Analysis of Security Mechanism in Adhoc Network with Machine Learning Techniques

Uma Maheshwari [1,*], Suresh Babu [2], Mahendra khan [3], Kadiyam Rajshekar [4], Manideepika Manchikalapati [5]

[1,2,3] Hindusthan Institute of Technology, Anna University, India

[4,5]QIS Engineering College, Nehru University, India

Emails: umamaheshwari@hit.edu.in; sureshbabu.v@hit.edu.in; k.mahendrakan@gmail.com; rajshekar.k@qiscet.edu.in; manideepika.m@qiscet.edu.in

Corresponding Author Mail: umamaheshwari@hit.edu.in

Abstract

In an ad hoc network, the routing protocol takes into account a variety of activities, including maintaining network connection, transmission scheduling, channel evaluation, and preserving network connectivity. Additionally, it determines network architecture. In addition, a number of different elements determines the performance of a routing protocol. These include node mobility, which is responsible for multiple link failures, support for quality of service (QoS), network size, the amount of traffic, and the level of security. The performance may occasionally also be affected by the manner in which the network is behaving in addition to the kinds of apps that are running in that environment. Selecting an appropriate protocol that is based on security is highly crucial in order to set up an effective network. A significant amount of effort has been put into improving the safety mechanisms that are built into routing protocols, most prominently in WSNs, MANETs, VANETs, and WMNs. Only MANET will be the topic of discussion here. Mobile Ad-Hoc Network is a wireless network that does not need infrastructure and is composed of mobile nodes. Mobile ad-hoc network, also known as MANET, is one of the most promising forms of next-generation wireless networking technology. It has garnered a significant amount of interest because it is self-organized and can be deployed at a cheap cost. In comparison to a traditional network, a MANET presents a number of challenges that are especially difficult to overcome when it comes to the duty of routing. The many difficulties that are inherent with MANET have made it an excellent subject for academic investigation. This provides a concise overview of security in MANETs as well as the issues that relate to maintaining them. Understanding the different routing mechanisms and the potential attacks that might be mounted against them is the first step in designing a reliable security mechanism. Within the scope of this study effort, we have provided specifics on the detection and prevention of various routing attacks, with the primary emphasis being placed on the network layer assaults that are unique to MANET. When compared to other study fields, MANET presents the greatest challenge in terms of maintaining network security. In recent years, a significant amount of research has been carried out to investigate several forms of assault; nevertheless, most of the surveys have been carried out without any kind of performance analysis. There is a paucity of research that seeks to find an all-encompassing study of the impact of the many different attacks that bring the overall performance of the Adhoc network down. On the other hand, secure routing in the face of a black hole attack can be difficult because preferences are often incomplete. The in-degree centrality and importance degree measurement applied to the collected consensus-based trust from decision-makers solves the issue of incomplete preferences and improves the accuracy of trust at the same time. Utilizing Network Simulator, we examine how well the suggested approach works. Based on the findings of the simulations, it has been demonstrated that the detection accuracy and throughput of the proposed CREDIT are both significantly higher than those of existing work, making the proposed CREDIT scheme superior.

Doi: https://doi.org/10.54216/IJWAC.000103

Keywords: Ad-Hoc Network; Mobile ad-hoc network; routing protocol; Black-hole attack

1. Introduction

The MANET routing protocol [1]is a topic of current research interest. It is one of the developing areas that enables users to communicate without any physical infrastructure, regardless of their geographical location, and the network itself does not require any physical infrastructure. Applications of MANET are currently being used in a wide variety of fields, ranging from task forces to emerging operations and disaster relief to military services. The provision of security [2] is of the utmost importance in such applications. MANET is susceptible to severe security attacks because of the involvement of mobile nodes. These attacks can be caused by a number of factors, including restricted physical security, compelling topology, scalability, and the absence of a central authority. Security solutions for MANET are extremely difficult to implement as a result of these factors.

