iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48677

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

Wireless Ad Hoc Network Routing Protocols Performance Evaluation under Security Attack

Aabid Farooq[1], Jasdeep Singh[2]
[1]*M. Tech Scholar, Department of Computer Science Engineering, RIMT University, Mandi Gobindgarh Punjab, India*
[2]*Professor, Department of Computer Science Engineering, RIMT University, Mandi Gobindgarh Punjab, India*

Abstract:** A mobile ad hoc network is made up of portable wireless nodes (MANET). The communication between these mobile nodes is not managed centralized. A self-organizing, self-configuring network known as MANET allows mobile nodes to roam around at whim. The mobile nodes can act as a router by receiving and sending packets. Due to the significance of routing in MANET, this thesis also evaluates several routing systems' efficacy. We compared the three routing protocols AODV, DSR, OLSR, and DSDV. Throughput, network load, and latency are the three metrics used to gauge how well-performing different routing systems are. The three routing techniques are well described using metrics. Information is transmitted end-to-end and hop-by-hop over the connections to the destination nodes using the proactive and reactive protocols of MANET. In multi-hop mobile ad hoc networks, energy consumption at the mobile nodes' end and its effective use are crucial factors. Nodes and other routing resources in MANETs cannot afford to run out of battery power while carrying out mission-critical operations like military or rescue missions. The effectiveness of MANET protocols such AODV, DSDV, OLSR, and DSR is studied in this study. Throughput, packet delivery ratio, and energy use are included while computing the Mobile Ad-hoc Networks' performance parameters. The circumstances that were simulated using various simulators are included in the research. The related research compared the performance of several protocols in MANETs with varying node mobility, stop length, and node density while examining the NS-2 scenario. The optimum routing system for mobile ad hoc networks will be identified after a comparison and analysis of these protocols.

I. INTRODUCTION

In daily communication, wireless networks have remained a key component. It is frequently employed in industrial applications, personal area networks, and even military applications. Due to its many beneficial characteristics, including as ease of installation, dependability, cost, bandwidth, total necessary power, security, and network performance, it has become quite popular in a variety of applications. However, it also utilizes fixed infrastructures, much like wired networks [7], such as cordless phones, cellular networks, Wi-Fi, microwave communication, Wi-MAX, satellite communication, RADAR, etc.

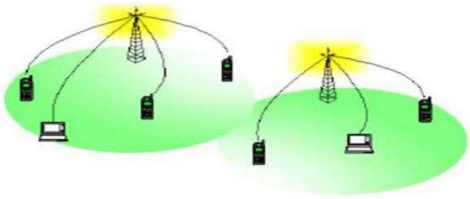


Figure 1 Infrastructure based wireless network

Due to the large population of independent mobile users, the demand for effective and dynamic communication in emergency/rescue operations, disaster relief efforts, and military networks, as well as for many applications, next-generation wireless ad-hoc networks are now widely employed [3], [2]. The network has a wide geographic coverage but has an unstable topology that can change abruptly..Because they are decentralized, these networks have more network scalability than infrastructure-based wireless networks. Ad-hoc networks perform better in crucial situations like natural catastrophes and military conflicts because they require little configuration and operate quickly [8], [4]. Depending on their intended use, ad hoc networks can be divided into three groups: wireless mesh networks (WMNs), wireless sensor networks, and mobile ad hoc networks (MANETs) (WSN). A MANET is a mobile node network that operates independently [4].

The typical effects of radio communication channels, many users' interference, multiple paths fading, shadowing, etc. are difficult for these nodes to handle.

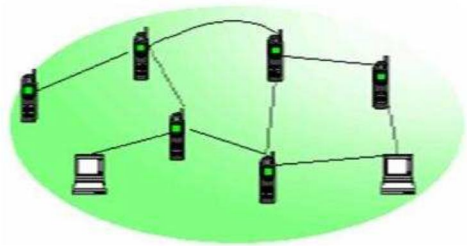


Figure 2 Mobile Ad-Hoc Network

It is quite difficult to create the best routing protocol for MANET. In these dynamic situations, it is crucial to develop an effective algorithm that will aid in determining the connectedness of network organizations, link scheduling, and routing [5]. The accuracy and success of the route computation determine how effective a routing algorithm is. In static networks, the shortest path algorithm is often an efficient method for determining the best route, however in a MANET environment, this straightforward notion is not necessarily true [21]..To choose a new route, several aspects must be taken into account, including extended power [3], wireless link quality, path losses, fading, interference, and topological changes [21]. To optimize any of these effects, networks should adjust their routing pathways adaptively based on circumstances at any time [18]. Any of these standards not being met may result in decreased network reliability and performance in MANETs. To maintain the standard of routing protocols, the Internet Engineering Task Force (IETF) - MANET working group is regularly developing new protocols. The functions of IP routing protocols that are appropriate for wireless routing applications in both static and dynamic topologies were specified by the working group [10].

To keep the routes current, these routing pathways are frequently announced inside the network. Destination Sequenced Distance Vector (DSDV) and Optimized Link State Routing Protocol are protocols that fall within the aforementioned category (OLSR). Reactive routing protocols set up source-to-destination routing pathways as needed. These routing techniques include Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV).

According to OLSR [3], each node has a routing table that details the routes to every other node in the network. Nodes publish their routing details, such as address, sequence number, and number of hops, in DSDV [4].

When data transmission is necessary in AODV [5] (RFC: 3561), the source node broadcasts a route request (RREQ) packet to its neighbors. Unicast Route reply (RREP) is provided to the source if the destination is located. A route error (RERR) packet is transmitted in the event of a failure to the source node. The reactive subset of routing protocols includes DSR [6]. While DSR employs a source routing technique where transmitted packets contain the whole path to the destination, it uses an AODV-like route discovery process. Each node in DSR stores a fresh route it discovers. Route caching speeds up the route search process, however the performance is also impacted by stale caches.Due to their dynamic topologies, constrained wireless connections, interference issues, lack of centralized management, and established infrastructure, MANETs are inherently unsafe.

