes - power conservation - long delays - high overhead in large networks
AODV	freshest & shortest path	yes	routing table	erase route, notify source/local route repair	- hop-by-hop routing - low overhead - adaptable to highly dynamic topology - long delays

TORA	shortest path/next available	no	routing table	link reversal and route repair	- link reversal routing - multiple routes - low overhead - temporary routing loops
ABR	strongest associativity & shortest path	yes	associativity (routing) table	localized broadcast query	- stability-based routing - routes last longer
LAR	shortest path	no	route cache	erase route, notify source	- location-based routing - localized route discovery - low overhead - GPS required
CBRP	first available route	no	routing table and cluster-member table	erase route, notify source and local route repair	- cluster-based routing - low overhead - cluster maintenance - temporary routing loops
SSA	strongest signal strength & stability	yes	signal stability (routing) table	erase route, notify source	- signal strength & stability-based routing - routes last longer - long delays

Table 2. Comparison between Reactive Routing Protocols

8.3. Hybrid Routing Protocols

The hybrid routing protocols for Mobile Ad-hoc Networks are advanced protocols that are both proactive and reactive in nature. These routing protocols were initially designed to increase scalability. By partitioning the network into zones or clusters, the control overheads are reduced. Also, the delays caused by the route discovery process are reduced considerably. To be specific, the mobile nodes in hybrid protocols proactively maintain routes to nearby nodes, and reactively determine routes to farther nodes through the route discovery process whenever needed.

8.3.1. Zone Routing Protocol (ZRP)

In Zone Routing Protocol (ZRP), the Mobile Ad-hoc Network is divided into routing zones as per the distance in hops between mobile nodes. The nodes within a zone maintain connectivity proactively by exchanging their link-state information periodically. Thus, if the source and destination belong to the same zone, a route will be available immediately. On the other hand, if the destination node lies outside the routing zone of the source, the source node reactively initiates a route discovery process. The major advantage of ZRP is that control overhead is reduced by limiting it only within a zone. Also, the route discovery delays are reduced because it is needed only for destinations outside the routing zone of source node. Furthermore, the route requests are propagated via peripheral nodes, i.e. the boundary nodes of a zone where the destination belongs are able to reply back to the source node that they have a route to the destination proactively maintained within the zone. There is no need for the route request packet to reach to the actual destination node for getting a route reply. [30]