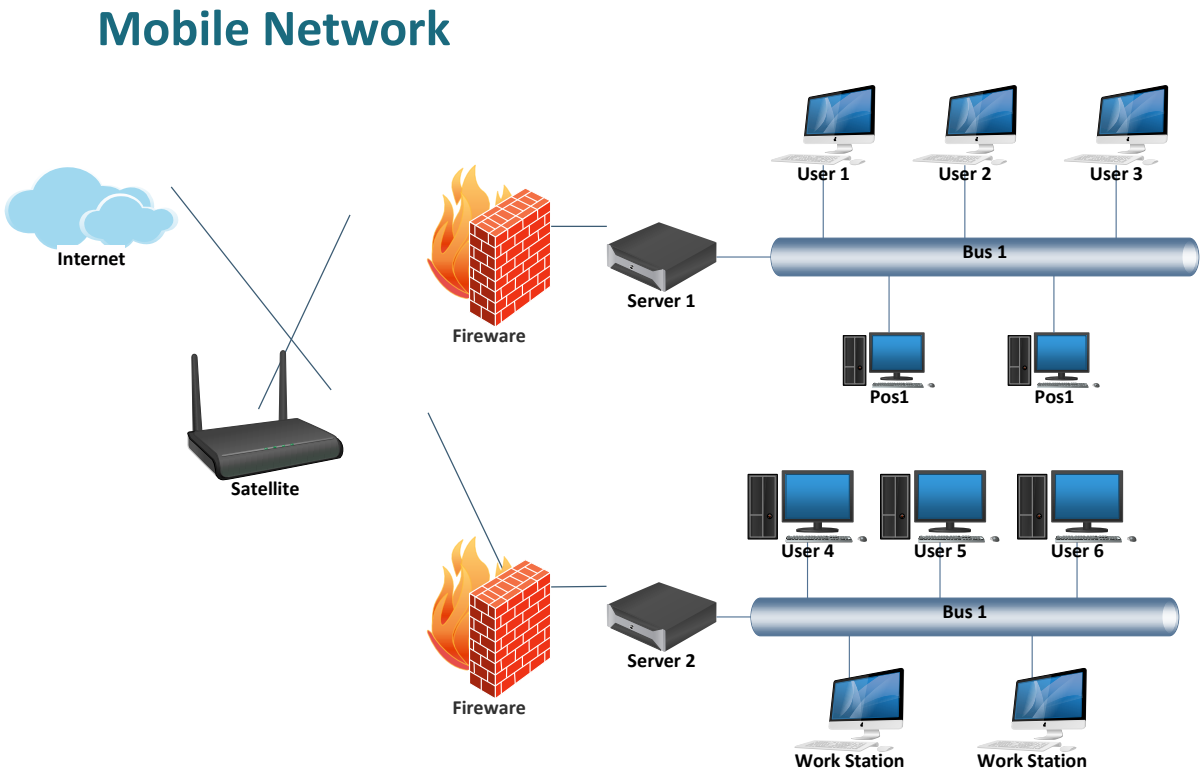

Figure 1: Mobile Adhoc Network

In addition, the security methods that are utilized for wired networks cannot be easily applied to MANETs. Providing a security solution for MANET that is effective against attacks is a very challenging task. First things first: before we can offer any security solutions [3] against attacks, we need to have a solid understanding of the various possible forms that attacks can take. In a MANET, ensuring that messages are securely transmitted over the communication channel is of the utmost importance. There are several solutions that have mechanisms for classified prevention and detection, but these mechanisms are unable to guarantee the classifications of mobile nodes. The prevention approach relies heavily on cryptographic procedures, which are not compatible with the properties of MANETs. In addition to such solutions, they are successful in the discovery of a few attacks [4]; however, these mechanisms are unable to recognize other attacks, particularly packet-dropping attacks such as black-hole and flooding attacks. The trust-based secure solution for the MANET routing protocol that we presented may be found in this proposed work.

1.1 Objectives

The primary goals are outlined in the following paragraphs.

Doi: https://doi.org/10.54216/IJWAC.000103

1. Investigate both the structure of the Mobile Adhoc Network (MANET), as well as its characteristics. In addition, research should be done on MANET routing algorithms, including an analysis of the benefits and drawbacks of each.
2. Conduct research on and analysis of the effect that severe attacks had on the AODV reactive routing technology used in MANET. We are doing research on a number of different kinds of assaults that have been launched against AODV, including blackhole attacks, flooding attacks, sinkhole attacks, and rushing attacks, among others. These particular attacks include modifying, fabricating, and impersonating the routing packets of the AODV protocol.
3. Design and implementation of a novel strategy that is capable of defending against blackhole attacks and dropping of packets, both of which have a significant detrimental effect on the performance of the AODV reactive routing protocol.
The idea of trust would serve as the foundation for the construction of this strategy in order to validate a high trustworthiness ratio of nodes. Because of limitations on MANET resources, this cryptographic mechanism would not be incorporated into the use of any other cryptographic mechanism. It is a very difficult task to design a safe and effective routing system for MANET. Decentralized authority is the foundation on which more modern routing systems are built. In addition, it is assumed that the nodes that make up a MANET work together and that no malicious activity disrupts the routing protocols. MANETs are frequently more susceptible to severe security breaches than other wireless and wired networks. This is typically the case as a result of inherent properties such as the mobility of nodes, decentralized authority, trusted third parties, and limited resources. Due to the nature of MANET, implementing safe mechanisms like cryptographic and trust-based algorithms may be a challenging endeavor because of the intrinsic properties of the system. Researchers are motivated to find ways to prevent different severe assaults, ranging from diverse passive eavesdropping to active attacks since MANET presents a variety of security issues. The main emphasis of this proposed work is on some of the most damaging routing attacks that may be launched against MANET. By using the NS-2 network simulator, we have finished the detailed implementation of these attacks inside the AODV routing protocol. Researchers, practitioners, and scientists who are working in the field of wireless Adhoc and sensor networks will benefit from reading the proposed work. In addition to that, we will detail the contributions made by the proposed work.

1.2 Contribution

1. We have conducted in-depth literature research on the topic of security in MANET and the difficulties that are linked with it. Understanding the different routing mechanisms and the potential attacks that might be mounted against them is the first step in designing a reliable security mechanism. It provides information regarding the detection and prevention of possible routing attacks, with the primary emphasis being placed on network layer attacks that are unique to MANET.
2. An investigation of the effectiveness of some of the most damaging routing attacks against MANET is carried out. By using the NS-2 network simulator, we have finished the detailed implementation of these attacks inside the AODV routing protocol. 18 An Examination of the Safety Measures Contained Within Ad-Hoc Networks

3. Make a suggestion for a secure AODV protocol that is based on the Consensus Routing and Environmental DIscrete Trust (CREDIT) system. Both the detection of blackhole attacks and the enhancement of routing performance via the use of discrete and consensus trust measurement are goals of the new CREDIT protocol that has been suggested. 4. In order to guarantee secure routing, suggest a trustworthy watchdog node-based intrusion detection scheme (also known as TWIST). The TWIST model that was proposed has the goal of achieving a secure MANET by detecting and mitigating an attack of packet dropping using an IDS model that is based on a finite state machine.

2. Related Work

[4] defines a mobile ad hoc network, also known as a MANET, as a sort of multi-hop wireless network that may be thought of as a collection of wireless mobile devices that are capable of configuring and organizing themselves on their own. There is no need for any kind of central coordination since the devices that make up a MANET are able to engage in direct communication with one another within their broadcast range without the need for any kind of base station. Therefore, the MANET [5] may alternatively be characterized as a decentralized network. This definition describes a network in which there is no base station to coordinate the flow of messages.

Routers, which are used in wired networks, and access points, which are used in wireless networks are examples of the additional devices that are required in traditional networks in order to identify the paths that must be taken

Doi: https://doi.org/10.54216/IJWAC.000103

in order to establish communication between nodes. However, with a MANET [6], each node is solely accountable for its own routing, whether it is the transmission of RREQ packets or control messages. Every node in the network acts similarly to a router in that it will forward any packets that are not directly relevant to the node's own purpose. Since MANET does not make use of any pre-existing infrastructure, it is often referred to as an infrastructure-less network. As a result, setting up the network is very simple and inexpensive [7]. Every node in the network has complete mobility with regard to entry and exit at any given moment. The term "massive ad hoc network" (MANET) refers to a kind of wireless local area network (WLAN) that is formed organically as devices join. Due to the fact that the structure of the network and its nodes are not pre-defined. [Corson et al. 1999] found that the Analysis of Security Mechanisms in an Adhoc Network could readily move independently and that it followed the dynamic topology [8].