Furthermore, security is frequently not given the proper care while designing MANETs routing protocols. This work offers a thorough analysis of the performance effects of security attacks on the four well-known MANET routing protocols (OLSR, DSDV, AODV, and DSR).

II. OBJECTIVES

The objective of this thesis work is:

1) To study proactive and reactive protocols
2) To analyse and compare the performance of both proactive and reactive protocols with and without black hole and grey hole attack.
3) To implement the scenarios using NS2 simulator.
4) To evaluate the performance in terms of Packet delivery ratio, End to end delay, normalised routing load and normalised throughput.

III. LITERATURE REVIEW

In the past ten years, there have been several research projects aimed at developing an effective routing protocol that is suited for MANET real-time network applications. Different routing systems employ various techniques to prevent routing loops. Routing may result in an infinite loop issue if the target node is not present in the network or if the link fails. Some protocols make use of the feasible distance, the DAG method, and the destination sequence number to guarantee loop-free routing.

While TORA utilises a link reversal algorithm and AODV uses a sequence number for each destination, DSR uses the source route to eliminate loops..The two elements that directly affect the routing efficiency are the routing loop and the preservation of full reachability [7]. With regard to packet delivery ratio and end-to-end latency in the Random Waypoint mobility model, AODV protocol outperforms DSDV and TORA. AODV also exhibits higher throughput than DSDV, TORA, and DSR protocols in high mobile node situations [4]. The performance of the routing protocols OLSR, AODV, DSR, and TORA is examined using OPNET modeller 14.5 for varied network sizes, node mobility, and traffic loads [5], [11].

IV. METHODOLOGY

A. Routing protocols

For wireless ad hoc networks, there are several varieties of routing protocols. Reactive or proactive routing protocols are the two categories under which these protocols fall [8]. The ad hoc routing techniques known as hybrid routing protocols provide both proactive and reactive benefits. Reactive or on-demand routing protocol is the name of the first type of protocol. Routing protocols that are proactive or table-driven fall under this category. Reactive MANET Protocol is the name of the first type of protocol (RMP). Only when the source node wants to communicate with the other node can communication take place in these protocols. Nodes with high levels of mobility or nodes that only sometimes send data are best suited for reactive MANET protocols. We'll take a look at a few reactive routing techniques.

Proactive MANET Protocol is the name of the sec kind of protocol (PMP). Active network layout detection is done via proactive routing protocols. Every node can retain a routing table, which can be used to identify a route more quickly. The proactive routing protocols offer minimal latency for route decision-making and strong dependability on the present network topology [14].

B. Reactive Routing Protocols

Reactive routing systems are sometimes known as on-demand routing protocols since they build routes when they are required. Sending route requests across the network will enable you to obtain these routes. This algorithm's disadvantage is that it has a large latency when scanning a network. In this thesis report, we will discuss AODV and DSR, and the simulation analysis will be provided in the fifth section of the study..

1) AODV (Ad hoc On-demand Distance Vector)

An on-demand routing protocol is AODV. A simple method for changing the connection state is provided by the AODV algorithm. For instance, only the network nodes that are directly impacted by a connection failure receive alerts. All routes through this impacted node are cancelled as a result of this message. It creates unicast routes from source to destination, which accounts for the low network utilization. Because routes are created based on demand, network traffic is minimal. AODV forbids retaining excess routing that is not in use. [21].

In an ad hoc network, AODV is in charge of enabling two nodes to develop a multi hop route if they choose to join. AODV avoids counting to infinity by using Destination Sequence Numbers (DSN), which is why it is loop-free. This is what makes this algorithm unique. A node provides its DSNs and all routing information when it makes a request to a destination. Based on the sequence number [10], it also chooses the best path. Route Request (RREQs), Route Replies (RREPs), and Route Errors are the three AODV messages (RERRs) [1]. These messages find and maintain the source-to-destination path using UDP (user datagram protocol) packets. For instance, the node making the request will use its IP address as the message's originator IP address. It simply implies that not all messages were routed by the AODV automatically. The Time-To-Live (TTL) in the IP header controls how many hops routing messages go in an ad hoc network. The requesting node broadcasts an RREQ message throughout the network whenever the source node wishes to establish a new route to the destination [9]. Figure 3.2 below illustrates how this information will be utilized to create a reverse routing for RREP messages coming from the destination node. The dotted orange line, representing the shortest route from destination B to source A, shows how the destination node B responds with an RREP message. The request's original author received the RREP. Only by unicasting an RREP back to the source is this route accessible. From the RREQ's originator to each node, the nodes that are receiving these messages are cached. An RERR message is issued when a link fails. The RERR notification gives details about unreachable nodes. The IP addresses of each node that is the following hop before reaching the destination. The table contains all of the network's routing information. There are four route entries in the routing table: the destination IP address, the destination sequence number (DSN), the valid destination sequence number flag, and the other state and routing flags (e.g., valid, invalid, repairable being repaired) Network interface (v) and Hop Count (vi) (number of hops needed to reach destination) the lifespan list of antecedents, and (viii) the next hop (Expiration time of the route).

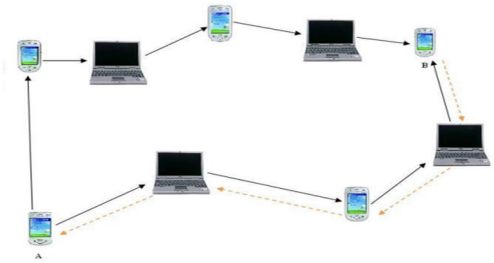


Figure 1 RREQ and RREP messages in MANET using AODV

2) DSR (Dynamic Source Routing)

On demand routing protocol, also known as Dynamic Source Routing Technology, is a reactive routing protocol. Because it is a source routing protocol, it is both straightforward and effective. It is applicable to wireless ad hoc networks with several hops [22]. The DSR network completely manages its own configuration and organization. Just two mechanisms—route discovery and maintenance—make up the protocols. For the benefit of fresh, simple routes that become available, the DSR changes its route cache often. The node will divert the packet to that route if any newly discovered available routes were discovered. The direction of the travel must be known to the packet. As a result, the packet was configured with route information to go from sender.