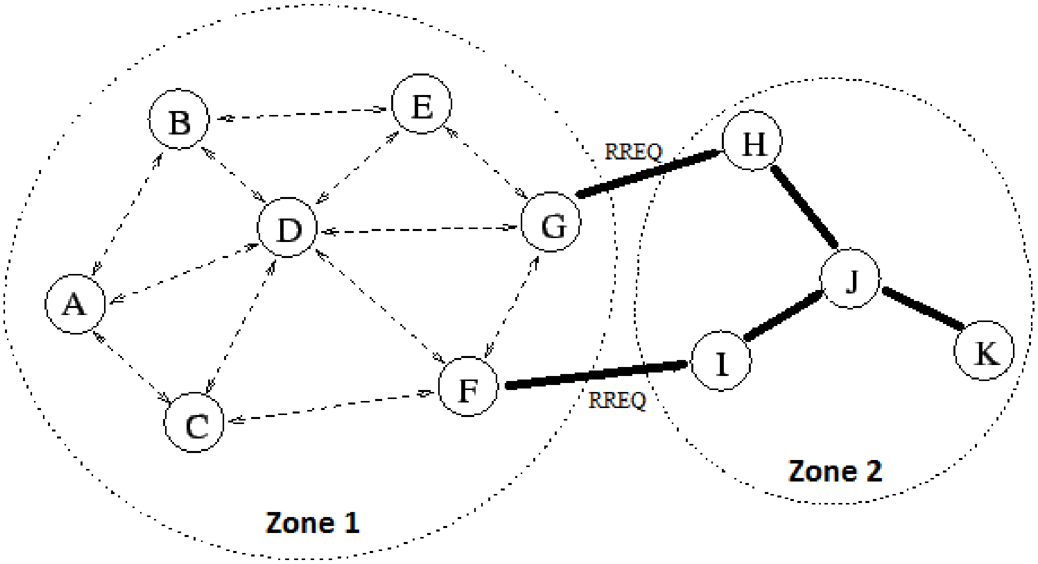


Fig.9. Zone Routing Protocol

8.3.2. Zone-based Hierarchical Link State (ZHLS)

The Zone-based Hierarchical Link State (ZHLS) hybrid routing protocol requires every mobile node in the network to know their physical locations via a GPS. The network is divided into zones based on geographical coordinates, rather than distance in hops between the mobile nodes. Moreover, this protocol uses a hierarchical addressing scheme where each node has a node ID and a zone ID. The zone ID of a node is determined according to its geographical location. Also, the network topology consists of two levels: node level topology and zone level topology. ZHLS routing protocol proactively maintains two types of link state updates: the node level Link State Packet (LSP) periodically broadcasted by each node within a zone, and the zone level LSP broadcasted by the gateway nodes throughout the network every time a link is broken or created. If the destination lies in the same zone as the source, a route already exists. If the destination lies in a different zone, the source node sends a ‘location request’ to all other zones through its zone’s gateway or boundary nodes. Once a boundary node of the zone in which destination belongs receives the location request packet, it replies back with a ‘location response’ which contains the zone ID of the destination. On receiving the zone ID, source node transmits data packets to that particular zone and the boundary node then forwards it to the actual destination using the intra-zone routing table. An advantage of this protocol is that there is no control overhead associated with cluster-head or location manager selection as compared to other routing protocols following similar approach of partitioning the network. ZHLS is highly adaptable to dynamic network topology and thus scalable to large networks as well. [30]

The table below compares the 2 hybrid routing protocols discussed according to the route metric used in the routing process, ‘Hello’ message for maintaining the neighbor relationships, route re-configuration, features and advantages/disadvantages.

Protocol	Route Metric	‘Hello’	Route Re-configuration	Features and Advantages / Disadvantages
ZRP	shortest path	yes	route repair at point of failure, notify source	- zone-based, link-state routing - low overhead - reduced delays - reduced re-transmissions - overlapping zones
ZHLS	shortest path or next available	no	location request	- zone and location-based, link-state routing - low overhead - reduced delays - reduced single point of failures - GPS required

Table 3. Comparison between Hybrid Routing Protocols

9. CRYPTOGRAPHIC SOLUTIONS

There has been research going on to try to find different ways to secure the routing protocols in Mobile Ad hoc Networks against the various attacks discussed earlier. Some of the existing solutions are stand-alone routing protocols, while others are add-on mechanisms to the traditional routing protocols. It is important to ensure that the add-on mechanisms trying to secure the network do not hinder the routing operation in MANETs. One of the most effective solutions for securing these networks is integrating the use of cryptography in routing protocols in order to strengthen the protocols themselves, as well as the network. These solutions can be classified into three main types depending on what type of cryptographic method is used. They are as follows:

i) Using asymmetric cryptography
ii) Using symmetric cryptography
iii) Using hybrid cryptography

9.1 Using Asymmetric Cryptography

This solution for securing routing in Mobile Ad-hoc Networks requires a universally Trusted Third Party (TTP) that issues certificates for binding a mobile node’s public key to its persistent identifier. An example of routing protocol that uses this approach is the Authenticated Routing for Ad-hoc Networks (ARAN) protocol.

9.1.1. Authenticated Routing for Ad-hoc Networks (ARAN)

The Authenticated Routing for Ad-hoc Networks (ARAN) protocol is an advanced source-initiated on-demand routing protocol for MANETs which utilizes cryptographic certificates for securing routing. It attempts to achieve the security goals of authentication and non-repudiation through three operational stages: preliminary certification, route discovery and shortest path confirmation. The third stage, i.e. shortest path confirmation is optional.