The primary goal of the MANET is to enable networking to take place at any time and in any location. [9] The packet radio network was the first wireless network system and is also considered to be the first generation of MANET. It was later sponsored by the Defense Advanced Research Project Agency (DARPA) in the early 1970s. DARPA is an acronym that stands for the Defense Advanced Research Project Agency [10]. In order to provide an infrastructure-free packet-switched network, it relied heavily on CSMA [11] and ALOHA [12] as its primary networking protocols. Does the second generation begin in the early 1980s, when the considerable emphasis is paid to the cost, scalability, and security concerns of the network? If so, the second generation begins at this time. [13] , which stands for Global Mobile Information System, and NTDR [14], which stands for Near Term Digital Radio, were the two most significant innovations of this generation.

The first two versions of the mobile Ad-hoc network were developed in response to a variety of challenges faced by the military. The addition of combat activities was the primary focus of both previous and current iterations of the program. The third version of MANET [15] was designed primarily with business applications in mind. A mobile ad hoc network is shown in figure 1. Mobile Ad-Hoc Network Compared to Sensor Network in Terms of Feature The deployment of MANET and WSN was dispersed. Extremely High Probability of Failure Rare More Point-to-Point Communication Mode Broadcast Centri Mode [16] Based on Address Based on Data Redundancy Point-to-Point Communication Mode Changes in Network Topology That Are Lower, Higher, and Lower in Data Rate Topology of Rare, Frequent, and Frequently Replaceable Batteries that Are Not Rechargeable Long and Short Range Dynamic Communication Long and Short Range [17].

Table 1: Mobile Adhoc Network Vs Sensor Network Challenges in Mobile Ad-hoc Network

Feature	MANET	WSN
Deployment	Seattered	Very Dense
Failure Rate	Vary Fare	More
Communication Mode	Point to Point	Broadcast
Centri Mode	Based on Address	Based on Data
Redundancy	Low	High
Data Rate	Higher	Lower
change in Network Topology	Rare	Frequent
Battery	Replaceable	Not Rechargeable
Topology	Dynamic	Dynamic
Communication Range	Long	Small

Doi: https://doi.org/10.54216/IJWAC.000103

The MANET architecture is quite unlike that of traditional networks. According to [18] it offers a considerable level of flexibility in terms of the topology, infrastructure, size, and status of the network. An Examination of the Safety Measures Contained Within Ad-Hoc Networks The management of anything with this degree of adaptability is often more difficult. According to [19] some of the most challenging aspects of MANET include the mobility of the nodes, limited power and bandwidth, and the provision of Quality of Service (QoS). Challenges Mobility Power Quality of Service Bandwidth Security [20]

Figure 2: Challenges in MANET

• Mobility: MANET enables the devices to freely move in any direction by providing them with the flexibility to do so. It makes it possible for nodes to join, leave, or build the network at any time and from any location. Mobility is beneficial to the devices; nevertheless, it makes working with MANET [21] more difficult. According to "Mohapatra et al. 2012," high mobility results in frequent link breakage, which creates difficulties in routing since any node that is a part of the transmission path may alter its location or even quit the network at any moment.

• Electricity and Bandwidth: Because mobile devices run on batteries, they have a limited amount of power available to them. In addition to this, they struggle with the issue of constrained bandwidth. Because of this, MANET has to have an extremely efficient routing algorithm that can figure out the best possible routes for data packets to take so that they may be transferred while using the least amount of power and bandwidth possible. The power provided by batteries in a MANET is more susceptible to intrusion attempts [22] found that some of the invaders make an attempt to interrupt the power supply. Because of this, it might cause the network to partition, and it might also cause the battery to drain. The connection capacity of the wireless network is much lower when compared to that of the wired network. Interference and channel fading are more likely to occur with wireless communications. This occurs as a result of noise on the channel and several users using it at the same time.

• Quality of Service: QoS is the issue that is responsible for the MANET becoming a more difficult region. MANET is a wireless network, and wireless connections, in contrast to wired links, are subject to increased data loss, distortion, delays, and changes in speed and capacity. This makes it challenging to provide quality assurance for the service being provided via wireless links. Since a dynamic topology is followed by MANETs, it is extremely difficult to obtain accurate information regarding the state of the network and the devices, and it is even more difficult to provide quality service.

3. Proposed Methodology

MANET is a collection of mobile nodes that are capable of configuring themselves and operating together as part of an ad hoc network. Because there is no permanent infrastructure, nodes may be added to the network in whatever order they like. It implies that a mobile node is able to travel in a random or free manner while still being able to communicate with other nodes that are within its radio range. Each node in a MANET exhibits two distinct behaviors at the same time. They are capable of functioning in the network both as a router and a host. Examples of MANET include PDAs, smartphones, computers, etc. In addition to that, MANET has a few restrictions in place as well. There is a possibility that a MANET node will have restricted access to its energy resources, limited communication, and limited computing found that a MANET is much more vulnerable to a variety of severe assaults when compared to a wired network. There are several explanations for this.

Doi: https://doi.org/10.54216/IJWAC.000103

1. The limited energy of the node prevents elaborate security calculations from being performed.

2. Because the wireless network is an open network, the transmission of a data packet during the routing of any information or the sharing of any information is unreliable, and an attacker may simply conduct eavesdropping or intercept the message. Even while utilizing the reliable link, MANETs' broadcasting nature makes it possible that the connection will still be unstable.

3. In an ad hoc network, there is no centralized authority that manages the nodes. It might be difficult to determine whether or not all of the network nodes are engaged in the activity.

4. Because users are mobile, the topology of the network is always shifting and evolving. In this sense, routing in Manet becomes a more difficult task.