To prevent recurring discoveries that it has the capacity to determine its path in this manner, this information was maintained in the packet. DSR operates via two fundamental mechanisms: route discovery and route maintenance. Route request (RREQ) and route reply are the two messages used in route discovery (RREP). A node broadcasts the RREQ packet throughout the network whenever it wants to transmit a message to a particular recipient. After receiving this RREQ message and adding their own addresses, the neighbor nodes in the broadcast range rebroadcast it throughout the network..

The RREQ will not be broadcasted over the whole network if a route is identified in that node's route cache. As a result, it will transmit the RREQ message to the target node. The first communication that arrived at its target included complete routing information. That node will transmit an RREP packet with complete route information to the sender. The RREQ packet is thought to have chosen this path since it is the shortest. The source node may now begin routing packets since it has all the necessary information about the route in its route cache. The method of route finding is shown in Figure 3-3. Here, there are four nodes: A, B, C, and D. Node A serves as the source, while node D serves as the destination.

Node A will first check its route cache to see whether it has a direct path to node D before sending a data packet there. Node A will send an RREQ message throughout the network if it lacks a direct path to node D. The RREQ message will be received by neighbor node B. To see if it has a direct path to the target node D, node B will first check its route cache. If it does, it will proceed. Consequently, an RREP message will be sent to source node A... The source node A will begin transmitting data packets (DP) along the identified route in response to that message. If it was unable to find the path from node B to node D, it sent the message RREQ to the following node C and cached the route AB. Until the RREQ message reaches destination node D, the procedure continues. The destination node D sends an RREP message to the source node A after caching the routes AB, BC, and CD in its memory.

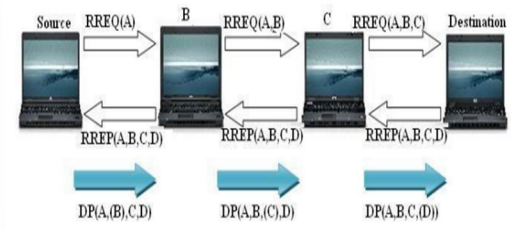


Figure 2 Route discovery procedure in MANET using DSR

Figure 3-4 displays the four nodes A, B, C, and D. Destination node D receives a message from node A. While receiving the ACK message up to node B, the transmission continues up to node C. If node C sends an RREQ message to node D but does not get an ACK message back from node D. The node C is aware that the transmission is having an issue. So, the source node A receives an RRER message from node C. It then looks for a different path to the final target node D. Figure 3-4: MANET's route maintenance process utilizing DSR

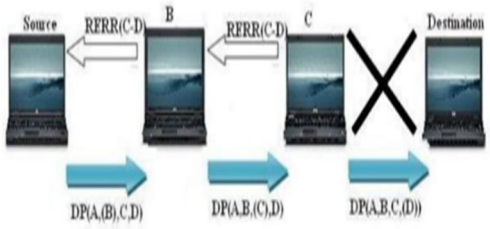


Figure3 Route maintenance procedure in MANET using DS

Routing Protocols that Are Active Proactive protocols construct and maintain the routing information for each node. Whether or not the route is required has no impact on the proactive routing protocols [20]. Control messages are sent out at regular intervals. Even in the absence of data flow, control messages are still sent. Proactive routing methods are ineffective at using bandwidth because of these control messages. The use of proactive routing techniques has both benefits and drawbacks. One of its benefits is that it makes it simple for nodes to initiate a session and obtain routing information. The drawbacks include excessive data retention by nodes for route management and a sluggish recovery time after a particular connection breakdown.

C. OLSR (Optimized Link State Routing)

Because it continuously keeps and updates its routing table, this proactive routing system is also known as a table-driven protocol. In order to offer a route if necessary, OLSR keeps track of the routing table. Any ad hoc network is able to use OLSR. OLSR is referred to as a proactive routing protocol due to its characteristics. In figure 3-5, multipoint relay (MPR) nodes are displayed. The route packets are not transmitted by every node in the network. Route packets are only broadcast by Multipoint Relay (MPR) nodes..These MPR nodes can be chosen from the source node's neighbors. A list of MPR nodes is maintained by every node in the network. This MPR selector was discovered through the exchange of HELLO packets between nearby nodes. Before any source node plans to transmit a message to a particular destination, these routes are constructed. Every node in the network maintains its own routing table. This is the reason why OLSR has less routing overhead than other reactive routing techniques and offers the network's quickest path to the target. Building additional routes is not necessary since the already used route does not add significant routing overhead. The route finding latency is decreased.

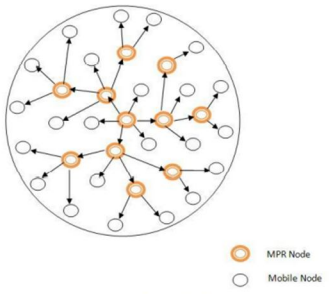


Figure. 4 MPR node sends the TC message

Network nodes communicate with one another by sending HELLO messages. In OLSR, these signals are transmitted at regular intervals to ascertain the connection status. Figure 3-6 helps us to comprehend this. If nodes A and B are neighbors, node A notifies node B with a HELLO message. We can infer that the connection is asymmetrical if B node gets this message. If B node now transmits the identical HELLO message to A node. This is the first example, sometimes known as an asymmetric relationship. Now, if two-way communication is available, we may refer to it as a symmetric link, as seen in Figure 3-6 below. All of the neighbor information is contained in the HELLO messages.As a result, the mobile node can have a database with data on all of its multiple hop neighbors. When symmetric connections are created, a node selects the smallest possible number of MPR nodes. At specified TC intervals, it transmitted topology control (TC) messages including connection status information [20]. The routing tables are likewise calculated using TC messages. Information about MPR nodes is also provided in TC messages.