The *preliminary certification* process requires a trusted Certification Authority (CA) to be a part of the network. Before trying to connect to the MANET, each node must contact the CA for requesting a certificate for its address and a public key. In the *route discovery* process, the source node broadcasts a signed Route Discovery Packet (RDP), which contains its own certificate, a nonce, a timestamp and the address of the destination node. Each intermediate node in the network receiving the RDP validates the signature with the certificate, updates its routing table with the neighbor from which it received the RDP, signs it and forwards it ahead to its neighbor. Before forwarding, it removes the signature of previous neighbor node. Each intermediate node does so, but the source node's signature and certificate are always kept intact. The signature plays an important role in securing the network as it prevents malicious nodes from introducing false RDPs that may modify existing valid routes or form loops. The destination node, on receiving the RDP, replies back with a signed Reply packet (REP) which contains its own certificate, a nonce, timestamp and the address of the source node. The REP is transmitted back along the reverse path through a similar process. On receiving the REP from destination node, the source verifies it by checking the nonce and signature before transmitting data packets to it. Each node in the network maintains a routing table which contains entries for active routes. Another security measure in ARAN is that only the destination node is allowed to reply to RDP with a REP. Intermediate nodes cannot reply back even if they have a valid route to the destination. In the optional *shortest path confirmation* process, after the source node has a route to the destination node, it broadcasts a signed Shortest Path Confirmation (SPC) message which contains the destination address, a nonce, timestamp and its certificate similar to the route discovery process. The destination node on receiving the first SPC, verifies its validity and replies back with a Recorded Shortest Path (RSP) message. The source node on receiving the RSP verifies it and confirms the shortest path to the destination. [6]

Moreover, in the ARAN protocol, failed links are reported by the neighbors through a broadcasted signed Error (ERR) message that contains a nonce and timestamp. The signature ensures that the ERR message is not sent by a malicious node, thus avoiding fabrication attack. Also, the timestamps acts as a protection against replay attacks. This protocol effectively protects Mobile Ad-hoc networks from modification, fabrication and impersonation attacks.

9.2. Using Symmetric Cryptography

This solution uses symmetric cryptography for securing routing in MANETs. A very common mechanism used for this purpose is ‘hash functions’. Hash functions can be used specifically for hop count authentication. Examples of protocols providing this solution are SRP, SEAD and Ariadne.

9.2.1. Secure Routing Protocol (SRP)

The Secure Routing Protocol (SRP) is basically an extension that can be applied to the existing reactive routing protocols. This protocol provides security against attacks that try to disrupt the route discovery phase. The source node initiating the route discovery can identify and discard the route replies from malicious nodes that try to introduce false routing information in the network. This protocol requires a Security Association (SA) between the source node and the destination node, which is utilized to establish a shared secret key between the two nodes. For initiating the route request, source node generates a MAC by a keyed hash algorithm, which is placed in the SRP header. Before forwarding the route request packets ahead, the intermediate node measures the frequency of those requests received by its neighbors and maintains a priority ranking which is inversely proportional to the frequency of queries. A malicious node transmitting fake route request message will have low frequency of route requests and thus a low priority ranking, causing its request to me served last or ignored. When the destination node receives a route request packet, it verifies its integrity and authenticity by calculating the keyed hash and comparing it with the MAC contained in the SRP header that was generated by the source node. If the route request is genuine, the destination node replies back with a route reply using the same process. When the source node receives the route reply packet, it verifies the MAC generated by the destination node contained in the SRP header. Any route reply message that was not sent by the destination node will be discarded.

SRP effectively eliminates fabrication and modification attacks where the attacker tries to modify or replay the routing packets through a malicious node. This protocol is very effective as it provides end-to-end authentication and is also immune to spoofing attacks. [6]

9.2.2. Secure Efficient Ad-hoc Distance vector (SEAD)

The Secure Efficient Ad-hoc Distance vector (SEAD) is a proactive routing protocol based on the traditional DSDV protocol. This protocol focuses mainly on protection against modification and replay attacks. It uses ‘hash chains’ to authenticate hop counts and sequence numbers. A hash chain is created when a one-way hash function is applied repeatedly to a random value. The elements of a hash chain can be used to secure the periodic updates of the routing protocol. SEAD protocol also requires a trusted entity between the source and destination that can provide authentication and public key distribution, which distributes one authentic element of the hash chain between the two nodes. It can be used later to authenticate all other elements of that hash chain. When a mobile node sends a routing update message, one element of the hash chain is included for each entry. It also includes the address of destination node, the metric and the sequence number of the destination and a hash element equal to the one received when the node learnt that route update. This hash element can be authenticated by all the nodes receiving the update message as they have an already authenticated element of the same hash chain. In this way, the sequence number, metric in the routing update message as well as the sender is authenticated. Authenticating the source of each routing update message protects the network against impersonation attacks. Also, a Denial of Service attack can be countered by the receiving node specifying the exact number of hashes it performs for each authentication. [31]