It is possible to launch an attack at any level of the TCP/IP protocol stack that is used by the MANET. However, according to existing works, assaults that target the network layer or the routing layer do the greatest damage to the system. There are two types of routing assaults: an insider attack and an outsider attack. Insider attacks are more common than outer attacks. The external attacker does not have access to any authentication information about data packets or control packets. Utilizing cryptographic protocols allows for the identification and prevention of an external attacker. An inside attacker, on the other hand, is far more hazardous than an external attacker. Because every insider node has access to every piece of cryptographic information, these attackers may not be able to directly manipulate the encryption scheme. state that it is essential to have a comprehensive understanding of the behavior of an assault before attempting to guard against an insider attack. The primary objective of this proposed work is to investigate the ways in which the AODV protocol may be manipulated, exploited, or otherwise tampered with by a malicious node.

3.1 Adhoc On-Demand Distance Vector Routing

The RFC(3561) paper serves as the foundation for the AODV Routing Protocol. It is a kind of routing technology known as reactive routing. When necessary, AODV will generate a new route. When compared to other routing protocols used in MANETS, AODV provides superior performance. It is the protocol that is spoken about, compared to, and expanded upon the most when compared to other protocols. In the routing table, AODV simply maintains a single routing record for the destination. As a result of this, it requires a minimal amount of network resources in MANET, has a smaller memory footprint, is more efficient while operating in highly mobile environments, and has a smaller memory footprint overall. AODV employs DesSeqNum, which stands in contrast to other reactive procedures (Destination Sequence Number). A current and accurate routing route to the destination may be maintained with the help of the destination sequence number. Every node will only continue to update its destination path in the event that the DesSeqNum of the most recently received packet is higher than the value that was most recently recorded at the routing node. There are a few things that need to be taken into mind before AODV can be improved.

- There is room for more development in terms of Network QoS.
- It is important to take into consideration the optimum route-finding procedure.
- The Route Maintenance mechanism has to have the route maintenance process optimized in order to account for path failures while the data is being sent.
- There must be a specific provision in AODV for the implementation of protective measures against assaults.

3.2 AODV Protocol Functioning

To comprehend performance analysis and to be able to alter a protocol, it is critical to have a solid grasp of how a protocol operates and how it should be changed. In its most basic form, the AODV protocol is comprised of two processes: the first of which is discovery, and the second of which is route maintenance. In the following sections, the functionality of the protocol will be explored with the assistance of a flowchart of the action of an AODV node, which can be found in section 3.2.

Discovery of the Route

Doi: https://doi.org/10.54216/IJWAC.000103

During the process of route discovery, the source node sends out a flood of route request packets, known as RREQs, over the whole network. The source address (SA), the broadcast id, the destination address, the sequence number (Seq no.), and the hop count, among other things, are stored in the route request packet (RREQ). An RREQ packet may be recognized on a network by its broadcast id as well as its Sequence number. In a network, if a neighboring node gets an RREQ packet and that node maintains information on a route to a destination, then that neighboring node instantly sends a uni-cast route reply (RREP) packet to the original source node. The source IP, the destination IP, the sequence number, the hop count, and the lifespan of the packet are all included in an RREP packet. In addition, if an intermediate node's routing database does not have any route information for the destination, the node will instantly send the packet to other intermediate nodes that are coupled with it. In addition to this, it revises the record for the route reverse in the routing table so that it may be used later. In conclusion, the destination node will send an RREP packet as a response to the source if it has received any RREQ packet.

Route Maintenance:

In a wireless network, there is always the possibility that a connection may break. because of a problem with the connectivity when the data was being sent. It results in lost packets and reduces the overall performance of the network. The AODV routing protocol includes a route maintenance mechanism to help deal with problems like these that might arise during the process of routing data packets over a network. The RRER message is what the route maintenance mechanism sends out when it encounters a link failure error. If a connection failure occurs while data is being sent via this approach, every intermediate node will use unicasting communication to alert its upstream nodes of the failure. RRER packets retain some information, such as the unreachable destination sequence number, the unreachable destination IP address, and the destination count.