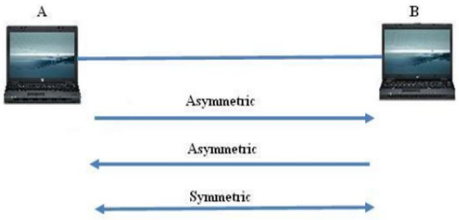


Figure 5 HELLO messages in MANET using OLSR

D. The DSDV protocol

One of the earliest protocols created for ad hoc networks is the (Dynamic Destination - Sequenced Distance -Vector Routing Protocol) [11]. To calculate the pathways, DSDV uses the Billman-Ford (DBF: Distributed Bellman- Ford) method. Each node notifies its surrounding nodes of all possible destinations that may be reached using a metric, which is the number of hops. It has a sequence number (SN) to distinguish between old and new highways..The updating of the routing table can either be limited to modified entries or complete reception of all table neighbours (which necessitates sending several data packets per table) (in provided they are not too many). Two issues—routing loops and counting to infinity—are resolved by the DSDV. However, the pace of update dissemination is still quite sluggish. The usage of out-of-date table entries is the major cause of mobility for large losses.

E. Security Attacks in MANETs

In MANETs, there are two different kinds of security threats: active attacks and passive attacks. In active attacks, a malicious node assumes the identity of a reliable node inside the network and publishes false routing information as a part of the active route, such as a shorter travel time to the target or a higher sequence number. In passive attacks, the attacker simply listens to the dialogue that is already taking place on the network rather than directly participating in it.

The goal is to get the precise information from the data rather than altering it or discarding packets. In this study, we looked at how two recent attacks—the Black-hole and Gray-hole—affect the operation of MANET routing protocols. Black-hole Attack: In this type of attack, a malicious node lures traffic into the network by asserting that it has the highest sequence number and the fastest path to the target before dropping each packet that is passed via it [8, 9].

In a gray-hole attack, the malicious node wants to partially reject packets that are either going somewhere specific or are of a specific traffic type [10]. Because of this, when dealing with general traffic kinds, the malicious node acts properly. However, as soon as packets are of a specific type or are travelling to a specific place, they are lost.

V. EXPERIMENTAL ANALYSIS

Simply said, Network Simulator (Version 2), sometimes referred to as NS2, is an event-driven simulation tool that has been successful in helping researchers better understand the dynamic nature of communication networks. Using NS2, it is possible to simulate both wired and wireless network operations and protocols (such as routing algorithms, TCP, and UDP). Generally speaking, NS2 gives users a mechanism to define these network protocols and simulate the related behaviour.

Object-oriented Tool Command Language and C++ are the two main languages used in NS2 (OTcl). While the fundamental workings (i.e., a backend) of the simulation objects are defined by the C++, the simulation is built up by the OTcl by putting the objects together, configuring them, and scheduling discrete events (i.e., a frontend). TclCL is used to link the OTcl and C++ together. Variables in the OTcl domains are frequently referred to as handles when mapped to a C++ object. [17]

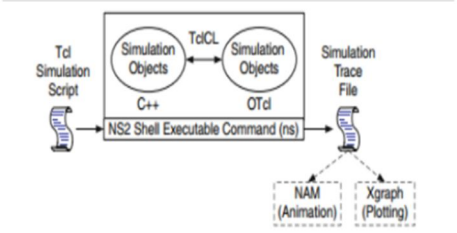


Figure 8 NS Architecture

After simulation, NS2 delivers simulation results as either text or animation. NAM (Network Animator) and XGraph are two examples of tools that are used to understand these results graphically and interactively. Users can extract a pertinent portion of text-based data and modify it into a more plausible presentation to investigate a certain network activity. Additionally, the simulator already includes a variety of scheduling tools, management rules queues, and transmission systems (layer 1 of the TCP/IP architecture) for studies on congestion control. The categories for the key components that are currently offered in NS

A. Parameters under study

1) Packet delivery Ratio: The packet delivery ratio (PDR) measures how many packets a traffic source transmits to how many packets a traffic destination receives. It assesses both the accuracy and effectiveness of ad hoc routing protocols by measuring the loss rate as perceived by transport protocols. In any network, a high packet delivery ratio is needed.

2) Average End-to-End delay: The average amount of time a packet spends moving across the network is known as the packet end-to-end delay. It is measured in seconds and covers the period of time from the sender's packet creation to the destination's application layer. Therefore, encompasses all network delays caused by routing operations, MAC control exchanges, buffer queues, transmission times, etc. Utilizing the NS-2 simulator, this work has evaluated routing strategies quantitatively. Under the simulation configuration presented in Table 1, we have examined the performance of four well-known routing protocols (a) OLSR, (b) DSDV, (c) AODV, and (d) DSR for the following performance metrics. The ratio of data packets transmitted from the source to those received at the destination is known as the packet delivery ratio (PDR).

3) *End-to-end delay typical:* It is the typical amount of time needed to send a data packet from source to destination. Routing load normalized (NRL): It refers to the quantity of routing packets sent with each data packet.

Table 1 Values and parameters used in simulation

Parameters	Values	Parameters	Values
Pause Time	20s, 40s, 60s, 80s, 100s	Packet Size	512bytes
Data Rate	4 kbps to 32 kbps	Scenario Size	1000m x 1000m
Mobility Speed	1-15m/s	Simulation Time	600s
Number of Nodes	50	MAC Protocol	802.11
No of Sources	10	Mobility Model	Random Waypoint
Transmitter Range	250m	Attack Type	Gray-hole, Black-hole
Bandwidth	11Mbps	No of Malicious Nodes	10%
Traffic	CBR over UDP	Protocols	AODV,DSR, DSDV, OLSR

Performance Assessment It has been done to analyze the performance of the routing protocols in the MANET for different node pause times and data rates. Additionally, we evaluated and contrasted the performance of these well-known MANET routing algorithms in three different situations: (a) without assault (when the network is not under security attack); (b) under gray-hole attack; and (c) under black-hole attack.

VI. SIMULATION AND RESULTS

A. Packet Delivery Ratio (PDR)

Our simulation findings demonstrated that at different pause times, PDR of the routing algorithms we considered performed well (data rate set to 16kbps). The PDR of AODV and OLSR is higher than that of the other two routing systems. Additionally, the proactive route maintenance of OLSR and the route request and response mechanism of AODV allow both protocols to function well in high mobility environments (or low pause time). Due to its intricate routing table maintenance at each node, PDR of DSDV is the least considered protocol. The PDR of all routing protocols decreases under a gray-hole attack, as shown in Fig. 5.1(a). OLSR and DSR are less susceptible to assaults than AODV. The PDR of all the procedures substantially decreases under black-hole assault, as can also be shown in Fig. 1(b).