9.2.3. Ariadne

The Ariadne is a secure on-demand ad-hoc routing protocol based on the traditional DSR protocol. This protocol provides end-to-end authentication of messages. It also requires a shared secret key to be distributed between the source and destination node and uses Message Authentication Code (MAC) to provide authentication. Ariadne uses the TESLA broadcast authentication protocol to authenticate the route request packets, where the sender generates a one-way key chain and defines a schedule according to which it reveals the keys of the chain in reverse order from generation. In the route discovery process, the route request packet consists of various fields such as source node's address, destination node's address, an ID that identifies the current route discovery, a TESLA time interval which specifies the expected arrival time of the packet to the destination, a hash chain and two empty lists: a node list and a MAC list. Each intermediate node receiving the route request packet verifies that the TESLA time interval is not too far in the future and that its corresponding key is not revealed yet. Once verified, this intermediate node inserts its own address in the node list field, replaces the hash chain and adds the MAC of entire packet to the MAC list field of packet, before forwarding it ahead. If the verification fails, the packet is discarded. When the destination node receives the route request packet, it checks its validity by ensuring that the corresponding keys from the TESLA time interval specified have not been revealed yet and that the included hash chain can be verified. Finally, the destination node replies back with a route reply packet that contains the same fields as the corresponding route request packet, and in addition a target MAC field and an empty key list. The target MAC is nothing but the computed MAC of the preceding fields of the route reply. The route reply packet is forwarded back to the source node via the reverse of the route included in the node list of request, as soon as the destination's key is revealed after the specified time interval. The intermediate node receiving the route reply packet waits until its key is revealed from the TESLA time interval specified. Once revealed, it adds its key to the key list field of the packet and forwards it to the next intermediate node in the route. Each intermediate node follows this process. Once the source node receives the route reply packet, it verifies that each key in the key list is valid, that the target MAC is valid and that each MAC in the MAC field is valid. The route reply is accepted by the source node and data transfer is initiated only if all the verifications pass.

In the route maintenance phase, the Ariadne protocol ensures that the route error messages generated because of failed links in the network are genuine messages. The neighbor node of the failed link that generates the route error message includes TESLA authentication information in it and each node forwarding the route error message authenticates it. All the intermediate nodes buffer the route error message, but its authentication is completed only after the node generating that route error message reveals the key. Ariadne provides protection against modification, fabrication, impersonation and wormhole attacks performed by malicious nodes in the network. Also, flooding attacks are avoided that can lead to a routing cache poisoning attack. The route discovery process of Ariadne protocols enables nodes to discard false or excessive route request packets. One important requirement for proper functioning of this protocol is that there must be clock synchronization between all the mobile nodes in MANET. [33]

9.3. Using Hybrid Cryptography

This solution uses both asymmetric as well as symmetric cryptographic operations in the routing protocols. A common approach for this solution is to digitally sign the fixed fields of routing messages so that they cannot be modified, and to use hash chains for hop count authentication.

9.3.1. Secure Ad-hoc On-demand Distance Vector (SAODV)

The Secure Ad-hoc On-demand Distance Vector (SAODV) routing protocol is a security extension applied to the traditional AODV routing protocol. This protocol uses digital signatures and hash chains, a combination of asymmetric and symmetric cryptographic schemes, for securing the Mobile Ad-hoc Network. To be specific, the digital signatures are used for authentication of the fixed fields of routing message packets. For securing the unfixed hop count field of control messages, a new one-way hash chain is created for each route discovery process. As the SAODV protocol uses asymmetric cryptography for digital certificates, a trusted third party certificate authority is required to be part of the network through which each mobile node must acquire and verify the public key of other nodes participating in the network. Because of the use of hash chains, the SAODV protocol has additional fields in the message as compared to AODV protocol, for example hash function, max hop count, top hash, hash, etc. The nodes transmitting either a route request packet or a route reply packet digitally signs all fields of the message, except the ‘hop count’ field and the ‘hash’ field. Each intermediate node receiving the route request message or route reply message verifies the integrity of the message via digital signature and the hop count via comparison of result of the application of hash function ‘max hop count’ minus hop count times to the ‘hash’ and the value of the ‘top hash’. Before forwarding the packet ahead, the intermediate node replaces the value of ‘hash’ by the result of calculation of the one-way hash of the hash field itself to account for the new hop. Moreover, in this protocol, route error messages that are generated are secured using digital signatures. Each node that generates or forwards a route error message cryptographically signs the entire message, except the destination sequence number. [32]