Doi: https://doi.org/10.54216/IJWAC.000103

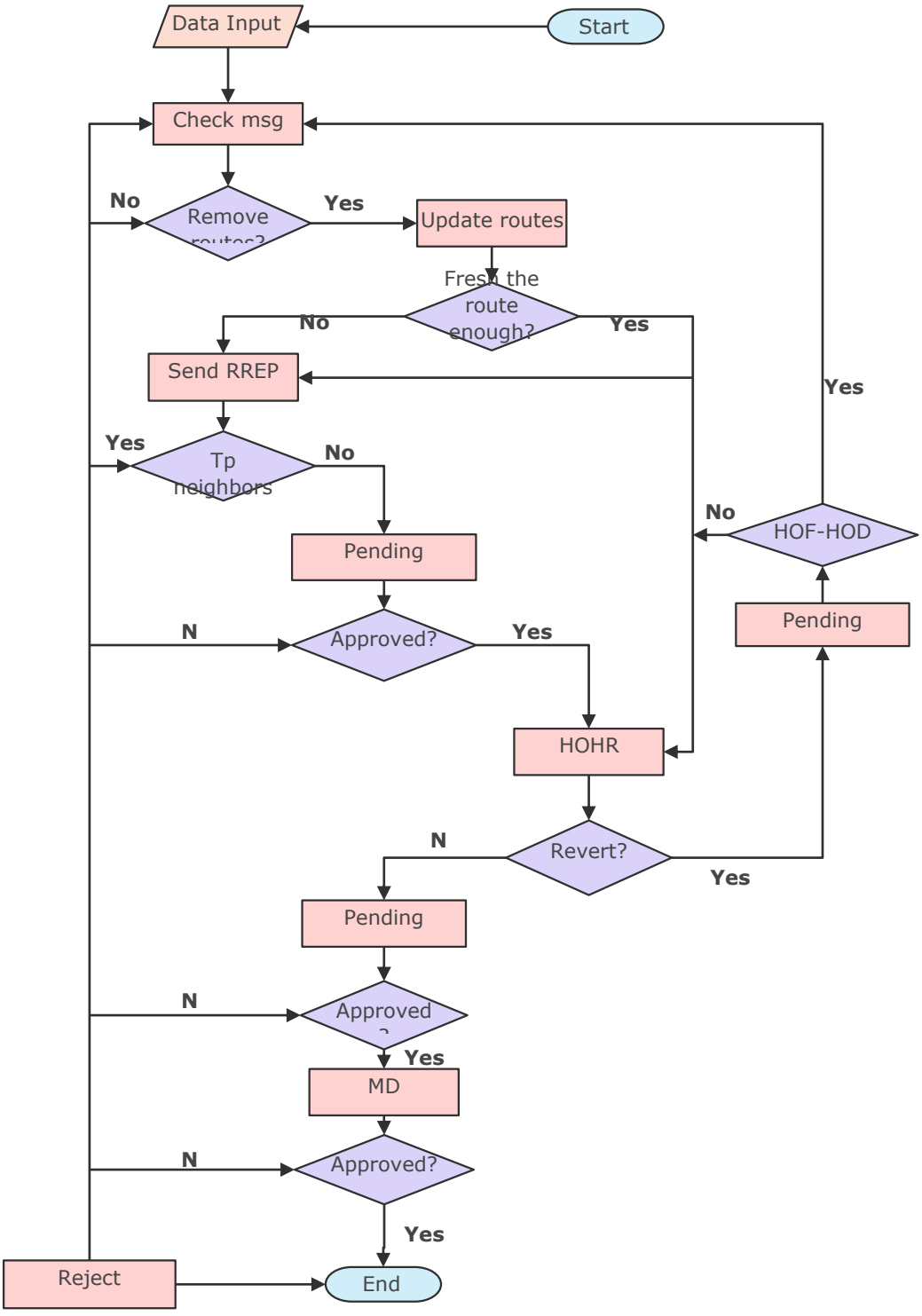

Figure 3: Flowchart of the Proposed Routing Algorithm

Doi: https://doi.org/10.54216/IJWAC.000103

The general Einstein Product is: $T(x,y) \leftarrow (x-y)/[1+(1-x)(1-y)]$ or $T(x,y) \leftarrow (x-y)/[2-(x+y-xy)]$ (1)

Where $x \in [0,1]$ and $y \in [0,1]$ are real number values. A function T is called a triangular norm (t-norm for short) if and only if it is commutative, associative, and monotonic [Zhang et al. 2018].

T normal function form argument is evaluated:

$$T(x_1, x_2, \dots, x_m) \leftarrow \frac{2m_{i=1}^{\infty} x_i}{\prod_{i=1}^{m}(2-x_i)+\|_{i=1}^{m} x_i} \quad (2)$$

Where $x_i \in [0,1]$ $(i = 1,2,\dots,m), T(x_1, x_2 \dots x_n) \leq \min(x_1, x_2 \dots x_n)$.

A T is a mapping T: $[0,1]^2 \rightarrow [0,1]$ having following properties:

- Commutativity: $T(x,y) = T(y,x)$
- Monotonicity: $T(x_1,y_1) \geq U(x_2,y_2)$ if $x_1 \geq x_2 and y_1 \geq y_2$
- Associativity: $\mathrm{T(x, T(y, z)) = T(T(x, y), z)}$

Calculate Consensus Trust Measurement using Einstein Product CT represents the consensus trust value. The CTij is measured using the Einstein Product, as shown in equation (7). Moreover, the consideration of ImD maximizes the consistency degree.

$$CT_{ij} \leftarrow \frac{2\Pi_{j=1}^{m}(ImD_j * DT_{ij})}{\Pi_{j=1}^{m}\left(2-(ImD_j * DT_{ij})+\Pi_{j=1}^{m}(ImD_j * DT_{ij})\right)} \quad (3)$$

Example:-From the above example and fig 3, bode 6 determines the consensus treat on node 5 ty conessua trust equation.

$$\mathrm{CT(6,5)} = 2(0.1852^{*}0.86^{*}0.1807^{*}0.90^{*}0.2033^{*}0.62^{*}0.178^{*}0.95)/(2-0.1852^{*}0.85)(2-0.1807^{*}0.9)(2-0.2033^{*}0.62)$$
$$(0.1852^{*}0.85^{*}0.1807^{*}0.90^{*}0.2033^{*}0.62^{*}0.178^{*}0.95)$$
$$= 0.0010913/(11.61+0.000645) = 0.000005992$$

Calculate Overall Trust Mesurment:-In Equation (4), OT represents the overall trust value.

$$OT_{ij} \leftarrow \left([1-(\mathrm{Com})^{-1}]DT_{ij} + [1-(1-(\mathrm{Com})^{-1})]CT_{ij}\right) \quad (4)$$

A route with a high level of credibility is chosen by going via a node with a similar level of credibility. As a result of taking into account both benefit and cost metrics in the trust assessment, it lessens the effect that black hole attacks have on the efficiency of the routing. Therefore, the discrete and consensus-based trust assessment used in MANETs helps to increase communication security without negatively impacting the performance of the routing.

In a similar manner, the OT value on nodes 1 and 13 is determined. Node 13, which is part of this group, has a high trust value. Therefore, the second option in 5.2 will be used to route the data. In addition, less trust is placed in node 5 among the others. Therefore, the RREP initiator of node 8 is being looked at as a possible suspicious node. With the help of the CREDIT technique, the MANET is able to correctly transmit the data packets to their intended location.

4. Experimental Analysis

An understanding of the functionality of protocols may be gained by performance analysis, which provides this understanding. In order to develop a protocol and have a better understanding of the numerous performance factors, this is helpful. In the next part, an in-depth performance study of a malicious AODV node has been carried out making use of a variety of different tests. The first test will examine what happens when the number of nodes that are immobile is changed.

Doi: https://doi.org/10.54216/IJWAC.000103

The simulation of MANETs has been run with anything from ten to one hundred times the normal number of nodes for this test. The pace of the nodes is 10 meters per second, and the pause duration is 30 seconds. The behavior of the AODV routing protocol, while it is being attacked with a changing number of nodes, is shown in both the figure and the table. PDR is impacted as a result of an increase in the number of nodes, as shown in figure 4. It demonstrates that if the number of nodes is less than 40, the PDR of the AODV that is being attacked is extremely bad. It is possible that this is due to a disruption in the network's connection somewhere. The results also demonstrate that there is a minuscule difference in terms of the PDR between a sinkhole attack and a blackhole assault. As part of the scenario, the adversaries will send the bogus route reply message. This false route reply message is intended to persuade other neighboring nodes in the network that it has the quickest route and the best route for a destination, as well as that a destination is located only the next hop from the attacker. After all of the nearby nodes have listened to this bogus route reply message, they have concluded that it must have originated from a real node.

As a result, they have updated their routing database to include the malicious node as their next hop on the way to their destination. After making the necessary changes to their routes, the nodes are now prepared to send their messages through an attacker node. When a data message is sent to a Blackhole node, the node immediately discards the message. As a result, the destination nodes are unable to receive packets.

Based on these findings, it seems that the network's packet delivery ratio is being negatively affected. In a sinkhole attack, the rogue node will not drop any messages and will instead forward all of them. The data that is coming from the attacker is disregarded by the nearby node since it is coming from the attacker. Because the routing database of each neighboring node contains information indicating that the attacker node is only the next hop on the path to the target.

Only in a very small percentage of instances is the destination really present to the following hop that the attacker is using. In this particular scenario, the packet will be sent to its intended location. The majority of the time, the message cannot be delivered to its intended recipient. mainly due to the fact that the attacker has inserted false information into the routing table. There is a marginal difference in the effectiveness of the network when a sinkhole attack is used as opposed to a blackhole assault because of this reason. The graph reveals a more favorable outcome for the Sinkhole assault. In addition, the PDR of the AODV protocol is dramatically reduced when it is subjected to flooding, Rushing, or selfish Attack compared to the standard AODV protocol. Figure 4 shows that EED has dropped as a result of all attacks; however, Figure 4. shows that throughput has significantly decreased as a result of the black hole and sinkhole assaults in comparison to the other three attacks.

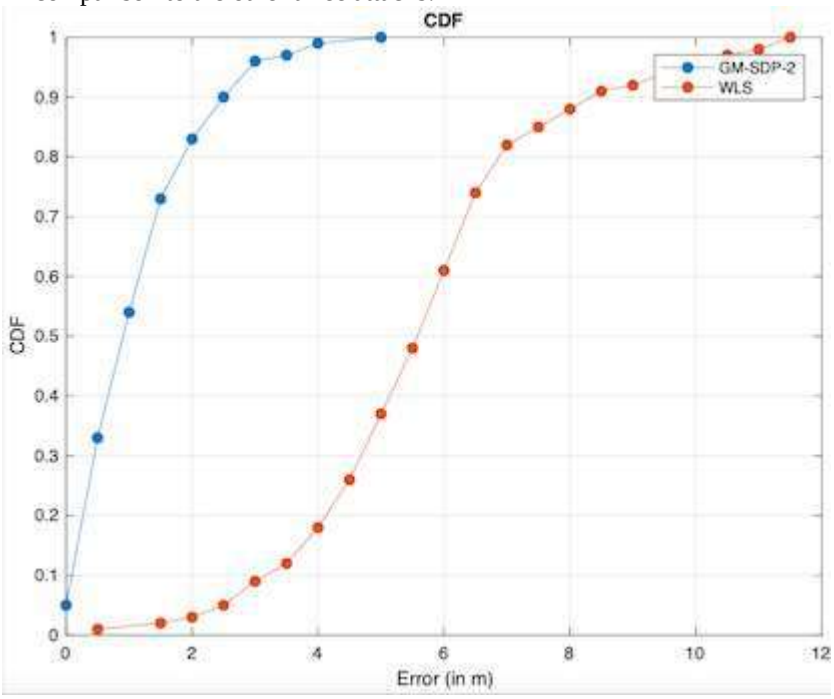

Figure 4: Varying No of Nodes.

Doi: https://doi.org/10.54216/IJWAC.000103

Test 2: Effect of Varying the Mobility of Nodes.

The simulation of normal AODV and AODV under attack was carried out by changing the speed from 0 meters per second to 30 meters per second and setting the pause time to 30 seconds. There were 100 normally mobile nodes that were randomly distributed throughout the network, and the performance matrix parameter was fixed. The simulation results are shown in figure 5 which shows that the PDR has fallen when subjected to a blackhole attack and a sinkhole assault, but that the PDR has remained almost equivalent when subjected to the other three attacks when compared to the standard AODV routing Protocol. In addition, the EED for the blackhole assault and the sinkhole attack is greater than the EED for the flooding attack, the selfish attack, and the rushing attack. From the results of the simulation, we can see that the flooding assault has caused the greatest amount of routing overhead. The flooding attack has raised the routing overhead in the network by flooding with Hello packets. Similar to the blackhole attack and the sinkhole attack, the increase in routing overhead caused by sending fake answers in response to a route request is caused by these attacks. As a result, the AODV protocol begins to act in an unexpected manner by producing extra routing packets. It should be noted that the routing overhead for selfish node assault, flooding attack, and rushing attack is comparable to that of standard AODV.
In conclusion, the simulation result shown in the image depicts the throughput of a network when subjected to a variety of assaults in turn. In a similar vein, both sinkhole and blackhole attacks have a significant impact on the packet delivery ratio as well as the throughput of the network. In addition to the effects of other assaults, flooding attacks can have a negative impact on throughput. This occurs as a result of the flooding of the media with hello packets, which makes the medium busy and prevents the transport of data packets. There is poor throughput in the network that has a high degree of density. This might be due to the fact that the high-density network has a large number of senders. The end result indicates that the assault caused by the black hole is a far more severe attack than previous attacks.

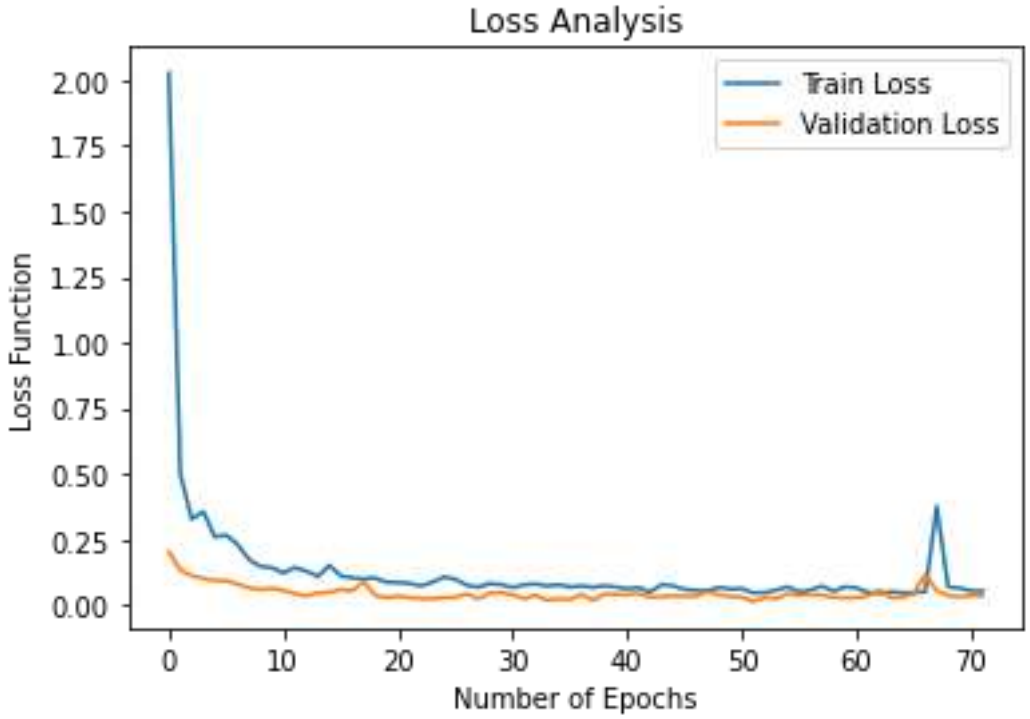

Figure 5: Effect of Varying the Mobility of Nodes

Test 3: Effect of Varying the Number No Attacker Nodes

The simulation has been run with varying numbers of attacker nodes in both attacks, ranging from one to five, with randomly distributed normal nodes set up to one hundred. The maximum speed was set at ten meters per second, and the pause time was set at ten seconds. This was done in a network environment with performance matrices parameters that were fixed. The decline in PDR% percentage and Throughput of AODV when it is under assault is shown in Figure 6 which shows that the number of malicious nodes has increased. In addition to this, the study indicates that the

Doi: https://doi.org/10.54216/IJWAC.000103

AODV routing protocol is more susceptible to blackhole attacks. Figure 6 on the other hand, shows that the EED of AODV under attack has grown in comparison to flooding Attacks whenever the number of malicious nodes increases.

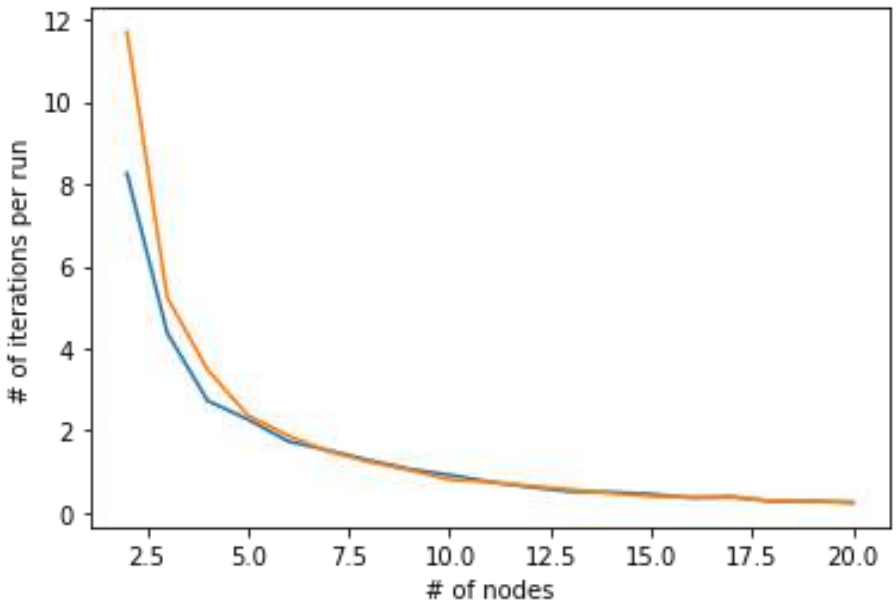

Figure 6: Effect of Varying the Number No Attacker Nodes

The quantity of control packets that are traded over the whole network is what is meant by the term "Overhead." Within the framework of the proposed approach, the mechanism for attack detection is carried out only by the watchdog node, and the exchanging of packets is confined to taking place locally between the appropriate neighbor nodes. When compared to the current system, which requires each node to watch the behavior of its respective neighbor nodes in order to identify any potential attacker nodes, which results in a greater amount of packets being sent between each node. In Figure 6.6, for an increasing number of nodes considering 25 and 100 nodes, the approximate difference in overhead between the proposed TWIST model and the existing DDPD scheme is 7 packets, and 15 packets, respectively. This is shown in comparison to Figure 6, which shows the overhead for only 10 nodes. As a result, the suggested TWIST method has a lower overall overhead compared to the DDPD system that is currently in use. There is a difference in the overhead of 21 packets between the suggested TWIST model and the present DDPD scheme when there are 50 nodes, and there is a difference of 30 packets when there are 75 nodes. As a result of this comparison, the TWIST approach that has been presented has a lower overhead than the system that is already in use.

6. Conclusion

Within the scope of this proposed work, we have conducted in-depth research on a variety of critical vulnerabilities and attacks. Based on the findings of the research, we have seen that MANET is experiencing a great deal of difficulty, most notably in the realm of security problems, for which there is no such reliable solution that can deal with the issue. Even the most fundamental routing protocols, such as AODV, DSDV, DSR, and TORA, lack the mechanisms necessary to keep a network safe. Both the problems with the network layer and the routing in the MANET require substantial attention. The network layer is not only vulnerable to traditional assaults, but it is also susceptible to MANET-specific attacks, which are notoriously difficult to defend against because of the open communication environment and the use of established protocols. It is recommended that such a routing mechanism be built since it should be able to ensure security while maintaining all of the attributes of MANET at the same time. A complete examination of the most demanding AODV protocol, while it was being attacked, has been done in addition to the discussion of security challenges and security remedies. Following an investigation into some of the most perilous assaults on AODV, such as the black hole, sinkhole, flooding, selfish attack, and rushed attack, at a number of different tests, we came to the conclusion that the performance of regular AODV had been diminished across the board. The results of the simulation showed that a selfish node attack or a rushing attack may be extremely successful if a malicious node is located between the source node and the destination node. This kind of attack also has the potential to

Doi: https://doi.org/10.54216/IJWAC.000103

bring the performance of the network down. Despite this, the impact of these two attacks will be significantly reduced if the malicious node is not located between the source and the destination. In addition, the findings indicate that the EED is greater during a blackhole assault and that the PDR of the network drops as a consequence. This is in contrast to the results of previous attacks. In addition, the blackhole attack and the sinkhole assault may have a significant negative impact on the performance of the network by transmitting false routing information in an effort to direct all of the network's traffic toward themselves. In conclusion, we came to the conclusion that the black hole attack has a more severe impact on the performance of the AODV protocol in the network.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Proceedings of ACM SIGCOMM 1994:234–244

[2] Cheng C, Riley R, Kumar SPR, Garcia-Luna-Aceves JJ (1989) A Loop-Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect. ACM SIGCOMM Computer Communications Review, Volume 19, Issue 4:224–236

[3] Murthy S, Garcia-Luna-Aceves JJ (1996) An Efficient Routing Protocol for Wireless Networks. Mobile Networks and Applications, Volume 1, Issue 2:183–197 ISSN : 0975-3397711

[4] G.Vijaya Kumar et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713

[5] Humblet PA (1991) Another Adaptive Distributed Shortest-Path Algorithm. IEEE Transactions on Communications, Volume 39, Issue 6:995–1003

[6] Rajagopalan B, Faiman M (1991) A Responsive Distributed Shortest-Path Routing Algorithm Within Autonomous Systems. Journal of Internetworking Research and Experiment, Volume 2, Issue 1:51–69

[7] Chiang C-C, Wu H-K, Liu W, Gerla M (1997) Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. Proceedings of IEEE SICON:197–211

[8] Chen T-W, Gerla M (1998) Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks. Proceedings of IEEE ICC 1998:171–175

[9] Iwata A, Chiang C-C, Pei G, Gerla M, Chen T-W (1999) Scalable Routing Strategies for Ad Hoc Wireless Networks. IEEE Journal on Selected Areas in Communications, Volume 17, Issue 8:1369–1379

[10] Jao-Ng M, Lu I-T (1999) A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks. IEEE Journal on Selected Areas in Communications, Volume 17, Issue 8:1415–1425

[11] Pei G, Gerla M, Hong X (2000) LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Network with Group Mobility. First Annual Workshop on Mobile and Ad Hoc Networking and Computing 2000 (MobiHoc 2000):11–18

[12] Tsuchiya PF (1988) The Landmark Hierarchy: A New Hierarchy for Routing in Very Large Networks. Computer Communication Review, Volume 18, Issue 4:35–42

[13] Jacquet P, Mu¨ hlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) Optimized Link State Routing Protocol for Ad Hoc Networks. IEEE INMIC 2001:62–68

[14] Toh C-K (1996) A Novel Distributed Routing Protocol to Support Ad-Hoc Mobile Computing. Proceedings of the 1996 IEEE 15th Annual International Phoenix Conference on Computers and Communications:480–486

[15] Dube R, Rais CD, Wang K-Y, Tripathi SK (1997) Signal Stability-Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks. IEEE Personal Communications, Volume 4, Issue 1:36–45

[16] Park VD, Corson MS (1997) A highly adaptive distributed routing algorithm for mobile wireless networks. Proceedings of IEEE INFOCOM 1997, Volume 3:1405–1413

[17] Jiang M, Li J, Tay YC (1999) Cluster Based Routing Protocol (CBRP). IETF Draft, August 1999, available at http://tools.ietf.org/html/draft-ietf-manet-cbrp-spec-01. Accessed 21 February 2008

[18] Broch J, Johnson DB, Maltz DA (1999) The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. IETF Draft, October, 1999, available at http://tools.ietf.org/id/draft-ietf-manet-dsr-03.txt. Accessed 21 February 2008

Doi: https://doi.org/10.54216/IJWAC.000103

[19] Perkins CE, Royer EM, Chakeres ID (2003) Ad hoc On-Demand Distance Vector (AODV) Routing. IETF Draft, October, 2003, available at http://tools.ietf.org/html/draft-perkins-manet-aodvbis-00. Accessed 21 February 2008

[20] McDonald AB, Znati T (2000) A Dual-Hybrid Adaptive Routing Strategy for Wireless Ad-Hoc Networks. Proceedings of IEEE WCNC 2000, Volume 3:1125–1130 26.

[21] McDonald AB, Znati T (1999) A Mobility Based Framework for Adaptive Clustering in Wireless Ad-Hoc Networks. IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Volume 17, Issue 8:1466–1487

[22] Boppana RV, Konduru SP (2001) An Adaptive Distance Vector Routing Algorithm for Mobile, Ad Hoc Networks. Proceedings of IEEE INFOCOM 2001:1753–1762.

Doi: https://doi.org/10.54216/IJWAC.000103