Our findings demonstrate that OLSR outperforms other routing protocols in terms of PDR when under attack because OLSR uses an election-based routing structure that reduces the likelihood of hostile nodes being included in the active route. In terms of PDR, AODV and OLSR perform better than every other procedure. DSR functions admirably for low data rates, but PDR declines as data rates rise. Under high data rates, DSR experiences stale route cache entries at each node, which fills up data queues and leads to packet drops. Although DSDV is not greatly impacted by data rate, it has a lower PDR than other routing methods.

Figures 5, 2(a), and 5.2(b) demonstrate that OLSR outperforms all other routing protocols under assault in terms of PDR. Additionally, Fig. 5 2(b) demonstrates how PDR for all taken-in routing protocols dramatically declines under the black-hole assault. The causes of these actions are the same as those that have already been examined in relation to Figures 9 (a) and 9 (b).

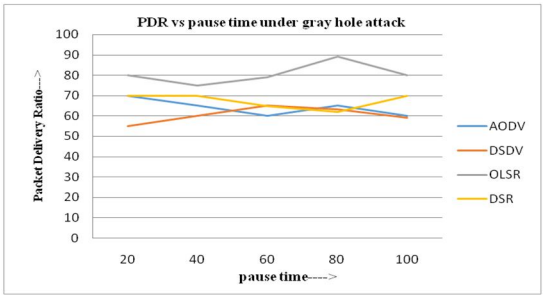


Figure 9(a) PDR vs. pause time under gray-hole attack

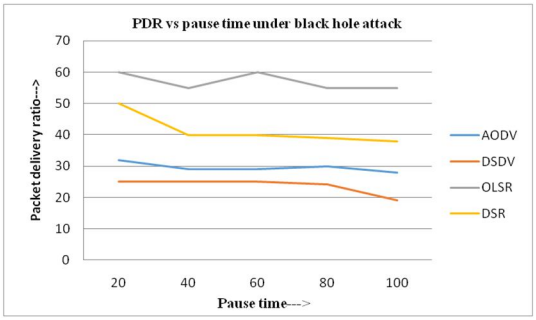


Figure 9(b) PDR vs. pause time under black-hole

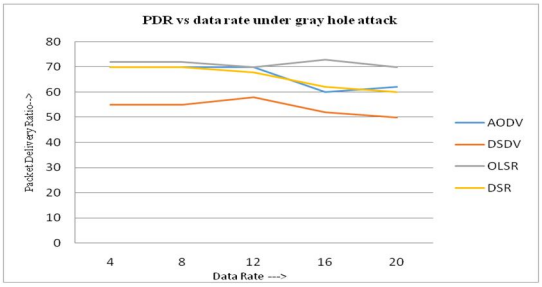


Figure 10 (a) PDR vs. data rate under gray-hole attack

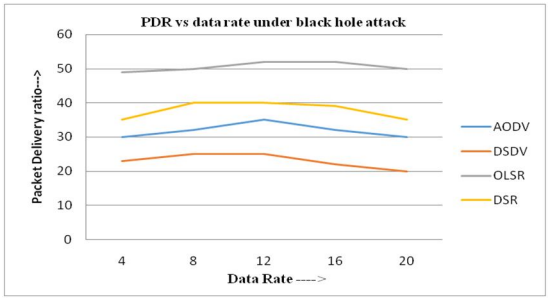


Figure 10(b) PDR vs. data rate under black-hole

B. Average End-to-End Delay

The end-to-end latency of all routing protocols decreases under gray-hole and black-hole assaults, as shown in Fig. 11(a) and 11(b). This is because there is a significant likelihood that there will be a rogue node along the path that will drop the packet when the hop count between the source and destination pair is high. The average end-to-end hop count thus declines, which finally results in a decrease in end-to-end latency. End-to-end latency is greater in the event of gray-hole attack than blackhole assault because the latter results in more packet drops, which shortens end-to-end pathways and reduces end-to-end delay. DSR is a reactive protocol, which means that it has a significant end-to-end latency, as shown by Figs..As a result, when a data packet arrives at a node, it searches for a route and takes longer than other packets. In addition, OLSR has a longer delay than AODV and DSDV. In reality, this is not the case; rather, AODV and DSDV both have low packet delivery ratios when compared to OLSR, which leads to minimal latency due to the lower end-to-end hop count. The average end-to-end distance between the source and the destination is enormous due to OLSR's increased packet delivery ratio, which causes a high end-to-end latency.

The average end-to-end latency for different data speeds is shown in Fig. 11. In comparison to other routing protocols, it can be seen that DSR has the largest average end-to-end latency for the same reason as was mentioned in relation to Fig 9. The average end-to-end latency of all three methods is seen in Fig. 11 to grow when the data flow is increased. The source of this rise in end-to-end latency for all four routing systems is high data rate congestion.