9.3.2. Secure Link State routing Protocol (SLSP)

The Secure Link State routing Protocol (SLSP) is designed to secure specifically the traditional proactive routing protocols used in MANETs. To be specific, this protocol's main aim is to secure the process of topology discovery and distribution of link state information within the network. A major advantage of this protocol is that it does not require a centralized key management server. SLSP can be divided into three main operations: public key distribution, neighbor discovery and link state updates. *Public key distribution* is performed by the mobile nodes broadcasting their public key certificates within their zone through signed Public Key Distribution (PKD) packets. The link state information is also broadcasted periodically through signed 'hello' messages, which also include the sender's MAC address and IP address. Each node receiving a hello packet can thus maintain a mapping of MAC address and IP address for other nodes in the network. 'Notification' messages are generated to discard suspicious messages, for e.g. if there are discrepancies like two IP addresses have the same MAC address or a node trying to claim MAC address of another node. The Link State Update (LSU) packets contain IP address of sender node, sequence number and the hop count which is authenticated using hash chains. Each node receiving an LSU packet verifies the attached signature of sender. This protocol effectively protects the network against Denial of Service attacks by each node maintaining a priority ranking of neighboring nodes, which is determined on the rate of control traffic they have observed. The neighboring nodes having the lowest rate of generating LSU packets are prioritized higher. Hence, a malicious node that tries to perform a flooding attack is not able to perform it effectively. [6]

10. SUMMARY

10.1. Conclusions

In this research paper, we determined the security criteria for protecting the Mobile Ad-hoc Networks against attacks. It is necessary to define the security goals in order to describe the security solutions that intend to achieve them. Further in the paper, entire list of vulnerabilities in MANETs were pointed out. Such networks are more prone to attacks compared to wired networks or fixed wireless networks because of their inherent characteristics. For example, lack of centralized management, limited power supply and the mobility of nodes causing the network topology to change dynamically make MANETs susceptible to threats from adversaries. Also, the traditional routing protocols were not very focused on security, since the primary area of research was to cope with the difficulties faced in routing itself because of the nature of network. MANETs can be used in various applications and each application typically has a unique security requirement. This made it even more difficult to research on the security solutions.

Furthermore, this paper discussed the different types of attacks that are known to be performed on the MANETs today. They were differentiated into different types. The attacks were mainly categorized according to the network protocol stacks of the OSI model. Most of the hazardous attacks are performed on the network layer where the routing process takes place for communications within the network. Thus, it is necessary to secure the routing protocols.

Next, the unicast routing protocols were introduced in detail. They were differentiated as proactive routing protocols, reactive routing protocols, hybrid routing protocols and the protocols that use cryptographic schemes for security. The proactive routing protocols maintain the network connectivity proactively via link state or distance vector algorithm, while the reactive routing protocols determine routes only when needed. On the other hand, the hybrid routing protocols use properties of both proactive and reactive protocols. Depending on the different application scenarios of Mobile Ad-hoc Networks, one routing protocol may be preferred over the other. But in most cases, the hybrid routing protocols prove to be more efficient. They overcome the limitations faced in both proactive and reactive protocols, and hence are more robust. Suitability of a routing protocol depends on various factors like application and scalability of the MANET, costs associated with it, etc. In some cases, proactive or reactive routing protocols may be the best suited protocol, while in other cases hybrid routing protocols or the more advanced ones using cryptographic methods may be suited. A set of generic mechanisms like secure neighbor detection, secure route delegation and randomized route request forwarding can protect the network against rushing attacks.

Moreover, the advanced routing protocols rely on cryptographic methods integrated into them to make the network secure, which is a very effective solution against attacks. These are mainly upgrades to the existing routing protocols to secure the Mobile Ad-hoc Networks. For example, the ARAN routing protocol provides security from Black Hole attacks where the malicious node may try to change the sequence number, hop count modification, source routing, or spoof the destination addresses. However, it requires a secure key management mechanism like a trusted third party to be a part of the MANET. The cryptographic solutions solve some major problems faced by Mobile Ad hoc Networks by effectively preventing the network against attacks like modification, fabrication, impersonation, replay, Denial of Service, wormhole, blackhole, flooding, etc. If the requirement of having a trusted third party in the network like a Certificate Authority (CA) is case of asymmetric solutions, and a Security Association (SA) in case of symmetric solutions is met, this approach for securing the routing protocols in MANETs provides protection against hazardous attacks, by making them robust.

To conclude, securing the routing protocols should be the first step in securing MANETSs because routing is the most vulnerable aspect. An attack on the routing protocols is hazardous as it can directly affect the performance and reliability of the network. If possible, the routing protocols using cryptographic solutions should always be preferred over reactive, proactive or the hybrid protocols. However, securing the routing protocols may not be sufficient. Even if the routing protocols used in MANETs are made secure, additional level of security may be required. The needs usually vary according to different networking scenarios and the security mechanisms in place for protection against attacks must be flexible. Other add-on mechanisms and security systems should also be considered for securing the network. There are various extensions that can protect against specific type of attacks. For example, the *Security-aware Ad-hoc Routing* (SAR) is a routing approach that treats secure routing as a Quality of Service (QoS) issue by introducing a security metric in the route discovery and maintenance mechanisms. The *Techniques for Intrusion Ad-hoc Routing Algorithms* (TIARA) is a set of design techniques that can be applied on the routing protocols used in MANETs. The main goal of these techniques is to diminish the impact of a Denial of Service attack once it is already performed and allow the acceptable communications in network.

10.2. Recommendations for Further Study

Security is Mobile Ad hoc Networks is a wide and complex area of study. This paper focused mainly on securing the routing aspect in such networks by trying to make the routing protocols more robust. Even though securing routing is the most important aspect in securing MANETs as a whole, there are other ways these networks can be protected against attacks. Most of these ways, not necessarily related to routing, are extensions that can be used in the network. For example, 'packet leashes' can be used for detecting, and thus protecting against wormhole attacks. The packet leash is some extra information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Each receiving node can determine whether a packet has traversed an unrealistic distance [6].

The 'watchdog' and 'pathrater' are two extensions that can be introduced in the Mobile Ad-hoc Network specifically in the DSR routing protocol, that try to detect and diminish the effect of malicious or selfish nodes, and thus improve the performance of network in presence of an attack. Watchdog secretly monitors the next node in the path to see whether it is forwarding packets as expected. Pathrater assesses the results of the watchdog and determines the most reliable path in case any misbehavior of node is recorded. Another set of extensions to the DSR routing protocol is the CONFIDANT. It includes a monitor, a reputation system, path manager and a trust manager that each node in the network must operate. Routes are created and maintained according to the monitored behavior of the nodes and the ratings assigned through observation.

In addition to these mechanisms, Intrusion Detection Systems (IDS) can be introduced in the Mobile Ad hoc Network that can help in further strengthening the network security. These extensions may not be easily available or could be difficult to deploy in certain network scenarios. When used along with the advanced routing protocols using cryptographic solutions, they can significantly overcome the security problems in MANETs. Hence, these extensions are definitely good topics for further research in securing the MANETs.

BIBLIOGRAPHY

[1] Athulya M.S. and Sheeba V.S.,"Security in Mobile Ad-Hoc Networks", *Third International Conference on Computing Communication & Networking Technologies,* 2012.

[2] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks- A Survey", *The 17th White House Papers Graduate Research In Informatics at Sussex*, 2004.

[3] P. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks", *The Seventh International Symposium on Communication Theory and Applications (ISCTA),* July 2003.

[4] D. Djenouri , L. Khelladi and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks", *IEEE Communications Surveys & Tutorials,* vol. 7, 2005.

[5] Shervin Ehrampoosh and Ali Mahani, "Secure Routing Protocol: Affection on MANETs Performance", *International Journal of Communications and Information Technology (IJCIT),* Vol.1, Dec. 2011.

[6] Patroklos G. Argyroudis and Donal O'mahony, "Secure Routing for Mobile Ad Hoc Networks", University Of Dublin, Trinity College, *IEEE Communications Surveys*, vol. 7, 2005.

[7] Priyanka Goyal, Vinti Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", *International Journal of Computational Engineering & Management*, Vol. 11, January 2011.

[8] Sheikh R., Singh Chande M. and Mishra D.K., "Security issues in MANET: A review*", Seventh International Conference on Wireless And Optical Communications Networks*, 2010.

[9] Michele Nogueira Lima, Aldri Luiz dos Santos and Guy Pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks", *IEEE Communications Surveys & Tutorials*, Vol. 11, 2009.

[10] Tameem Eissa, Shukor Abd Razak and Asri Ngadi, “Enhancing MANET Security Using Secret Public Keys”, *International Conference on Future Networks,* 2009.

[11] Marco Carvalho, “Security in Mobile Ad Hoc Networks”, *IEEE Security & Privacy*, 2008.

[12] D. Wang, M. Hu and H. Zhi, "A survey of Secure Routing in Ad Hoc Networks", *IEEE 9th International Conference on Web Age Information Management*, 2008.

[13] Andel T.R. and Yasinsac A., "Surveying Security Analysis Techniques in MANET Routing Protocols", *IEEE Communication Surveys & Tutorials*, 2007.

[14] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges”, *Journal of the Communications Network*, July 2004.

[15] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, “Security in mobile ad hoc networks: Challenges and Solutions”, *IEEE Wireless Communications*, 2004.

[16] Imrich Chlamtac, Marco Conti and Jennifer J. N. Liu, “Mobile ad hoc networking: imperatives and challenges”, *Ad Hoc Networks*, July 2003.

[17] Changling Liu and Jorg Kaiser, “A Survey of Mobile Ad Hoc Network Routing Protocols”, *MINEMA*, University of Magdeburg, October 2005.

[18] Liang Qin and Thomas Kunz, “Survey on Mobile Ad Hoc Network Routing Protocols and Cross-Layer Design”, Carleton University, August 2004.

[19] Mehran Abolhansan, Tadeusz Wysocki and Eryk Dutkiewicz, “A review of routing protocols for mobile ad hoc networks”, *Ad Hoc Networks*, 2004.

[20] Yih-Chun Hu and Adrian Perrig, “A Survey of Secure Wireless Ad Hoc Routing”, *IEEE Security & Privacy*, June 2004.

[21] Hongmei Deng, Wei Li and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Networks”, *IEEE Communications Magazine*, University of Cincinnati, November 2002.

[22] Sevil Şen, John A. Clark and Juan E. Tapiador, “Security Threats in Mobile Ad Hoc Networks”, Department of Computer Science, University of York, UK, 2010.

[23] Bing Wu, Jianmin Chenm Jie Wu and Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, *Wireless Network Security*, 2007.

[24] Routing Basics - http://docwiki.cisco.com/wiki/Routing_Basics

[25] Y.C. Hu, A. Perrig and D. B. Johnson, “Rushing attacks and defense in wireless ad hoc network routing protocols”, *WiSe*, 2003.

[26] The Difference between a Computer Virus, Worm and Trojan Horse - http://www.webopedia.com/DidYouKnow/Internet/virus.asp

[27] Padmalaya Nayak, V. Bhavani and B. Lavanya, “Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN”, *International Journal of Computer Applications* Volume 116, April 2015.

[28] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto and N. Kato, “A Collusion Attack against OLSR-based Mobile Ad Hoc Networks”, *IEEE GLOBECOM*, November 2006.

[29] Mehran Abolhasan, Tadeusz Wysocki and Eryk Dutkiewicz, “A review of routing protocols for mobile ad hoc networks”, *Ad Hoc Networks*, 2004.

[30] Changling Liu and Jörg Kaiser, “A Survey of Mobile Ad Hoc network Routing Protocols”, *MINEMA*, University of Magdeburg, October 2005.

[31] Y.-C. Hu, A. Perrig and D. B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks,” *INFOCOM*, 2003.

[32] M. G. Zapata, and N. Asokan, “Secure Ad hoc On-demand Distance Vector Routing,” *ACM Mobile Comp. and Commun. Review*, July 2002.

[33] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks,” *Mobicom*, September 2002.