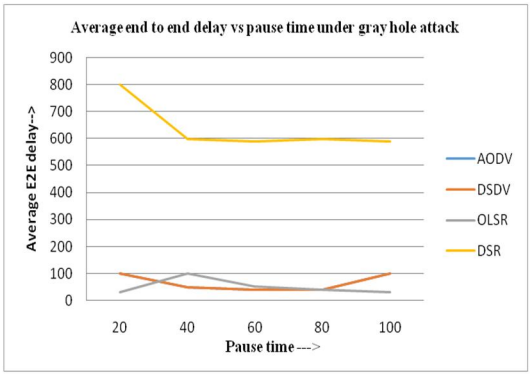


Figure 11(a) Average end-to-end delay vs. pause time under gray-hole attack

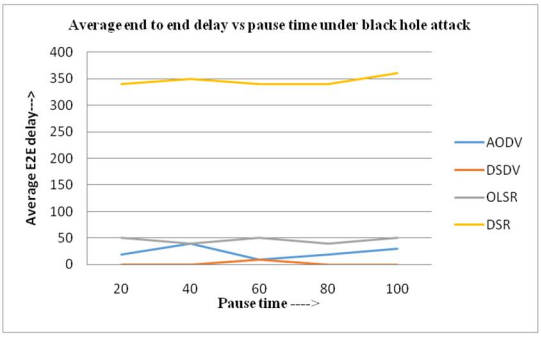


Figure 11(b) Average end to end delay vs. pause time under black-hole attack

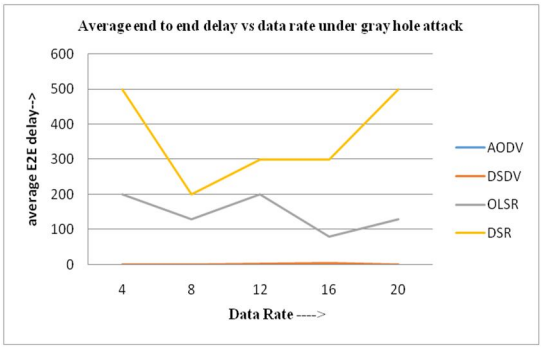


Figure 12 (a) Average end-to-end delay vs. data rate under gray-hole attack

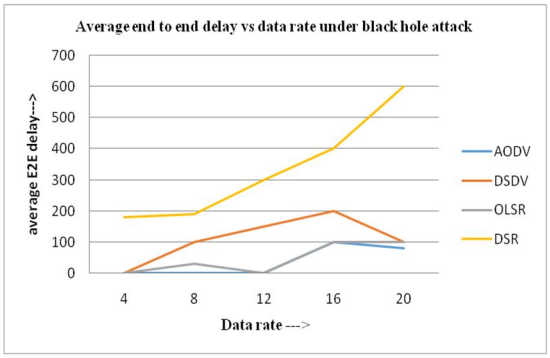


Figure 12 (b) Average end-to end delay vs. data rate under black-hole attack

C. Normalized Routing Load (NRL)

Figures12 (a) and 12 (b) depict NRL with varied pause times. In the absence of an attack, OLSR and DSDV have greater NRLs than the other two routing protocols. This is due to the frequent interchange of routing and control packets across nodes, as well as the occasional recalculation of MPR nodes, particularly during connection modifications. High routing load in DSR is caused by source routing and a large number of stale route caches at each node. Due to the irregularities in route answers, AODV's routing burden is a little high.NRL is smaller than the case of no attack under gray-hole and black-hole assault, as indicated in Fig. 13(a) and 13 (b). This is because malevolent nodes swiftly reply to route requests and discard a sig
nificant number of packets, which lowers the routing traffic in that network. Fig. 6 displays NRL for various data rates.

When compared to other low data rate protocols, OLSR's NRL is quite high since nodes send less data packets relative to a lot more routing packets (proactive nature of the routing protocol). The same is true for DSDV, where NRL diminishes as data rate rises.

In contrast, NRL for reactive methods is low for low data rate and rises as data rate increases. Figures 14(a) and 14(b) show that, in the presence of assaults, NRL falls for all procedures for the reasons mentioned in relation to Figure 5.

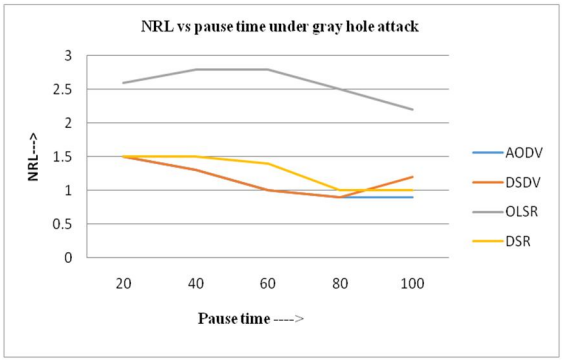


Figure 13 NRL vs. pause time under gray-hole attack

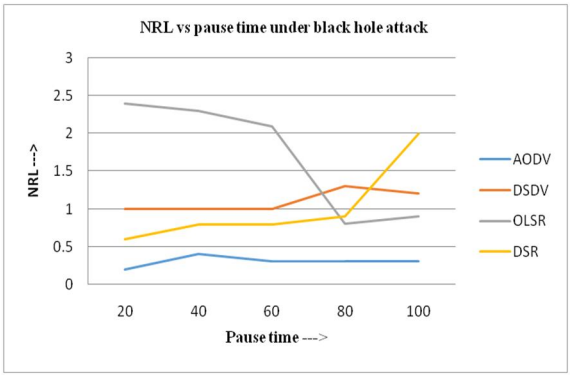


Figure 13(b) NRL vs. pause under black-hole attack.

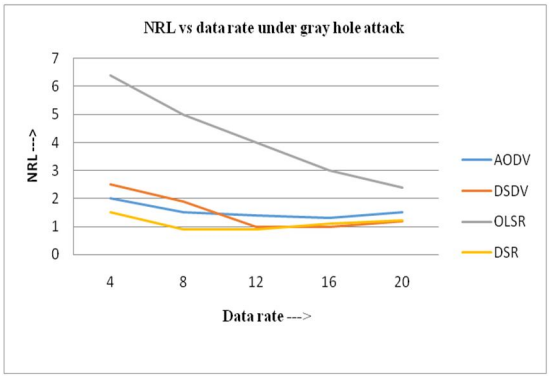


Figure 14 (a) NRL vs. data rate under gray-hole attack

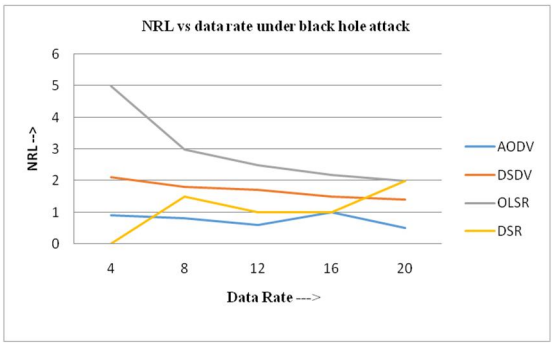


Figure 14 (b) NRL vs. data rate under black-hole attack

D. Throughput

is defined as the total number of packets delivered over the total simulation time. statistical computation shows that we do not reject the null hypothesis. That is, there is no significant difference for the different methods in terms of throughput performance (P − value > 0.05). This means that the results variations between the different algorithms are quite close. We stipulate that the small variations between the results are due to the network topology and traffic. The data sending rate of all the algorithms is set to a constant value for all the simulations. If most of the data traffic is between two nearby nodes (one-hop), the three algorithms would not differ significantly in terms of throughput.

Table 2 Summary of throughput for all the protocols

Groups	Count	Sum	Average	Variance
AODV	33	13193522.78	399803.7206	21230449877
DSR	33	11855083	359244.9394	8906585753
DSDV	33	11916653.61	361110.7155	26727816402
OLSR	33	12166744.32	346446.885	2322335938

Table 3 Analysis of throughput

Source of Variation	SS	df	MS	F	$P-value$	F_{crit}
Between Groups	34602089584	2	17301044792	0.9127	0.4048	3.0911
Within Groups	$1.81968E+12$	96	18954950677			
Total	$1.85428E+12$	98				

In this case, Fcrit = 3.0911 at α = 0.05. Since F = 0.9127 < 3.0911, the result are significant at the 5% significance level. So we will accept the null hypothesis, and conclusion can be drawn that there is strong evidence that the expected values in the three groups does not differ. The variation is quite small and can be eliminated at this significance level. The P −value for this test is 0.4048.

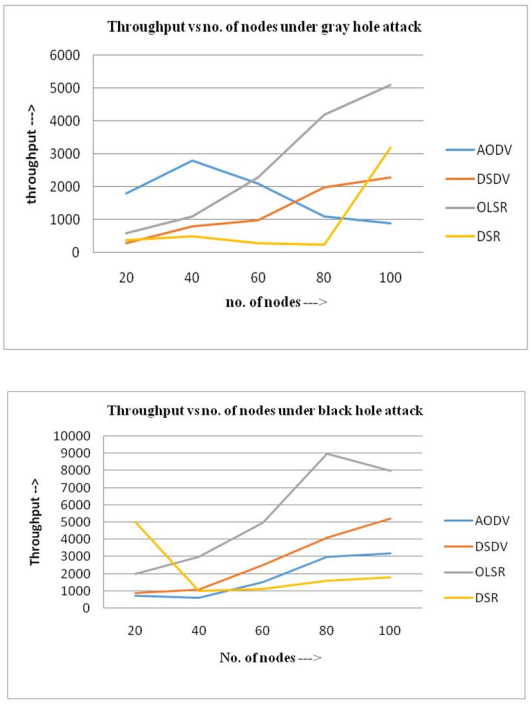


Figure 15 Comparison of throughput in both type of attack

E. Comparative Analysis of MANET Routing Protocols

Table 3 summarizes our conclusions about four routing methods we took into consideration (OLSR, DSDV, AODV, and DSR). In terms of packet delivery ratio under fluctuating mobility and data rate without assaults, AODV outperforms other routing methods. In contrast to other routing protocols, it has been found that AODV is more susceptible to security threats. DSR works better than other protocols, but only when there is little movement and little data flow. With a slightly greater average end-to-end latency and better NRL performance in an attack scenario, OLSR surpasses other routing protocols that have been taken into consideration. Furthermore, OLSR performs almost as well as AODV in the absence of an assault, although it has a little larger NRL than AODV. Comparatively speaking, DSDV has a lower PDR than other routing protocols. Additionally, it performs poorly when the node mobility and data rate are high.

Table 3 Comparative Analysis of MANET Routing Protocols

Routing Protocols	Attack	Packet Delivery Ratio	Average End to End	NRL	Throughput (kbps)
AODV	Black hole	30	0	0.5	1500
	Grey Hole	60	0	1.50	2100
DSR	Black hole	40	300	1	200
	Grey Hole	65	200	0.9	1000
OLSR	Black hole	80	29	3	5000
	Grey Hole	55	130	4	4000
DSDV	Black hole	25	100	1.1	1100
	Grey Hole	60	90	1.5	1000

VII. CONCLUSION

The four well-known routing protocols (OLSR, DSDV, AODV, and DSR) have all had their performance thoroughly analysed in this work.

Each of these well-known protocols has been shown to have merits and downsides while the network is operating normally (without an attack), making it impossible to single out one protocol as the best. However, none of the routing protocols under consideration were created with security in mind.

As a result, procedures that were most effective in no-attack settings do not perform as well while under attack.

This highlights the need of considering security issues while designing a routing protocol for MANETs.

In this work All of these protocols were analyzed and compared and the performance of both was examined over blackhole and greyhole attacks

NS2 simulator was used for implementation

The performance parameters into consideration were packet delivery ratio, end to end delay, Normalized routing load and normalized throughput.

It was observed that OLSR performs best in even being under attack.

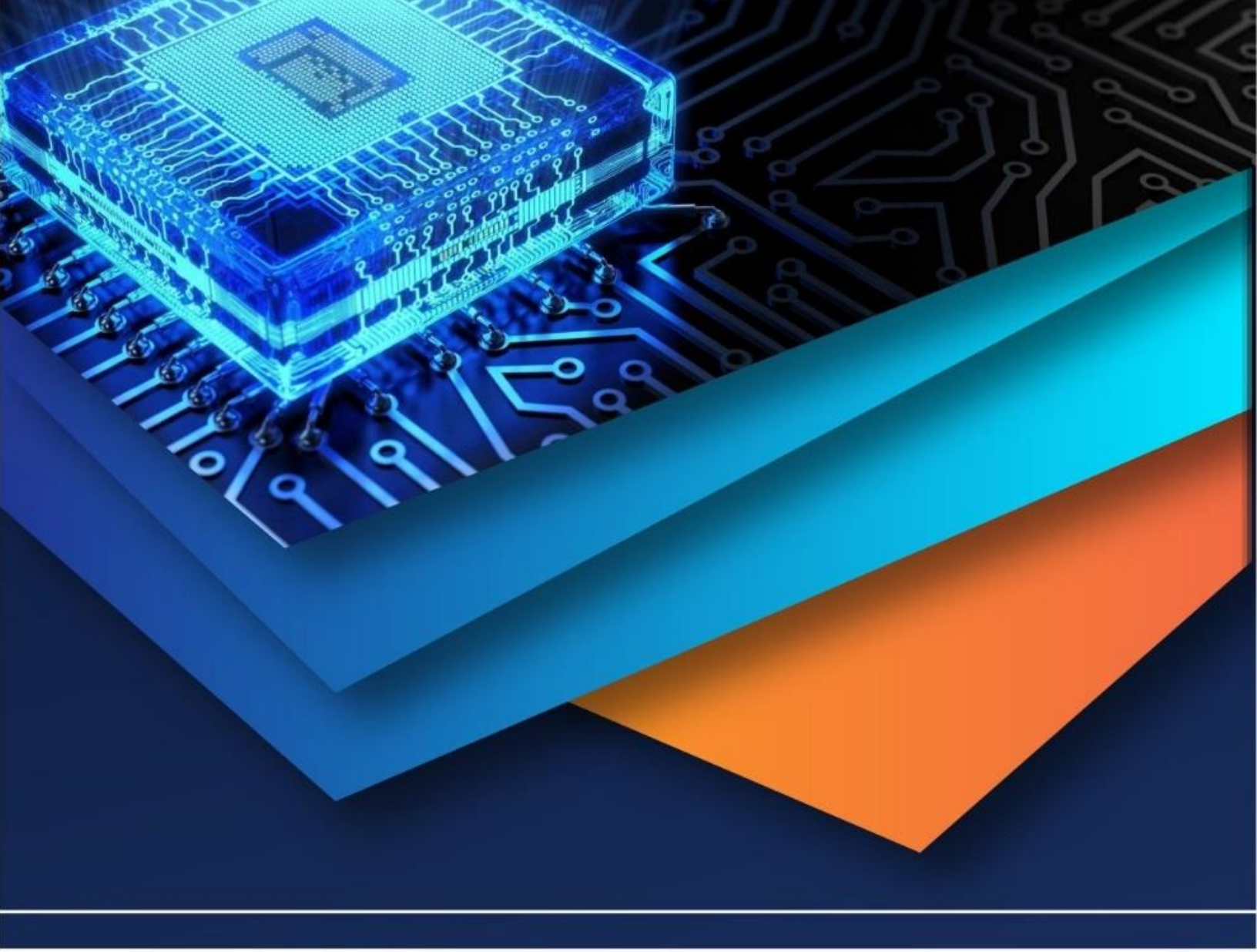
Additionally, there is a need for a general security framework that existing protocols may utilize to isolate hostile nodes from the routing path and reduce the effect of their actions.

A. Future Scope

Future work is about the development of modified version of the selected routing protocols, which should consider different aspects of routing protocols such as rate of higher route establishment with less route breakage and the weakness of the protocols mentioned should be improvised.

REFERENCES

[1] A.B. Malany, V.R.S. Dhulipala, RM. Chandrasekaran, “Throughput and Delay Comparison of MANET Routing Protocols” Intl. Journal Open Problems Comp. Math., Vol. 2, No. 3, Sep 2009.
[2] D.O. Jörg, “Performance Comparison of MANET Routing Protocols In Different Network Sizes” Comp. Science Project, Institute of Comp. Science and Networks and Distr ibuted Sys, University of Berne, Switzer land, 2003. [Online]. at:
[3] S. Ali, and A. Ali, “Performance Analysis of AODV, DSR and OLSR in MANET”, Masters Thesis, M.10:04, COM/School of Computing, BTH, 2010. [Online]. Available at:
[4] M.K. J. Kumara and R.S. Rajesh, “Performance Analysis of MANET Routing Protocols in different Mobility Models” IJCSNS International Journal of Computer Science and Network 22 Security, VOL.9 No.2, February2009.
[5] N Vetrivelan, and A.V. Reddy, “Performance Analysis of Three Routing Protocols for Varying MANET Size” Proceedings of International M. Conference of Eng. & Computer Scientists, Hong Kong, Vol. II IMECS 2008.
[6] W. G. LOL, “An Investigation of the Impact of Routing Protocols on MANETs using Simulation Modeling” Master Thesis, School of Computing and Mathematical Science, Auckland university of Technology, 2008. [Online]. Available at:
[7] A. K. Pandey, and H. Fujinoki, “Study of MANET routing protocols by GloMoSim simulator” Intl of network management NT, Wiley InterScience 15: 393–410, Intl. Journal Network Management 2005.
[8] S. Mittal, and P. Kaur, “Performance Comparison of AODV, DSR and ZRP Routing Protocols in MANET'S” Intl. Conf. on Adv. in Comp., Control, and Telecom. Technologies, Trivandrum, Kerala, India, 28-29, December, 2009.
[9] X. Hong, K. Xu, M. Gerla, “Scalable Routing Protocols for Mobile Ad-Hoc Networks” IEEE Network Magazine, Vol.16, Issue-4, page(s) 11– 21. Online]. Available at:
[10] [Online]. Available at: http://www.ietf.org/html.charters/manet-charter.html. [Accessed]: Feb.20, 2010. 53
[11] A. Shrestha, and F. Tekiner, “Investigation of MANET routing protocols for mobility and scalability” Int. Conference on Parallel and Distributed Computing, Applications and Technologies, Higashi Hiroshima, 2009.
[12] [Online]. Available at: http://tools.ietf.org/id/draft-ietf-manet-zone zrp-04.txt. [Accessed]: March 03, 2010.
[13] Z. J. Haas, and M.R. Pearlman “The performance of Query Control Schemes for the Zone Routing Protocol” IEEE/ACM transactions on networking, Vol. 9, No. 4, August 2001.
[14] J. Schauman “Analysis of the Zone Routing Protocol” Technical report, December, 2002. [Online]. Available at:
[15] A. Buhan, and M. Othman, “Efficient Query Propagation by Adaptive Bordercast Operation in Dense Ad-Hoc Network”, IJCSNS International Journal of Computer Science and Net. Security, VOL. 7, No. 8, Aug. 2007



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY