1-1-2012

Preventing Collaborative Blackhole Attacks on Mobile Ad Hoc Networks

Rajender D. Peddi
Ryerson University

PREVENTING COLLABORATIVE BLACKHOLE ATTACKS ON MOBILE AD HOC NETWORKS

by

Rajender Dheeraj Peddi

B.E., Osmania University, Hyderabad, India, 2010

A Thesis

Presented to Ryerson University

in partial fulfilment of the

requirements for the degree of

Master of Science

in the Program of Computer Science

Toronto, Ontario, Canada, 2012

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research

I further authorize Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my thesis may be made electronically available to the public.

Abstract

Preventing Collaborative Blackhole Attacks on Mobile Ad Hoc Networks

Master of Science
Computer Science
Ryerson University

This thesis proposes two protocols for addressing collaborative blackhole attacks in MANETs, referred to as the Detecting Blackhole Attack-Dynamic Source Routing(DBA-DSR) and Detecting Collaborative Blackhole Attack (DCBA) algorithms. The DBA-DSR protocol uses fake Route request packets to attract the malicious nodes before the actual routing process. The DCBA protocol uses our so-called suspicious value, which is based on the abnormal difference between the routing messages transmitted through a node, to identify the malicious nodes. In later stage, if the destination node detects significant loss in data packets, the initial detecting mechanism will be triggered again to identify malicious nodes. Simulation results are provided, showing significant improvement over the DSR protocol, as well as the Baited blackhole DSR protocol(chosen as a benchmark scheme), in terms of performance metrics such as packet delivery ratio, network throughput, average-end-to-end delay and routing overhead.

Acknowledgement

Foremost, I would like to express my sincere gratitude to my supervisor Dr. Isaac Woungang, and my co-supervisor, Dr. Sanjay Kumar Dhurandher, for their continuous support, patience, motivation, enthusiasm and time throughout my graduate studies.Their guidance helped me in all the time of research and writing of this thesis. It was a great privilege to work with them.

Besides my supervisors, I would like to thank my thesis committee for taking the time and effort to review my work and provide me with their insightful comments.

I would also like to acknowledge all the faculty members and supporting staff members of the Department of Computer Science and the School of Graduate Studies at Ryerson University for their support in terms of financial aid and work experience as a graduate assistant.

I also thank the fellow graduate students for supporting me in different ways throughout my journey as a graduate student. Special thanks to my friends Vincent Koo , Sweeney Luis and Subir Biswas, for their continuous support throughout this journey and for all the fun we have had in the last two years.

I wish to thank my parents, Rajender Peddi and Sreedevi Peddi and my sister Vidhatri Peddi. Without them, I would not be here today. Their love provided my inspiration and was my driving force. I owe them everything and wish I could show them just how much I love and appreciate them. I would also like to thank all my friends back in India for their support and love.

Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

ACK	Acknowledgement
AODV	Ad Hoc On-Demand Vector
BDSR	Baited Blackhole Dynamic Source Routing
CBR	Constant Bit Rate
CRRT	Collect Route Reply Table
DBA	Detecting Blackhole Attack
DCBA	Detecting Collaborative Blackhole Attack
DPRAODV	Detection Prevention and Reactive Ad Hoc On-Demand Vector
DRI	Data Routing Information
DSR	Dynamic Source Routing
FRp	Further Reply
FREq	Further Request
GloMoSim	Global Mobile Information System Simulator
GPS	Global Positioning System
MANETs	Mobile Ad Hoc Networks
REAct	Resource-Efficient Accountability
RREP	Route Reply
RREQ	Route Request
SAODV	Secure Ad Hoc On-Demand Vector
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Chapter 1

Introduction

Wireless networks can be classified into infrastructure-based networks and infrastructure-less networks. Mobile ad hoc networks (MANETs) belong to this latter class, where a mobile node can act as both a host and a router while forwarding the packets to other mobile nodes. MANETs are very easy to deploy and are dynamic in nature, thus, they can be used in places where geographical constraints are present, such as in battlefields, disaster management situations, to name a few. Since the mobile nodes in MANETs communicate over a wireless channel, message security and transmission are a major concern. Routing protocols in MANETs such as Dynamic source routing (DSR), and Ad hoc On demand Distant Vector routing protocol (AODV) were designed without considering any security constraints in MANETs. Thus, AODV-based MANETs or DSR-based MANETs may be vulnerable to several distinct types of attacks, for instance blackhole attacks, wormhole attacks, Sybil attacks, to name a few [1][2]. A Blackhole attack [3] is an attack where the malicious node(referred to as blackhole node) present in the network attracts all the data packets using the fake routing information. When the packets reach this malicious node, they merely disappear.

1.1 Motivation

Wireless networking has gained a lot of attention in recent years. The recent developments in the field have led me to focus my learning on wireless networks. Integrity, confidentiality, and availability of data can only be assured if all the security issues have been addressed. Thus security in MANETs has been one of the main concerns for the normal functionality of the network. The lack of a centralized monitoring system and easy to access open wireless channel make MANETs vulnerable to different types of attacks.

Blackhole attack, also known as packet drop attack has been one of the main threats to MANETs where the malicious node can attract and drop the data packets in the network. When multiple attackers synchronize their efforts to harm the network cause intense damage to the network. Collaborative attacks are very complex, powerful and sophisticated. Thus dealing with these types of attacks is more challenging and interesting.

1.2 Research Problem

In recent years, wireless mobile ad hoc networks have gained a lot of importance in the field of wireless communications. Therefore, the need for securing these networks has been a huge challenge.

This thesis mainly focuses on securing the MANETs against collaborative blackhole attacks. Much research has been done to secure the MANETs from blackhole attacks, but only few of them have addressed the issue of collaborative blackhole attacks.

One of the simplest and possible solution [4] to mitigate blackhole attacks in the MANET is to disable the intermediate nodes from replying to the RREQ packets, so, only the destination node can reply to the RREQ packets. But, there are some disadvantages using this solution. First, the routing delay is greatly increased. Second, a malicious node can take further action such as fabricating a RREP packet on behalf of the destination node. The source node cannot determine if the reply message is really originated from the destination

node or has been fabricated by the malicious node. When the data packet transmitted by the source node reaches the malicious node, it drops the packets instead of forwarding them to the destination node creating a blackhole. Collaborative attacks may cause more devastating impacts on a network as more than one attacker coordinate with each other to harm the network. Thus, in this thesis, we proposed a method to avoid collaborative blackhole attack while addressing the above mentioned concerns.

1.3 Thesis Contributions

The contributions of this thesis are threefold:

1. We Analyzed the effect of single blackhole attack on MANETs through simulations.
2. We Proposed the DBA-DSR scheme, a proactive routing protocol to mitigate and avoid single blackhole attacks in MANETs and compare it against the DSR protocol through simulations.
3. We Proposed a novel scheme so-called DCBA scheme which merges the advantage of proactive and reactive scheme for DSR based MANETs to avoid collaborative blackhole attacks in MANETs.

1.4 Thesis Organization

The remainder of this thesis is organized as follows:

- **Chapter 2** describes some background information on MANETs and the DSR routing protocol. Some of the most recent related works on blackhole attacks are also discussed.
- **Chapter 3** presents a detailed description of the methodologies of our proposed DBA-DSR and DCBA protocols.

- **Chapter 4** presents our simulation results of the proposed DBA-DSR and DCBA protocols.
- **Chapter 5** concludes our work and highlights some future research on the studied topics.

Chapter 2

Background Research

2.1 Preliminaries

2.1.1 Mobile ad hoc networks

MANET is a group of mobile nodes where nodes communicate with each other over a wireless channel in a cooperative manner without any fixed infrastructure. Mobile nodes can act as both a host and a router while forwarding the packets to other mobile nodes. Figure. 2.1 and Figure. 2.2 are examples of a wireless network and a Mobile adhoc network. In a wireless network, mobile nodes communicate with each other through the routers where as in MANETs, mobile nodes communicate with each other without using any infrastructure.

Since mobile nodes in MANETs communicate over a wireless channel, message security and transmission are indeed a major concern. MANETs are vulnerable to several distinct types of attacks, including blackhole attacks, wormhole attacks, sybil attacks, Denial of Message (DoM) attacks, to name a few [5][6].

2.1.2 Blackhole Attack in MANETs

A blackhole attack is an attack where the malicious node (so-called blackhole node) can attract the data packets by using a forged Route reply packet to falsely claim that it has

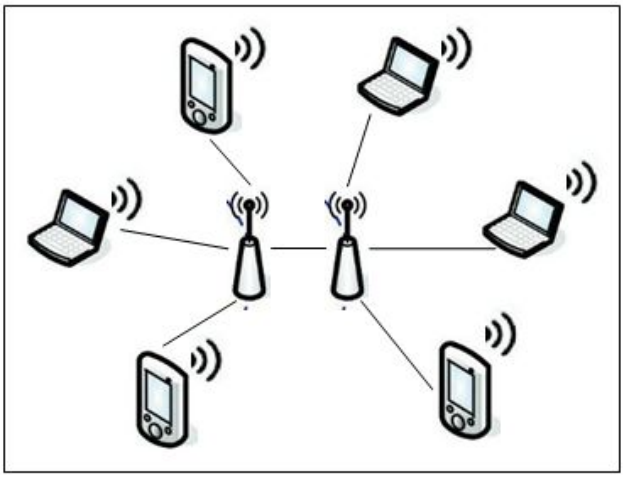

Figure 2.1: An Example of a wireless network

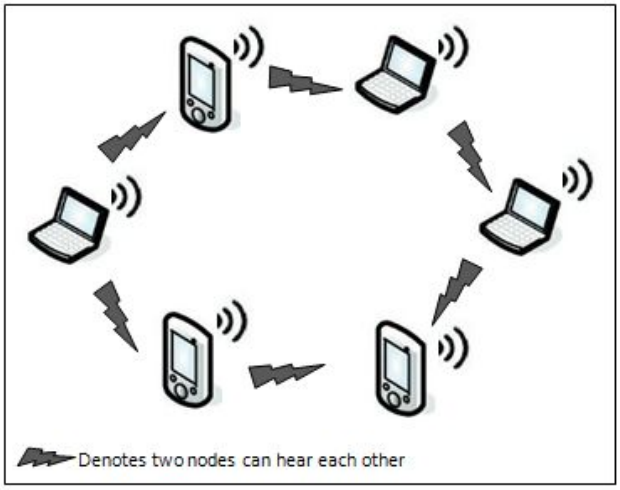

Figure 2.2: An Example of a MANET

a shortest route to the destination. When the packets reach the blackhole node, they are dropped. Blackhole attacks in MANETs can cause immense harm to the network. Examples of such harm include immense loss of packets and delay in the end-to-end transfer of data packets through the network.

A blackhole node has two fundamental properties. First, it takes advantage of the ad hoc routing protocol such as AODV or DSR to advertise itself as having a valid route to the destination node, even though the route is spurious, with the intention to intercept packets. Second, the blackhole node consumes the intercepted packets. As an example, let us consider the network depicted in Figure. 2.3, where in AODV or DSR protocol is used. In Figure. 2.3, whenever there is a need to transmit data, the source node S initiates a route discovery process by sending a RREQ packet. The malicious node M sends the RREP which contains the spoofed destination address, including the small hop count and a large sequence number. Now this route is used by the source node to send the data, and in this way, data will arrive at the malicious node. These data will then be dropped. In this way, the source and destination nodes will be in no position any more to communicate in the presence of the blackhole attack.

When two or more malicious nodes collaborate with each other, i.e. work as a group, the

damage can even be worse. This type of attack is known as collaborative blackhole attacks. For example, in Figure. 2.4, the malicious nodes M1 and M2 collaborate with each other in fabricating the RREP packet and send it to the source node. Upon receipt, the source node transmits the data packets using the fabricated information in the received RREP packet. Therefore, the data communication is initiated between the source towards the malicious node instead of the destination node. Thus, nodes M1 and M2 collectively work with each other in order to perform the collaborative blackhole attack in the MANET. Collaborative blackhole attacks are more dangerous than single blackhole attacks and can cause huge packet loss to the network.

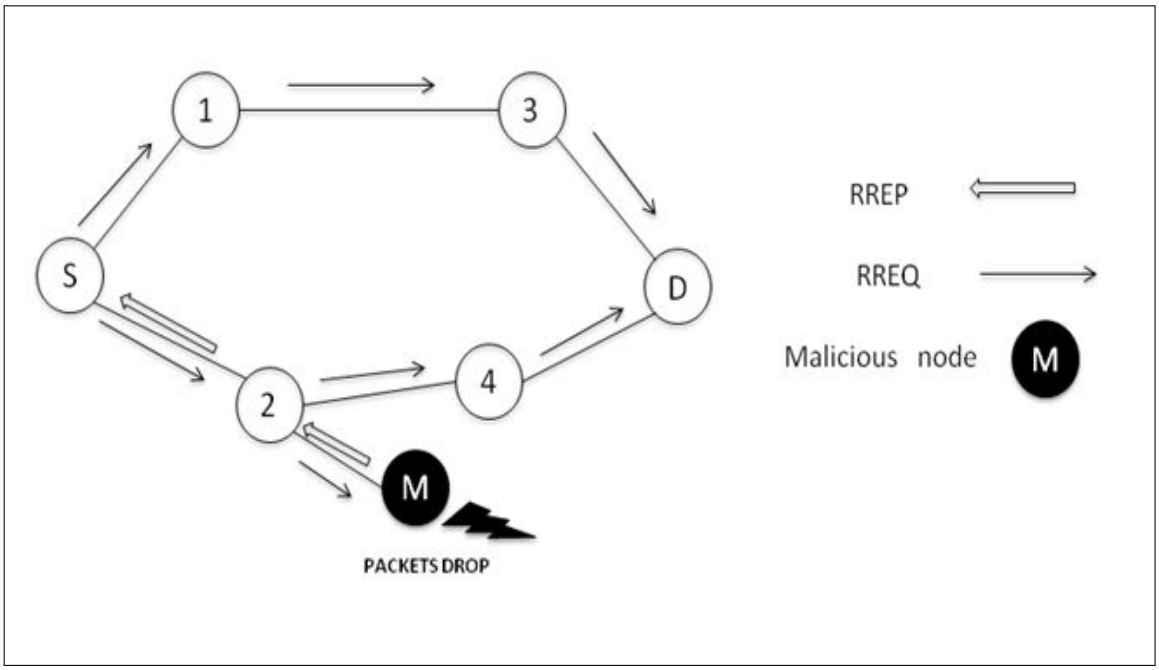

Figure 2.3: Example of single blackhole attack in MANET

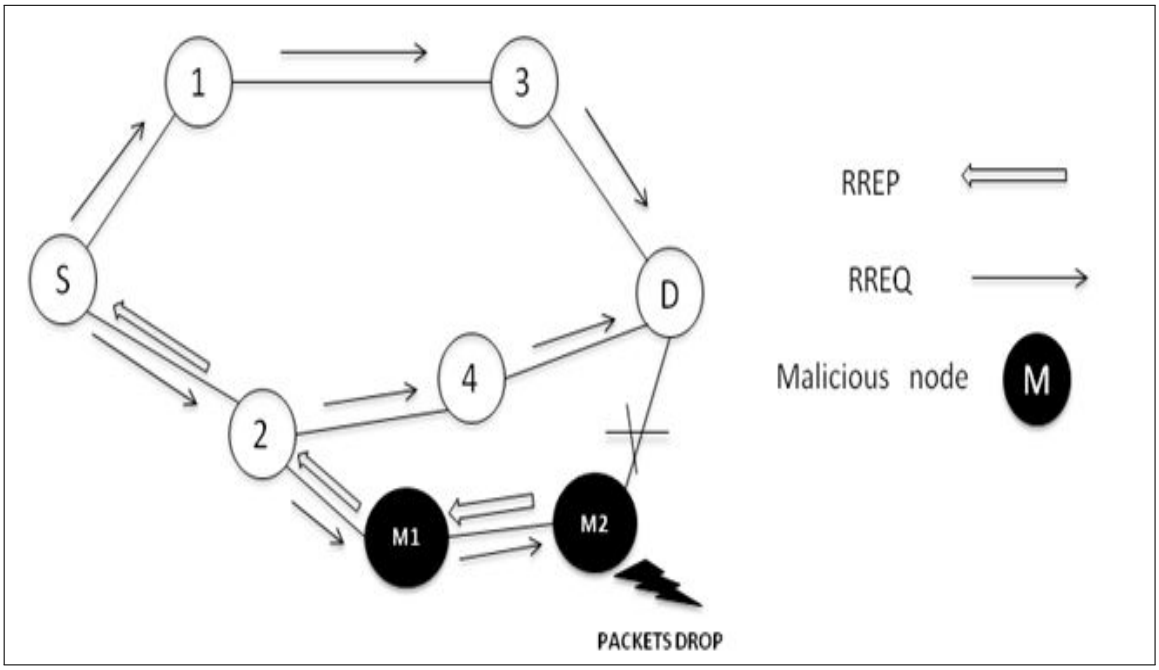

Figure 2.4: Example of collaborative blackhole attack in MANET

2.1.3 DSR Protocol

Routing protocols in MANETs can be classified in many ways. According to the routing strategy, these routing protocols can be categorized into Table-drive, On demand and Hybrid routing protocol[7, 8]. The DSR protocol[9] is typical example of On demand routing protocol for MANETs, which is simple, efficient and effective. It is a source routing protocol, which mainly consists of two processes: *Route discovery* and *Route maintenance*. In DSR, whenever the source node wants to send some data to the destination node, it initiates the route discovery process. In this process, the source node broadcasts the Route Request (RREQ) packet. All intermediate nodes which receive this RREQ packet check their routing table for the routing information to the destination node. If the intermediate node has the routing information to the destination, it replies with a Route Reply (RREP) packet to the source node. If no routing information is available in its routing table, the node simply forwards the packet to its available neighbour nodes, and so on. When the RREQ is forwarded to a node, the node adds its address information into the RREQ packet. That way, when the

destination node receives the RREQ, it can know all intermediate node's addresses along the route. The destination node can depend on the routing information among the packet to reply with the RREP to the source node and allow the source node to acquire the whole routing information on this route. On the other hand, route maintenance is the process maintained by the source node. When the network topology has changed or a connection failure has occurred, the source node is informed by means of a Route Error packet (RERR). In that case, the source node uses another available route to the destination to deliver the packets. This alternate route exists in the route cache or is discovered by restarting the Route Discovery process [10].

2.2 Related Work

Several works have been proposed in the literature, which deal with blackhole attacks in MANETs. A few recent representative ones are discussed as follows.

In [4] Deng et al. proposed a solution which asks every intermediate node to include the information on the next hop to destination in its route reply (RREP) packet when the intermediate node replies to the route request (RREQ) packet. While receiving the RREP, the source node does not transmit the data packets to the intermediate node immediately. Rather, based on the receiving information on the next hop, the source node sends a Futher-Request (FRq) to the next hop node to ask whether this node has a valid route to the destination. The source node receives a FutherReply (FRp) message from the next hop, which includes the check result. Whenever the source node receives the FRp message, it extracts the check result information from the FRp message. If the answer is yes, the route is built and the source node transmits the data. If the answer is no, the source node sends an Alarm Packet to alert other nodes in the network about that fact. However, this method has some drawbacks, namely (1) the process of checking the validity of RREP from an intermediate node through FRq and (2) FRp messages obviously lead to some overhead in the

network. These issues were not addressed by the authors [4]. Moreover, their proposed algorithm only addressed single blackhole attacks, and cannot mitigate cooperative blackhole attacks.

In [11], Ramaswamy et al extended the solution proposed in [4] for preventing cooperative blackhole attacks in MANETs. In their solution, each node maintains an additional table called Data Routing Information (DRI), which is used to identify the misbehaving nodes in the network. Whenever the intermediate node receives the RREQ packet, it replies with the RREP packet along with the node id of the next hop neighbour and the DRI entry for the next hop node to the source node. When the source node receives the RREP packet, it sends a FRq message to the next hop node. The next hop node in turn responds with the FRp message with the DRI entry for the intermediate node, the next hop node of the current next hop node, and the DRI entry for the next hop node of the current next hop node. If the next hope node is trusted, the source node checks whether the intermediate node is a blackhole node or not using the DRI entry of the intermediate node obtained from the next hop node. The same checking process is continued until the source node finds a trusted next hop node. Although by cross checking all the nodes, the blackhole attack can be prevented, the overhead caused by the FRq and FRp packets appeared to increase the end-to-end delay in the network.

In [12], Tamilselvan et al. proposed a solution for preventing blackhole attacks in MANETs based on the AODV protocol. In their solution, the source node waits till other node replies with the next hop details. When the source node receives the RREP packets, it records the sequence number along with the time the packet arrived in a collect route reply table (CRRT). After recording the route replies in the CRRT, it calculates the timeout value for each RREP based on the time the first RREP arrived, then it checks the CRRT for any repeated next hop nodes. The path with the repeated next hop node is considered to be safe. If there is no repeated next hop node in the CRRT, the algorithm chooses a random path from the CRRT. The main drawback of this solution is that if there are no repeated

next hop nodes in the CRRT, the risk of blackhole attack will be increased whenever the algorithm chooses a random path. In [13], the authors extended their above proposed solution to combat cooperative blackhole attacks. In this case, the Fidelity Table is used where each and every node in the MANET is assigned a fidelity level by which the reliability of the node is determined. The fidelity level of the node is based on the faithful participation of the node in the network routing operations. When the source node receives the RREP from the intermediate node, the fidelity level of the intermediate node and the next hop node are checked. In case the fidelity level of any node drops to 0, it is considered as a malicious node i.e. a blackhole and is eliminated.

In [14], Tsou et al. proposed a DSR based secure routing protocol called Baited-Blackhole DSR (BDSR) that can detect and avoid collaborative blackhole attacks in MANETs. In their approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node will be used (as the bait destination address) to bait malicious nodes to reply to the RREP message. Malicious nodes are thereby detected and prevented through a reverse tracing technique.

In [15], Marti et al. proposed a watchdog and pathrater scheme to detect malicious nodes present in a MANET. The watchdog method identifies the malicious nodes in the MANET by eavesdropping on the transmissions of the next hop node. Watchdog compares each overheard packet with the packets in the buffer, which contains the packets recently sent by a node. If there is a match between the packets, the node removes the packets from the buffer; otherwise it increments a failure tally for the neighbouring node. If a packet has remained in the buffer for longer than a certain timeout period. A node is identified as a malicious node if the tally exceeds a certain threshold bandwidth. In this situation, the source node is notified about this malicious node. The pathrater method then helps in finding the routes that do not contain those malicious nodes. In this scheme, each node keeps track of the trustworthiness rating of every known node. The pathrater chooses the shortest path if there are multiple paths to the destination. The main drawback of this method is

that it might not detect a malicious node in the presence of limited transmission power, false behaviour or partial dropping.

In [16], William et al. proposed a scheme (so-called REAct system) for detecting malicious nodes in MANETs. Their scheme is made of of three phases: audit, search and identification. The audit phase verifies the packets forwarded from the audit node to the destination node. The source node will choose an audit node to use bloom filter in order to generate a behavioural proof. The source node also uses bloom filter to produce a behavioural proof and compare it with against the proof produced by the bloom filter generated by the audit node. As a result of this comparison, the segment that has the malicious node is identified. However, this method has an oblivious drawback, i.e. it can identify the blackhole attack only after the damage has been done to the network.

In [17], Baadache et al. proposed a blackhole detection scheme for wireless ad hoc networks based on the principle of Merkle tree. However, their solution suffers from excessive computational routing overhead. Similarly in [18], Jain et al. introduced an algorithm for detecting and removing blackhole attacks in MANETs. Their technique consists in sending equal and small sized blocks of data and monitoring the flow of these data blocks independently at the neighborhood of both the source and destination nodes, with the goal to detect a chain of cooperative malicious nodes.

In [19], Anita et al. proposed a mechanism for detecting blackhole attacks in MANETs using a certificate based authentication method that can counter the effect of blackhole attack. They used certificate chaining for authenticating the nodes in the MANET. Their solution consists of two phases: certificate phase and authentication phase. Once the route has been established between the source and destination nodes, the nodes forming the route enter into the certification phase. The source node then identifies the next hop node and generates the public key then issues the public key certificate to the node that the source node is convinced of having the security parameters. The issued certificates have an expiry time, considered as a certain time interval. The source node transmits the data to the

destination node only if it receives the authenticated reply from the destination node. If the binding between the node and its key is found to be invalid, the issuing node revokes the certificate, and the node is considered to be malicious.

In [20], Lu et al. proposed a blackhole detection scheme (so-called Secure AODV) for MANETs that addressed some security weaknesses of AODV and avoid the blackhole attack. SAODV uses certain verification packets to verify the authenticity of the destination node directly by exchanging some random numbers. Whenever the source node receives a RREP packet, it immediately replies to the destination node with a verification packet secure RREQ packet which contains a random number generated by the source node. Upon receipt of secure RREQ packet, the destination node replies by a secure RREP packet that contains the random number generated by the destination node. In order to find the secure route, the source node then waits until it receives two or more secure RREP packets along two different paths with the same random number. However, this algorithm fails to identify the malicious nodes if it receives only one secure RREP packet. An enhanced version of the SAODV protocol was provided by Deswal and Singh in [21], where a password security was used for each routing node and routing tables were updated in a timeliness fashion.

In [22], Raj et al. proposed a scheme called DPRAODV to detect and isolate blackhole attacks in MANETs. In their approach, whenever the source node receives a RREP packet, the packet first checks the value of the sequence number in its routing table and does an additional check to find whether the RREQ sequence number is higher than a specified threshold value. This threshold value is dynamically updated at every predefined time interval. If the value of the RREP sequence is higher than the threshold value, that particular node is identified as blackhole node, which is blacklisted and an ALARM packet is sent to all other nodes in the network so that the RREP packet originated from that malicious node is discarded and the routing table for that node is not updated. The ALARM packet has the address of the malicious node as a parameter so that, the neighbours know that the RREP packet from the node is to be discarded. However, this algorithm suffers from excessive

overhead due to the fact the threshold value has to be updated at every time interval and special ALARM control packets should be handled.

In [23] Jaisankar et al. proposed a security approach to detect malicious blackhole nodes in MANETs. Their approach consists of two parts, detection and reaction. In their approach, before the source node sends the data packets, the leading RREP packet is examined between the intermediate node and the destination node. Every node in the network maintains a black identification table (BIT), which contains information about the number of packets received and sent through that particular node. A malicious node is then identified if the number of receiving packets differentiates from that of the sending packets. The second part of their approach is to isolate the blackhole node, thus each node maintains an isolation table (IT) and stores the black node ID. If a malicious node is found, the ID of this node is broadcasted to all other nodes in the network so that the malicious node is prevented from further participation in the routing operation. However, the proposed solution provides a higher packet delivery ratio than that observed in conventional schemes, with a little additional delay.

Most of the above-discussed solutions to avoid blackhole attacks in MANETs will fail when several nodes collaborate with each other to launch the attack. Thus, in the thesis, we address the issues concerning these attacks by proposing a DSR based protocol is to mitigate collaborative blackhole attacks in MANETs. Unlike other schemes for preventing blackhole attacks, in which the malicious nodes are identified only after the actual routing process started, in our solution, the blackhole nodes or collaborative blackhole nodes are identified before the actual routing process takes place.

Chapter 3

Methodologies

As discussed in Chapter 1 and Chapter 2, MANETs face various security threats such as attacks that are carried out against them to disrupt the normal operation of the networks. Among these threats, blackhole attack is a kind of attack which occurs in MANETs. In this chapter, we analyze the effects of blackhole attacks in MANETs and proposed some new solutions to mitigate them.

3.1 Single Blackhole Attack

3.1.1 Indroduction

To begin the study of collaborative blackhole attacks, we first investigated the effect of single blackhole attacks in MANETs. We develop a simple MANET scenario which is affected by a single blackhole attack. We use the GloMoSim simulator to create that scenario and measure the performance of the network under such attack. Simulation results are presented in chapter 4 that depict the effect of single blackhole attacks on MANETs based on predefined performance metrics.

3.1.2 Single Blackhole Attack Scenario

In this scenario, we simulate the blackhole attack in MANET. We use the Ad hoc on Demand Vector (AODV) routing protocol for this simulation. In blackhole attack, the malicious node advertises itself as having a shortest path to the destination node and drops all the received packets. The blackhole attack in AODV or DSR protocol can be summarized as follows:

1. The malicious node detects the active RREQ packet in the network and marks down the destination address.

2. The malicious node constructs a RREP packet with a fake route to the destination address. The sequence number is set to a highest value and the hop count is set to a lowest value.

3. The malicious node unicasts the RREP packet to the nearest neighbour or the source node directly.

4. The RREP packet received by the nearest neighbour relays the RREP packet towards the source node.

5. When the source node receives the RREP packet, it updates its routing table with the new information.

6. The source node starts sending the data packets using the fake information in the RREP packet.

7. When the malicious node receives the data packets, it simply drops them without forwarding the data packets to the destination node.

As an example, consider the blackhole attack scenario depicted in Figure. 3.1.

- The source node S needs to transmit data to the destination node D. It broadcasts the RREQ packets to all the neighbouring nodes.
- The malicious node M detects the RREQ packet and constructs the RREP packet with the fake routing information and unicasts the RREP packet to the neighbouring node **3**.
- The neighbouring node relays the RREP packet towards the source node S.
- The source node then updates its routing table with the fake information received through the RREP packet and transmits the data packets using the fake information.
- The malicious node M drops all the received data packets without forwarding them to the destination node D.

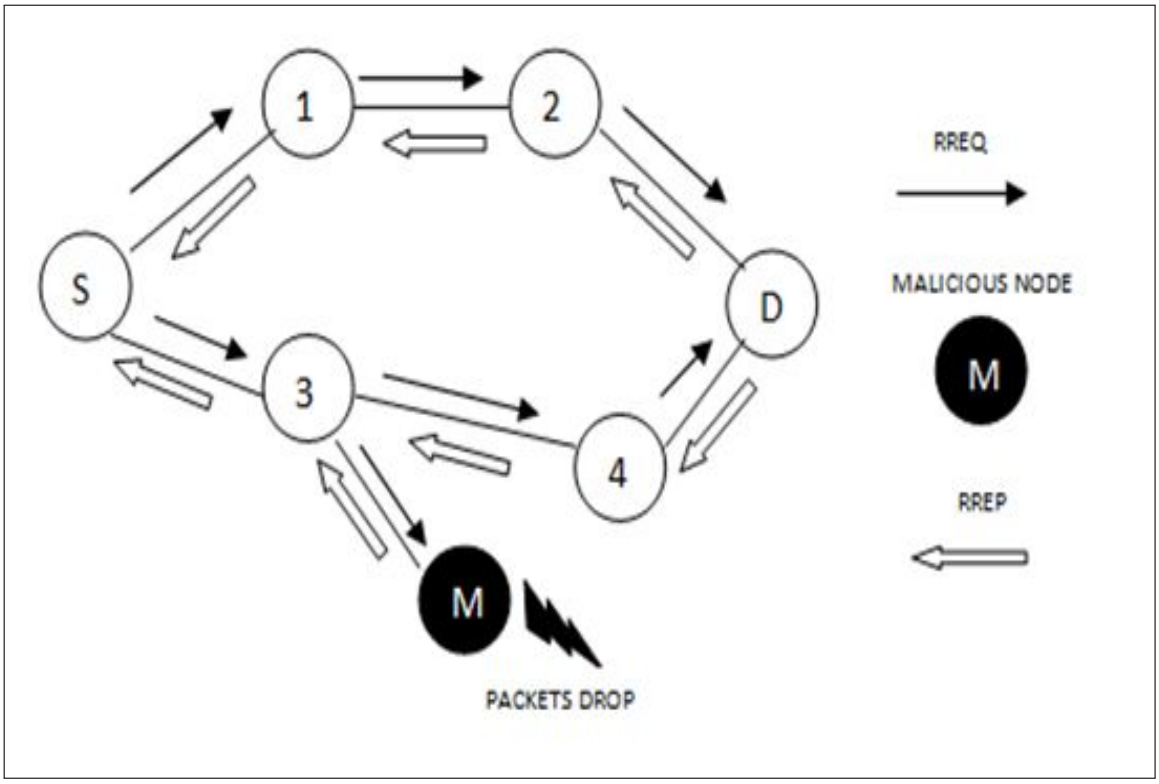

Figure 3.1: Single blackhole attack scenario.

3.2 Detecting Blackhole Attack on DSR based MANETs

3.2.1 Introduction

As in chapter 2, most of the solutions discussed to avoid blackhole attacks in MANETs are based on the AODV protocol. In this chapter, we propose an algorithm based on DSR protocol. Unlike other solutions for preventing blackhole attacks, in which the malicious nodes are identified only after the actual routing process started, in our proposed solution, the blackhole nodes are identified before the actual routing process takes place.

3.2.2 DBA-DSR Algorithm

Our proposed Detecting Blackhole Attack scheme for MANETs (DBA-DSR) is designed to identify and isolate the blackhole nodes present in the MANET. This protocol is a modified version of DSR, in which the concept of fake RREQ packets introduced in [14] are used to identify the malicious nodes. The reason of sending fake RREQ packets before initiating the actual routing process is to identify the malicious nodes in the network before the event of any damage. An acknowledgement scheme is invoked, where the data packets are only routed if and only if the source node receives the reply to the acknowledgement packet sent by the source node. Thus, if the initial stage of sending the fake RREQ packets fails to identify the blackhole node, the proposed strategy of sending and receiving acknowledgement packet can identify the blackhole nodes in the network. The fake RREQ packet that is used to find the blackhole nodes in the network is similar to the actual DSR RREQ packet, except that a fake destination address is utilized, which really does not exists. The fake RREQ packets behave just like normal RREQ packets but their lifetime is very limited. Our mechanism uses the same method as the RREQ packets in DSR to avoid congestion in the network. Figure. 3.2 illustrates the RREQ packet structure.

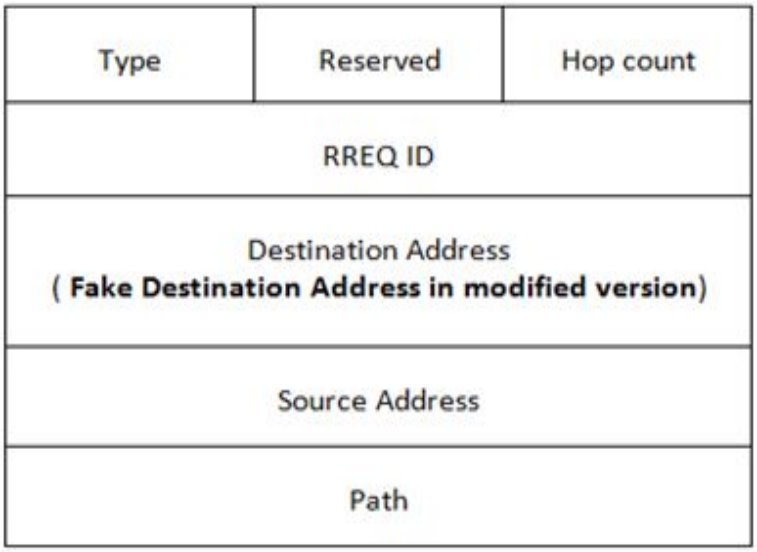

Figure 3.2: RREQ packet format

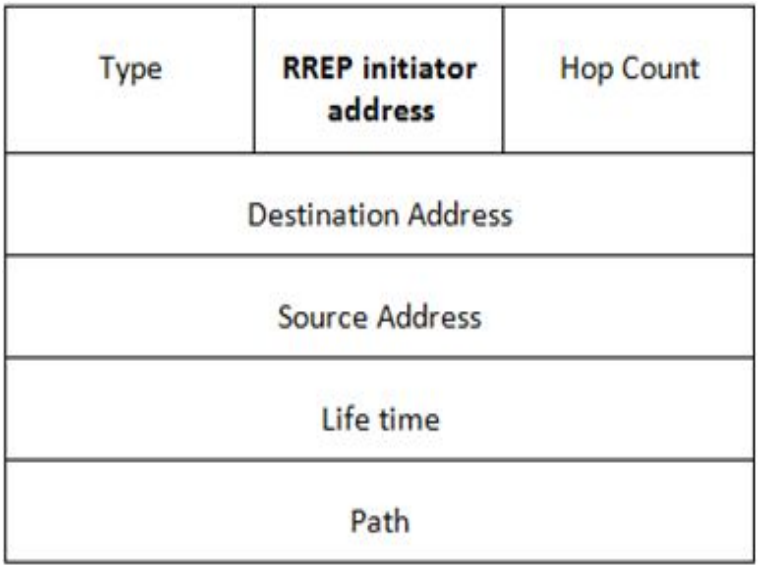

Figure 3.3: RREP packet format

This algorithm also modifies the DSR's RREP packet to find the address of the node that initiated the RREP packet. To do this, another new(referred to as RREP initiator address) field is added to the packet structure. The RREP initiator address field stores the address of the node that initiated the RREP packet. Whenever a node initiates the RREP packet,

its address is stored in this field so that the source node is aware of the address of this node. Figure. 3.3 illustrates the modified RREP packet structure.

The DBA-DSR algorithm works as follows:

1. Before starting the normal DSR routing procedure, the source node initializes a fake RREQ packet with a random destination address that does not exist.

2. Whenever the malicious node receives the fake RREQ packet, it creates a RREP packet with a fake route to the destination address and replies to the source node.

3. When the source node receives the RREP packet in reply to the fake RREQ, it identifies that there is some malicious activity in the network and checks the RREP initiator field in the RREP packet to identify the node which initiated the RREP packet in reply to the fake RREQ packet.

4. When the source node traces back the malicious node in the network, it records the address of the malicious node in a blackhole list table. This table stores the addresses of all malicious nodes. Nodes that are captured in this table are prevented from further participation in the routing procedure.

5. After the process of sending the fake RREQ is completed, the normal DSR routing process is started.

6. When the source node receives the RREP packet in reply to the original RREQ packet, it checks whether the RREP is from the destination node or from an intermediate node.

7. If the RREP is from the destination node, the algorithm considers the route to be safe and transmits the data through that particular route. If the RREP message is initiated by any other intermediate node, it will send an acknowledgment packet to the destination node to find out whether the route is safe or not.

8. If the source node receives a reply to the acknowledgment packet, it considers the route to be safe and transmits the data. If the reply to the acknowledgment packet is not received, the source node repeats the process of sending the fake RREQ to identify the malicious nodes in the network.

The pseudo-code of the DBA-DSR algorithm is shown below:

Algorithm 1 DBA-DSR

Require: DSR Protocol (MANETs)
RREQ: Route request packet
RREP: Route reply packet
SN:Source node
DN: Destination node
ACK: Acknowledgement packet
IN: Intermediate node

```
1: SN broadcasts fake RREQ packet
2: if SN receives RREP for fake RREQ then
3:     SN checks the RREP packet for the address of the node that initialized RREP and
   marks the node as malicious
4: else
5:     Proceed with normal DSR routing
6:     if RREP from DN then
7:         Consider the route to be safe and start transmitting the data packets
8:     else if RREP from IN then
9:         Send an ACK packet to the DN
10:        if Reply to ACK is received by SN from DN then
11:            Consider the route to be safe and start transmitting the data packets
12:        else
13:            Go back to step 1
14:        end if
15:    end if
16: end if
```

3.3 Detecting Colloborative Blackhole Attack in MANETs

3.3.1 Introduction

In this section, we propose a DSR-based protocol to mitigate collaborative blackhole attacks in MANETs. Unlike other schemes for preventing blackhole attacks, in which the malicious nodes are identified only after the actual routing process started, in our solution, the blackhole nodes or collaborative blackhole nodes are identified before the actual routing process takes place.

3.3.2 DCBA Algorithm

In this section, a modified version of the DSR protocol (our so-called DCBA) is proposed to find a secure route between the source and destination nodes and isolate the malicious blackhole nodes in MANETs. Our approach merges the advantage of proactive detection in the initial stage and reactive mechanism at the later stages if the proactive detection approach fails to identify the malicious blackhole nodes. Consequently, our mechanism is different from other methods that just use a reactive approach that would suffer a blackhole attack in its initial stage. In our proposed algorithm, malicious nodes are identified by means of our so-called *suspicious values* of nodes. A suspicious value is an important parameter to judge the behavior of a node (i.e. whether it is malicious or not malicious). As a source routing protocol, DSR can identify the addresses of all the nodes in a routing path once the source node has receive the RREP message in response to a RREQ message. However, the source node itself cannot identify exactly which intermediate node has the route information to the destination node and the reply RREP. This situation can result to the source node sending packets to a fake shortest path claimed by a malicious node (among available existing ones if any), yielding a blackhole attack that causes packets loss. However, it is difficult to identify which malicious node(s) generated the packets loss.

Our DCBA protocol combines a modified DSR and the BDSR protocol [14], to yield a

strong method for detecting collaborative blackhole attacks in MANETs. For the design of our protocol, the packet format of the RREP message in DSR is modified as follows. In the RREP, the reserved field is changed to the RREP initiator address field. The latter will store the address of the node that replies to the RREQ. This RREP initiator address field can help tracing the intermediate node that claimed it has the shortest route to the destination node. To achieve this goal, the concept of suspicious value attached to anode is introduced, which is described as follows.

In our proposed method, each node has its own suspicious value, which is based on the abnormal difference observed between the routing messages transmitted from the node. Suspicious values for each node are stored in a table (so-called suspicious values table). This table for each node is updated periodically after a certain time interval. Whenever the source node receives the route reply (RREP) packet in reply to the route request (RREQ) packet, it checks the RREP packet for the address of the node that initiated the RREP packet. The source node checks the suspicious value of the node that initialized the RREP packet. If this value is higher than the threshold level, then the node is considered as malicious and its address is stored in a blacklist table, preventing that node to further participate in the routing process. The threshold value is variable and can be adjusted depending on the performance of network.

In general, if an intermediate node is not the destination node, and it never broadcasts a RREQ, but forwards a RREP for the route, then its suspicious value is increased in the suspicious value table. Only the source node has the right to update or modify the suspicious value table. Thus, whenever the source node realizes that a node's suspicious value is to be increased, it will notify every other node in the network in order to have each of them update its suspicious values table. When the suspicious value of a node reaches the prescribed threshold value, it is considered as a malicious node.

3.3.2.1 Routing Mechanism

Whenever the source node wants to send some data to the destination node, it initiates the route discovery process. In this process, the source node broadcasts the Route Request (RREQ) packet. All the intermediate nodes that receive this RREQ packet check their routing table for the routing information to the destination node. If the intermediate node has the routing information to the destination, it will reply with a Route Reply (RREP) packet to the source node. When the source node receives the RREP packet, it checks the RREP for the address of the node that initiated the RREP packet using the RREP imitator address field in the RREP packet. Then, the source node checks the suspicious value of the node that initiated the RREP. If the suspicious value of that node is higher than the specified threshold level, then the source node sends an alarm message to all other nodes, indicating that there is a malicious node and updates the blacklist table with the address of that malicious node. If the suspicious value is below the specified threshold value, the source node starts routing the data packets. If the destination node detects that the packet delivery ratio drops below the prescribed threshold after the route had been built, the detection mechanism will be triggered again to avoid blackhole nodes that may have not been detected. Consequently, our mechanism is able to proactively detect blackhole nodes and react immediately. The pseudo-code of the DCBA algorithm is shown below, and a flowchart describing its operation is captured in Figure. 3.4

Algorithm 2 DCBA

Require: DSR Protocol (MANETs)
RREQ: Route request packet
RREP: Route reply packet
SN:Source node
DN: Destination node
ACK: Acknowledgement packet
IN: Intermediate node

SN broadcasts the RREQ packet
SN receives RREP
if RREP is from any IN **then**
    SN checks the RREP packet for the address of the node that initialized the RREP
    SN checks the Suspicious value of the intermediate node that initialized RREP
    if Suspicious value is below a threshold value **then**
        Consider the route to be safe and start routing the data packets
    else
        Mark the node as malicious node and build a blackhole list
    end if
else
    Start routing data packets
    if The packet delivery ratio is below the threshold value **then** Consider route to be danger
     and restart the routing process
    end if
end if

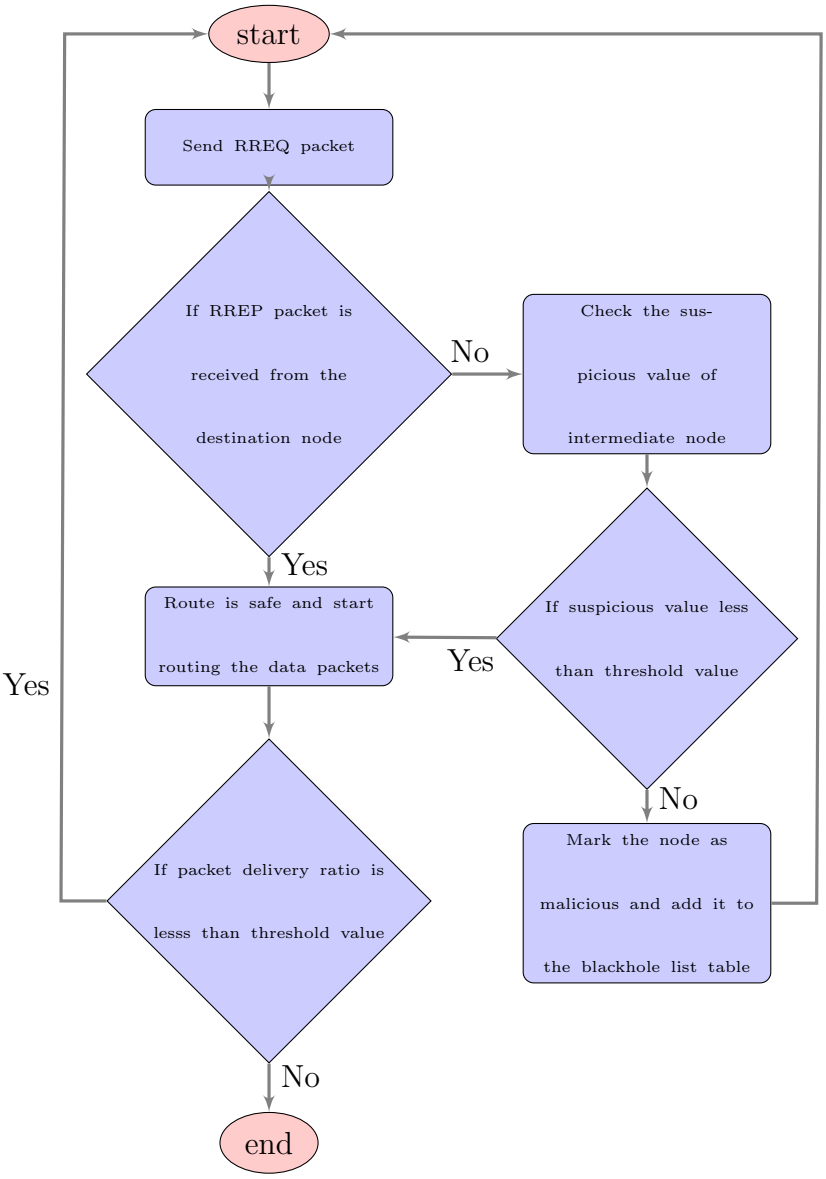

Figure 3.4: DCBA algorithm operations

Chapter 4

Performance Evaluation

This chapter discusses the performance and analysis of the algorithms proposed in this thesis. We use several performance metrics to evaluate the performance of all the proposed algorithms. We use the same simulation tool and operating environments for all the simulations.

4.1 Simulation Tool

Global Mobile Information System Simulator (GloMoSim) is a scalable network protocol simulation software that simulates wireless network systems. GloMoSim uses a parallel discrete-event simulation capability provided by Parsec [24]. This simulation tool is designed to be extensible and composable. It provides a high fidelity simulation results for wireless communication with detailed result sets for each layer in the network [25]. We use the GloMoSim 2.03 version to run our simulations using Parsec with RedHat-7.2 configuration files and a compiler based on a 32-bit linux operating system.

4.2 Performance Metrics

The following performance metrics are used for the evaluation of our proposed algorithms:

- **Packet delivery ratio**: This metric represents the ratio between the number of packets received at the final destination and the number of packets originated by the application layer sources.

$$Packet\ delivery\ ratio = \frac{Total\ number\ of\ packets\ received}{Total\ number\ of\ packets\ sent} \tag{4.1}$$

  The greater the packet delivery ratio, the better the performance of the network will be.

- **Average end-to-end delay**: This metric is the average time taken by the packet to reach the destination. This includes the time from generating the packet from the source node up to the reception of the packet by the destination node. It is expressed in seconds. This metric includes the overall delay of the network including buffer queues, transmission time and induced delay due to routing activities.

$$End\text{-}to\text{-}end\ delay = \frac{(arrival\ time - sending\ time)}{Number\ of\ connections} \tag{4.2}$$

  The lower the value of the end-to-end delay, the better the performance of the network will be.

- **Network throughput**: This metric represents the average rate of successful message delivery over a communication channel. It can be measured as bits per second (bps), packets per second (pps) or packet per time slot.

$$Network\ throughput\ in\ bps = \frac{Packet\ size\ in\ bits}{Latency\ in\ seconds} \tag{4.3}$$

- **Routing overhead ratio**: The routing overhead can be defined as the ratio of the amount of routing related control packets transmitted to the amount of data packets transmitted by the application traffic.

$$Routing\ \ overhead\ \ ratio = \frac{\sum control\ \ packets\ \ transmitted}{\sum data\ \ packets\ \ transmitted} \tag{4.4}$$

4.3 Single Blackhole Attack

4.3.1 Assumptions and Scope of Simulations

We assume that all the nodes which are part of the network are working normally. Initially the nodes are uniformly placed over the specified terrain dimensions and move at a varying mobility speed. The movement and direction of the nodes are randomized by the simulator. In this section we analyze the performance of the MANET in the presence of the Blackhole node.

4.3.2 Simulation Parameters

Table. 4.1 outlines the simulations settings used:

Table 4.1: Single Blackhole Attack Parameters

Parameter	**Setting**
Terrain dimension	2000 x 2000
Number of nodes	30
MAC protocol	IEEE 802.11
Radio range of a node	250 m
Traffic Type	CBR
Network layer routing protocol	AODV
Simulation time	150m
Data rate (Mbps) mobility model	Random way point
Speed	10-90 m/s with 10 m/s increments
Packet size	512 bytes
Pause time	Random (0 – 60 s)

4.3.3 Performance Metrics

The performance metrics used to evaluate the effect of single blackhole attack in MANETs are:

- Packet delivery ratio
- Average end to end delay
- Network Throughput

All the above metrics are measured against the node mobility in the network. Node mobility in the MANET is measured in meters/seconds(mps).

4.3.4 Simulation Scenario

In the blackhole scenario, 30 nodes are placed uniformly over the 2000 m x 2000 m flat space. Node **6** is the source node and node **28** is the destination, and node **1** is the malicious node. The malicious node in the network acts as a blackhole node. Whenever it receives a RREQ packet, it replies back to the source node with the fabricated RREP packet. Whenever the data reaches the malicious node, this node drops all the packets without forwarding them to the destination node.

4.3.5 Results

In this simulation, first we observed the effect of the Packet Delivery Ratio (PDR) measured for the AODV protocol when the node mobility increases. In Figure. 4.1, it can be observed that packet delivery ratio in the network with/without blackhole node decreases when the node speed increases. Moreover, the PDR is high in the network operating in normal condition compared to when the network operates in the presence of blackhole attack is present. This is due to the presence of the malicious node which drops the packets when it receives them.

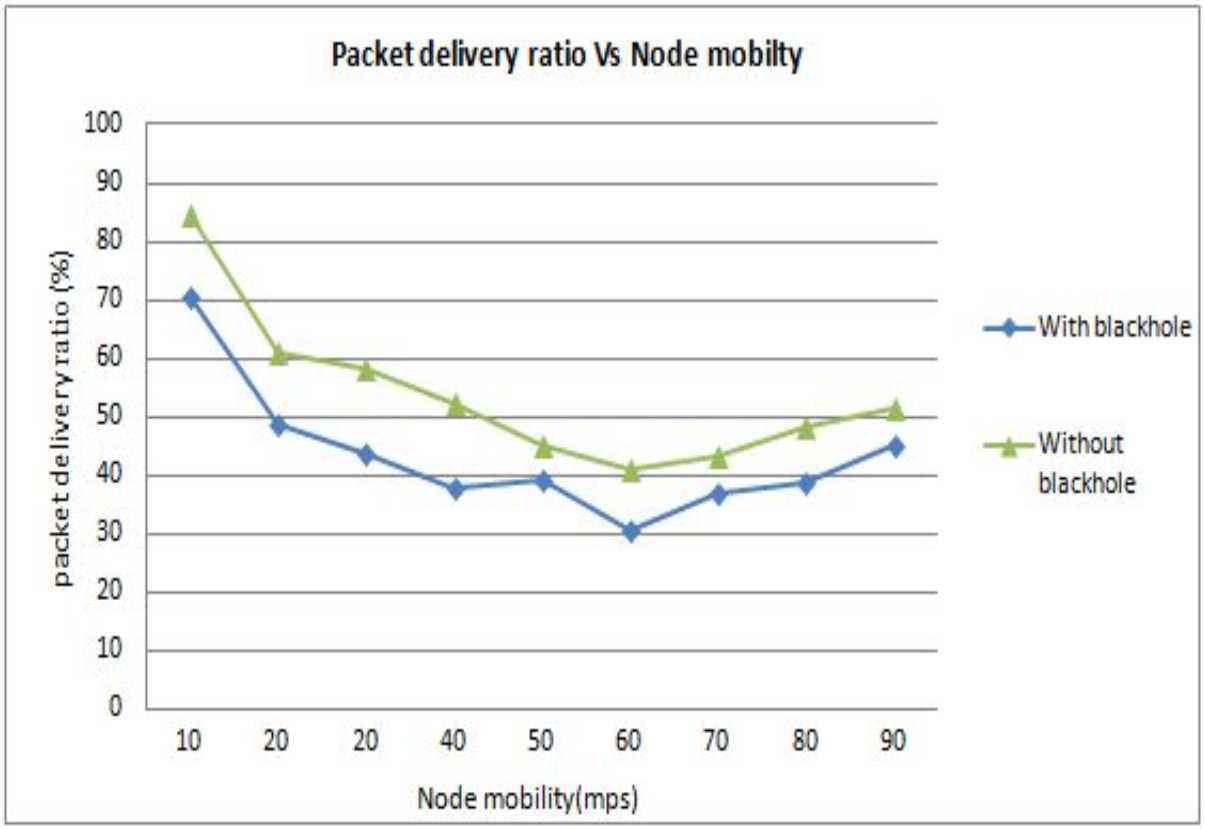

Figure 4.1: Single blackhole attack - Node Mobility Vs Packet delivery ratio

In Figure. 4.2, the results obtained when investigating the network throughput is depicted. It can also be observed that the network throughput decreases when the node speed increases, and this behavior is more pronounced when the network is under attack. This can also be attributed to the role played by the blackhole node, which is dropping the packets.

Finally, the effect of blackhole attack on the average end-to-end delay is investigated. The results are depicted in Figure. 4.3. It can be observed that the end-to-end delay is more pronounced when the network is under normal operation compared to when the malicious node is present. This might be due to the immediate route reply sent by the malicious node, where it does not check the routing table for finding the route.

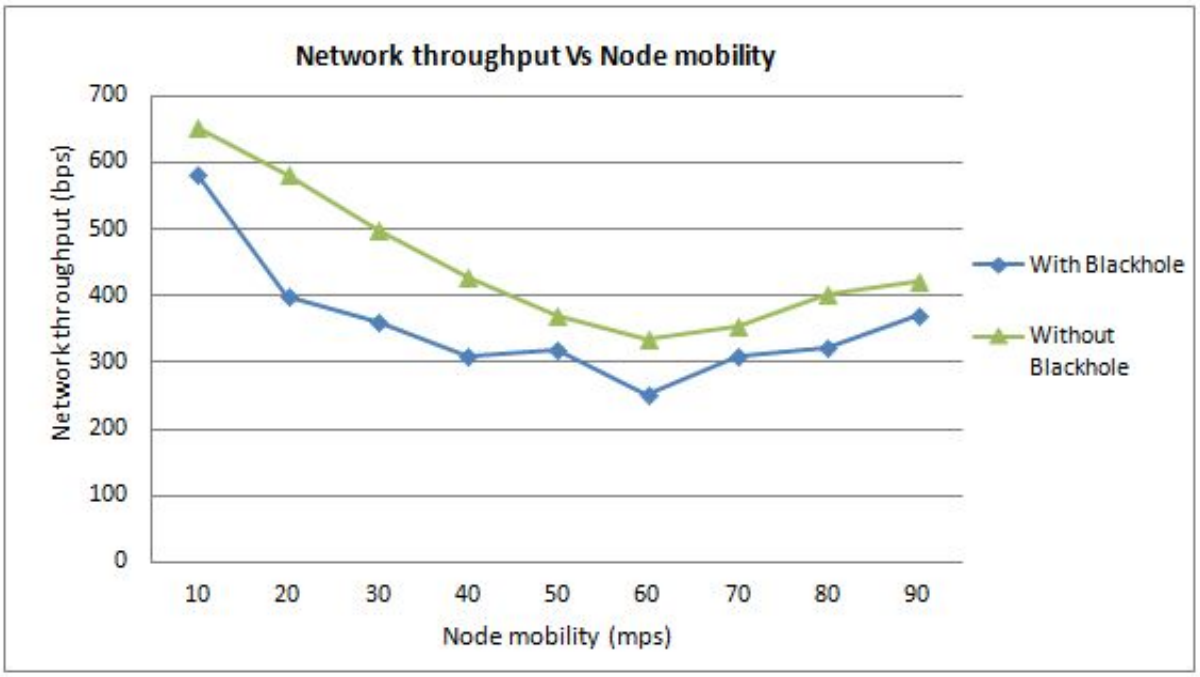

Figure 4.2: Single blackhole attack - Node Mobility Vs Network Throughput

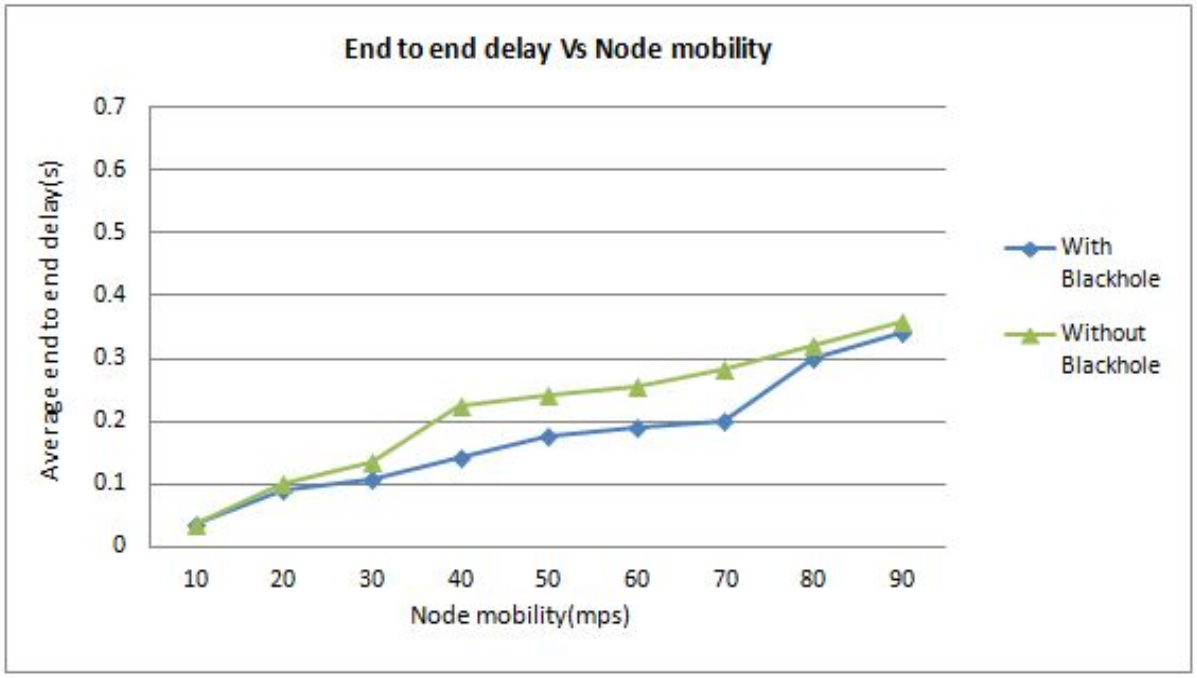

Figure 4.3: Single blackhole attack - Node Mobility Vs End-to-end Delay

4.4 DBA-DSR

4.4.1 Assumptions and Scope of Simulations

We assume that all the nodes in the simulation environment are working normally and are part of the network simulation. Each node is restricted to move within the specified terrain dimensions of the MANET. The simulator randomizes the movement and direction of each node. The main traffic generator used in this simulation will be the Constant Bit Rate (CBR). CBR is very stable and fast in generating the network traffic and is popular among modern communications.

4.4.2 Simulation Parameters

Table. 4.2 outlines the simulations settings used for the DBA-DSR algorithm:

Table 4.2: DBA-DSR Parameters

Parameter	**Setting**
Terrain dimension	1000 m x 1000 m
Number of nodes	50
MAC protocol	IEEE 802.11
Radio range of a node	250 m
Traffic Type	CBR
Network layer routing protocol	DSR
Simulation time	10 minutes
Data rate (Mbps) mobility model	Random way point
Speed	0 - 80 m/s
Packet size	64 bytes
Pause time	0 - 80 s

4.4.3 Performance Metrics

The performance metrics used to evaluate the performance of DBA-DSR protocol in MANETs are:

- Packet delivery ratio
- Network Throughput
- Routing overhead ratio

All three metrics are measured against node nobility, pause time and percentage of malicious nodes in the network.

4.4.4 Simulation Scenario

A MANET with 50 nodes is designed, and the choice of malicious nodes in the network is random. A source node and a destination node are selected, and about 500 data packets of 64 bytes each are transmitted from source to destination. The malicious nodes in the MANET drop all the packets received by them.

4.4.5 Results

The first performance metric used in the analysis of our solution is the packet delivery ratio. Figure. 4.4 depicts the effect of the packet delivery ratio on the node mobility in the presence of blackhole attacks in the network, where node mobility (mps) is the rate at which the nodes are moving in the network. It can be observed that DSR suffers heavy loss in packets in the presence of blackhole nodes. But, the DBA-DSR scheme gives a higher and consistent packet delivery ratio even in the presence of blackhole nodes.

When the mobility speed is increased, the packet delivery ratio of our protocol decreases since more link breakdowns make our protocol spend more time to find secure routes, which

result in higher packet loss. Second, the packet loss percentage of our new protocol is lower than that of the benchmark method (DSR) because our protocol takes more time to avoid blackhole nodes and to establish a secure route when the number of link breakdown increases. Thus, this delay causes lower packet loss percentage than that observed in the benchmark scheme. Third, the packet delivery ratio of the DSR decreases when the speed increases since more link breakdowns will cause more new route discoveries.

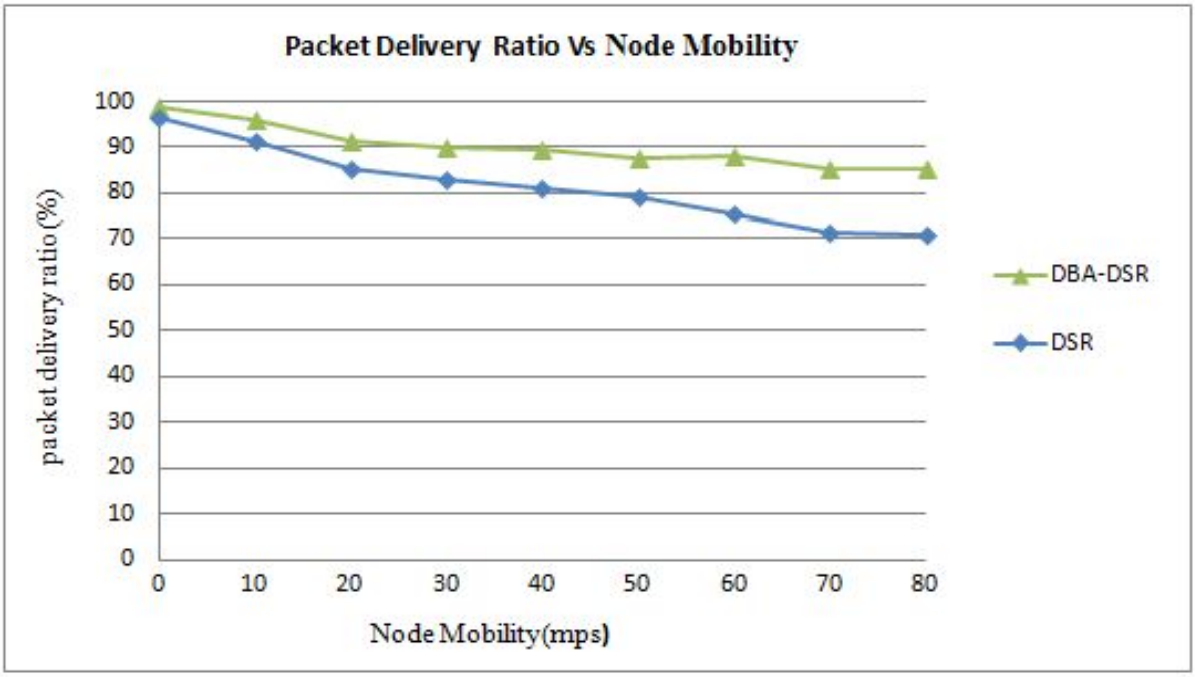

Figure 4.4: DBA-DSR - Packet delivery ratio Vs Node mobility

Figure. 4.5 depicts the effect of the pause time on the packet delivery ratio. It can be observed that in both schemes (DSR and DBA-DSR), the packet delivery ratio drops as the pause time is increased. It can also be observed that the DBA-DSR scheme is able to achieve better results in the presence of the blackhole nodes compared to the normal DSR. This may be explained by the fact that the normal DSR does not have any built-in security mechanism.

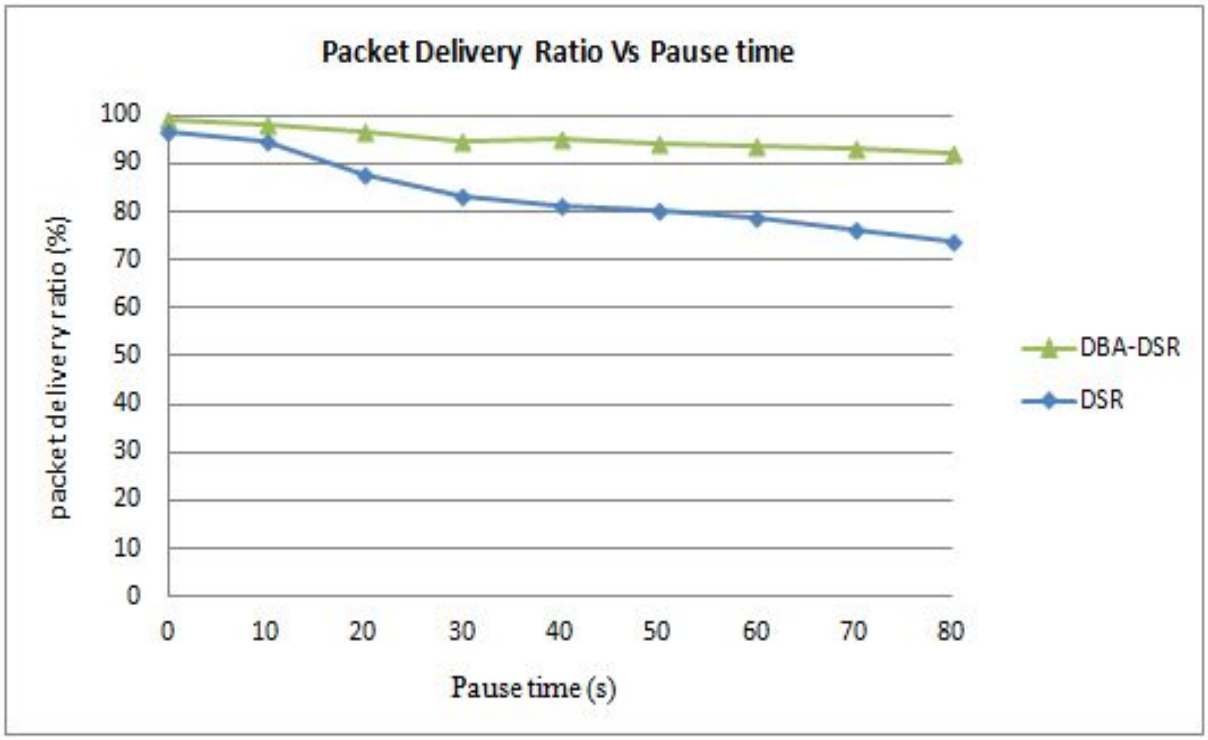

Figure 4.5: DBA-DSR - Packet delivery ratio Vs Pause time

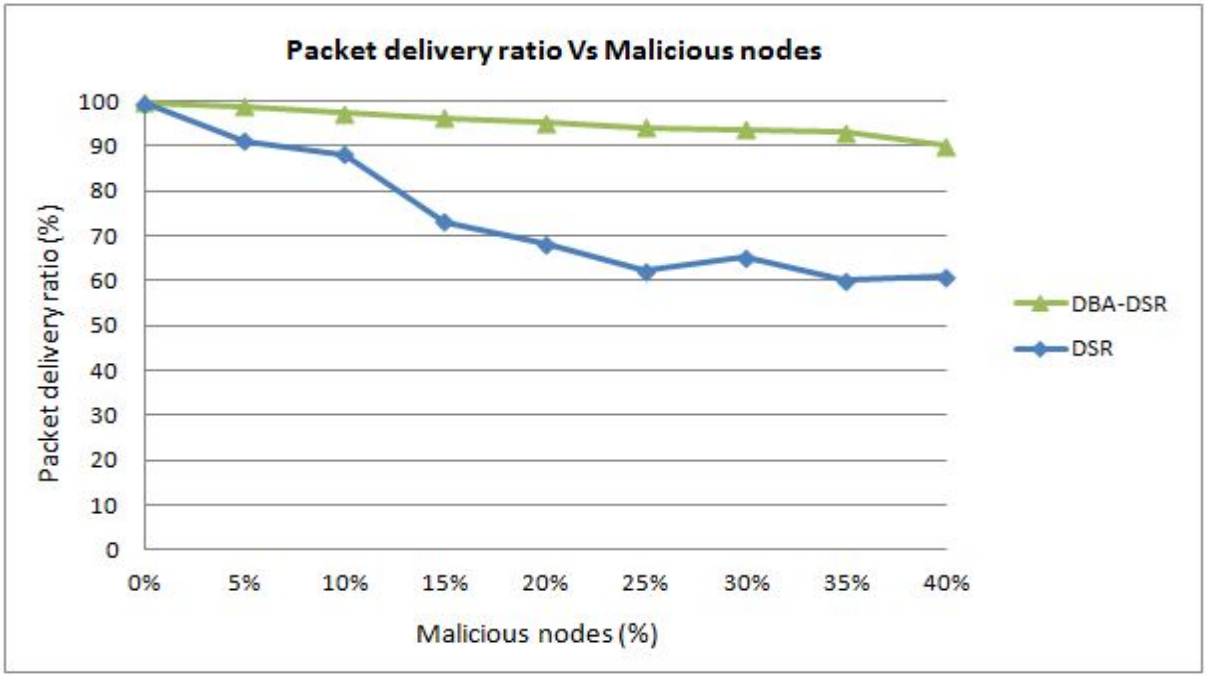

Figure 4.6: DBA-DSR - Packet delivery ratio Vs Malicious nodes (%)

Figure. 4.6 illustrates the impact that the percentage of malicious nodes in the MANET has on the packet delivery ratio. First, it can be observed that DSR heavily suffers from the blackhole attack. Therefore, its packet delivery ratio decreases as the number of malicious nodes in the network increases. Second, our protocol generates a higher packet delivery ratio percentage compared to the DSR protocol. This is due to the fact that our protocol can prevent the blackhole attack to occur in the network. When the number of malicious nodes is increased, the packet delivery ratio percentage decreases for both protocols. Furthermore, the packet delivery ratio of our protocol decreases slowly compared to that observed for DSR. This is due to the fact that the delay in finding the routes causes packet loss in the network. However, the DSR shows a significant decrease in the packet delivery ratio percentage when the number of malicious nodes increases since the frequency and the capacity of attacks increases, which cannot be prevented by DSR protocol.

The second performance metric used in the analysis of our solution is the network throughput. Figure. 4.7 depicts the effect of the node mobility on the network throughput. It can be observed that in both schemes (DSR and DBA-DSR), the network throughput drops as the mobility speed is increased. Our protocol generates a higher throughput than the DSR protocol. This is due to the fact that our solution prevents black hole attacks properly. The throughput of our protocol slightly decreases when the mobility speed increases since high mobility speed causes higher link breakdown probability, and in turn the protocol introduces more route discovery processes. Thus, both the protocols take more time to find secure routes.

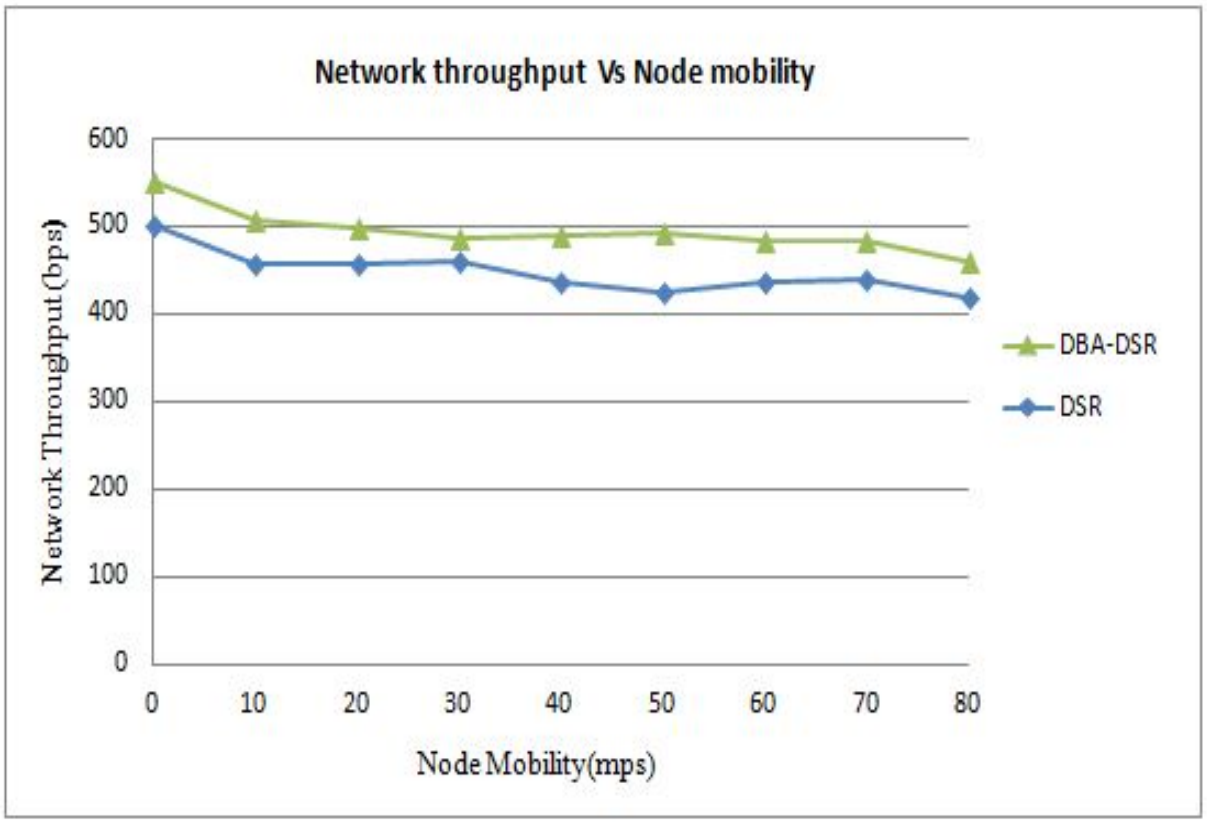

Figure 4.7: DBA-DSR - Network throughput Vs Node mobility

The effect of the pause time on the network throughput is depicted in Figure. 4.8. It can be observed that the normal DSR protocol under blackhole attack has lower throughput when compared to that of the DBA-DSR scheme under blackhole attack. This can be explained as follows. As nodes become more and more stationary, the path from source to destination becomes more stable. Therefore, data sent along transient routes (resulting from quick node movement) decreases, thus reducing the overall throughput. This is due to the fact that TCP retransmissions are counted as part of the useful network throughput.

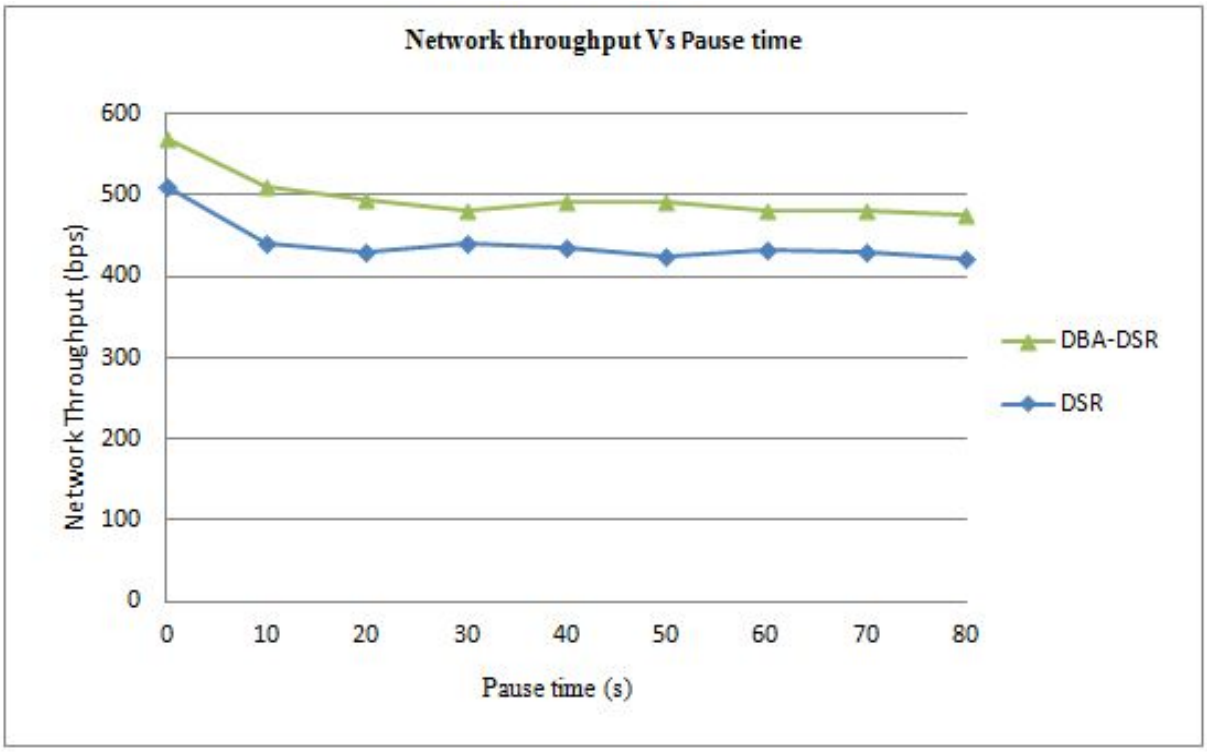

Figure 4.8: DBA-DSR - Network throughput Vs Pause time

The third performance metric used in the analysis of our solution is the routing overhead ratio in the network. The effect of the pause time on the routing overhead ratio is depicted in Figure. 4.9. When the pause time increases, DSR introduces the lowest overhead since it does not have any security mechanism or defensive method. But our method uses the proactive method to identify the malicious nodes before the actual routing process, and the acknowledgement scheme leads to a slight increase in the routing overhead, which is negligible in our case.

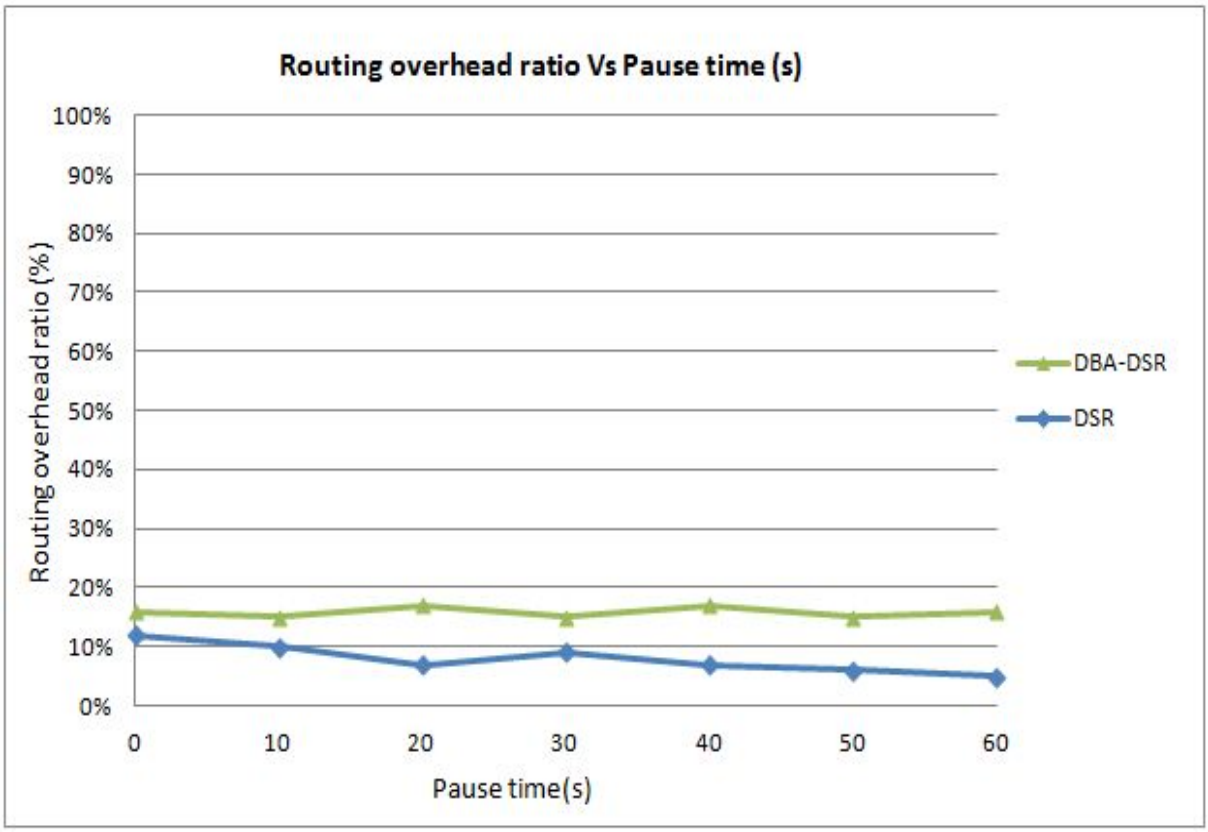

Figure 4.9: DBA-DSR - Routing overhead(%) Vs Pause time

The effect of the percentage of malicious nodes on the routing overhead ratio is depicted in Figure. 4.10. First, the DSR protocol introduces the lowest overhead. This can be explained by the fact that the DSR protocol does not use any additional requests for finding the secure routes. In addition, the routing overhead ratio for DSR decreases as the number of malicious node increases.This can be explained by the fact that malicious node in network will cause immediate reply to the route requests, which in turn will cause less overhead . Since the existence of more blackhole nodes forces our protocol to use more and more requests to identify and eliminate them, our protocol generates more overhead than DSR when the number of blackholes increases in the network.

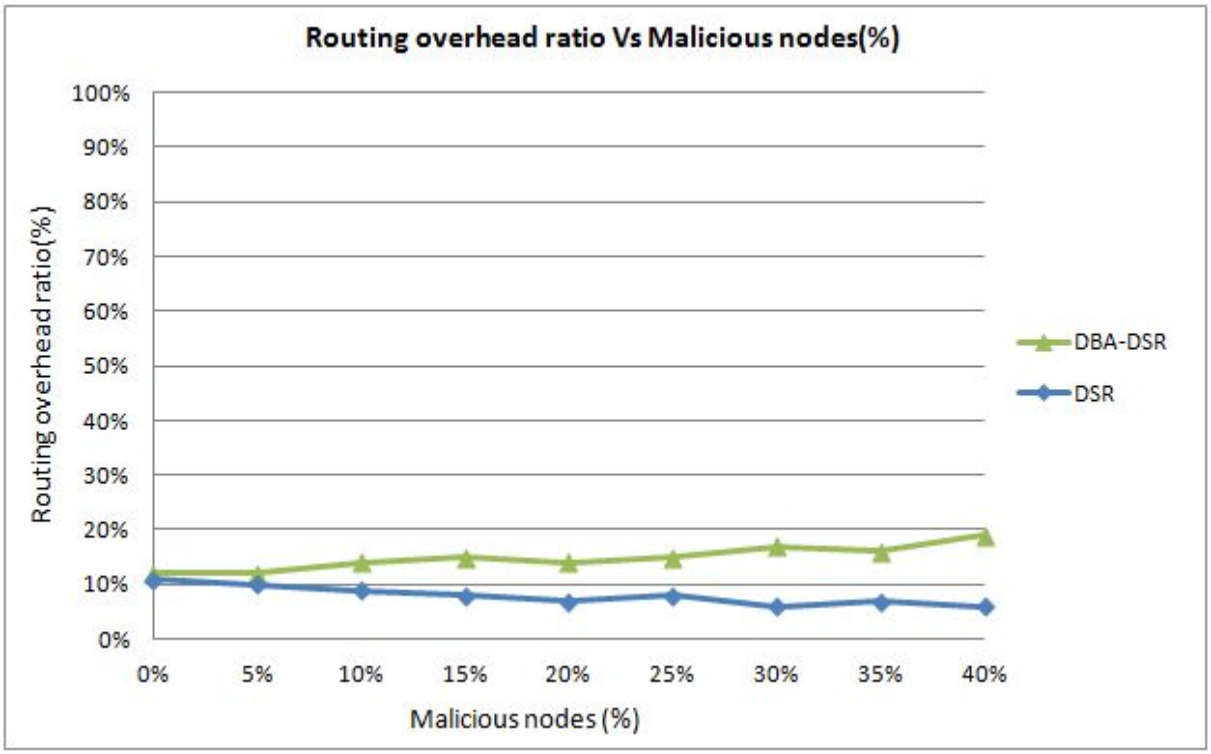

Figure 4.10: DBA-DSR - Routing overhead(%) Vs Malicious nodes(%)

4.5 DCBA

4.5.1 Assumptions and Scope of Simulations

We assume that all the nodes in the simulation environment are working normally and are part of the network simulation. Each node is restricted to move within the specified terrain dimensions of the MANET. The simulator randomizes the movement and direction of each node. The main traffic generator used in this simulation will be the Constant Bit Rate (CBR). CBR is very stable and fast in generating the network traffic and is popular among modern communications.

4.5.2 Simulation Parameters

Table. 4.3 outlines the simulation settings used for the DCBA algorithm.

Table 4.3: DCBA Parameters

Parameter	**Setting**
Terrain dimension	670 * 670
Number of nodes	50
MAC protocol	IEEE 802.11
Radio range of a node	250 m
Traffic Type	CBR
Network layer routing protocol	DSR
Simulation time	200s
Data rate (Mbps) mobility model	Random way point
Speed	0-80 m/s
Packet size	64 bytes
Pause time	0 – 60 s

4.5.3 Performance Metrics

The performance metrics used to evaluate the effect of single blackhole attack in MANETs are:

- Packet delivery ratio
- Network Throughput
- Routing overhead ratio
- Average end to end delay

All the metrics are measured against node mobility, pause time and percentage of malicious nodes in the network.

4.5.4 Simulation Scenarios

A MANET with 50 nodes is designed, and the choice of malicious nodes in the network is random. A source node and a destination node are selected, and about 200 data packets of 64 bytes each are transmitted from source to destination. The malicious nodes in the MANET drop all the packets received by them.

4.5.5 Results

The effect of the percentage of malicious nodes in the network on the packet delivery ratio (PDR) is first investigated. The results are captured in Figure. 4.11. It can be observed that DSR suffers heavy loss in packets in the presence of blackhole attack. This can be justified by the fact that DSR does not have any intrinsic detection and prevention mechanism to prevent blackhole attacks. Also the BDSR scheme uses a fake RREQ technique to find the blackhole attack, it can suffer packet loss if the malicious node does not reply to the RREQ packet. When varying the percentage of malicious nodes from 0% to 40%, DCBA generates a

higher and consistent PDR compared to BDSR scheme, even in the presence of collaborative blackhole nodes.

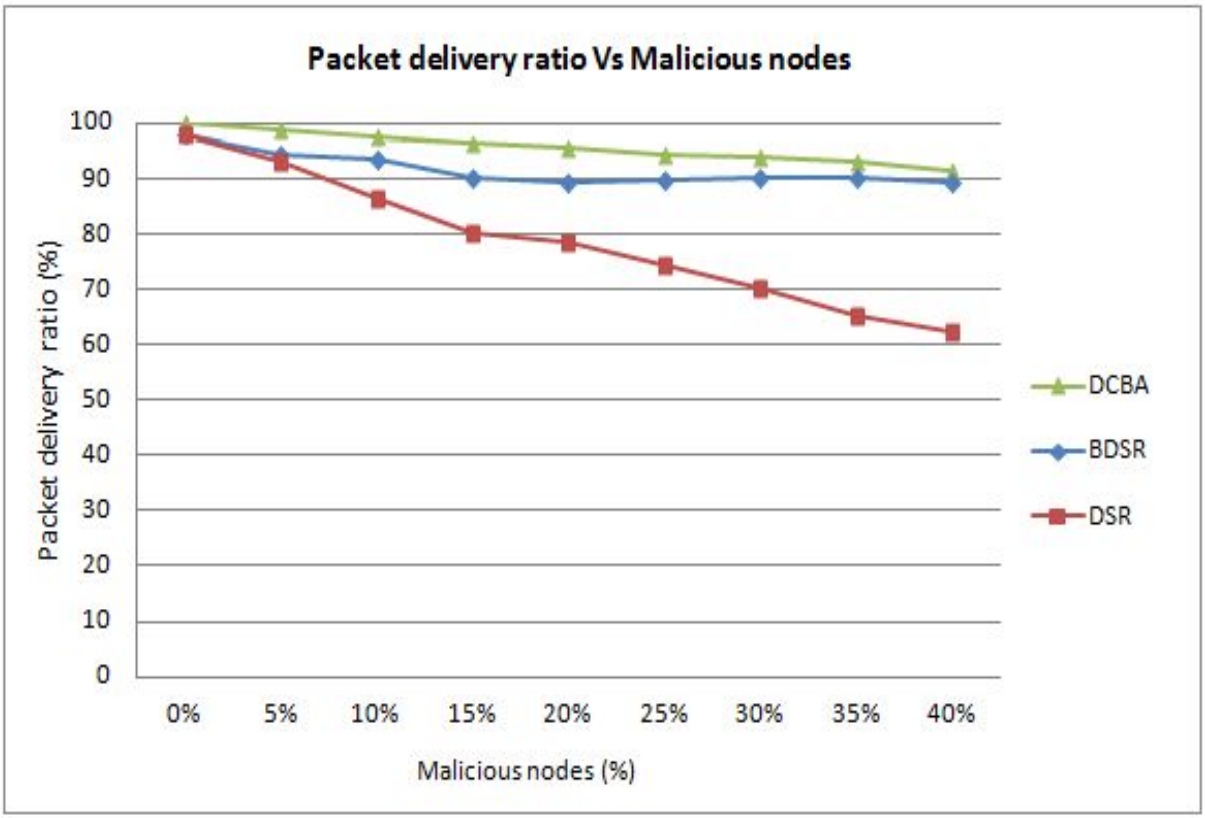

Figure 4.11: DCBA algorithm - Packet delivery ratio Vs Malicious nodes(%)

The effect of the pause time on the packet delivery ratio on is also investigated, and the results are depicted in Figure. 4.12. It can be observed that the packet delivery ratio drops as the pause time is increased. It can also be observed that our DCBA scheme generates higher packet delivery ratio compared to the BDSR scheme and the normal DSR protocol even in the presence of the collaborative blackhole nodes. Finally, it can be observed that the packet delivery ratio for the normal DSR protocol ranges between 94% and 66% for 5% and 40% of malicious nodes in the network respectively. Our protocol DCBA improves the situation by increasing the packet delivery ratio by more than 20%. This can be justified by the fact that the normal DSR does not have any built-in security mechanism.

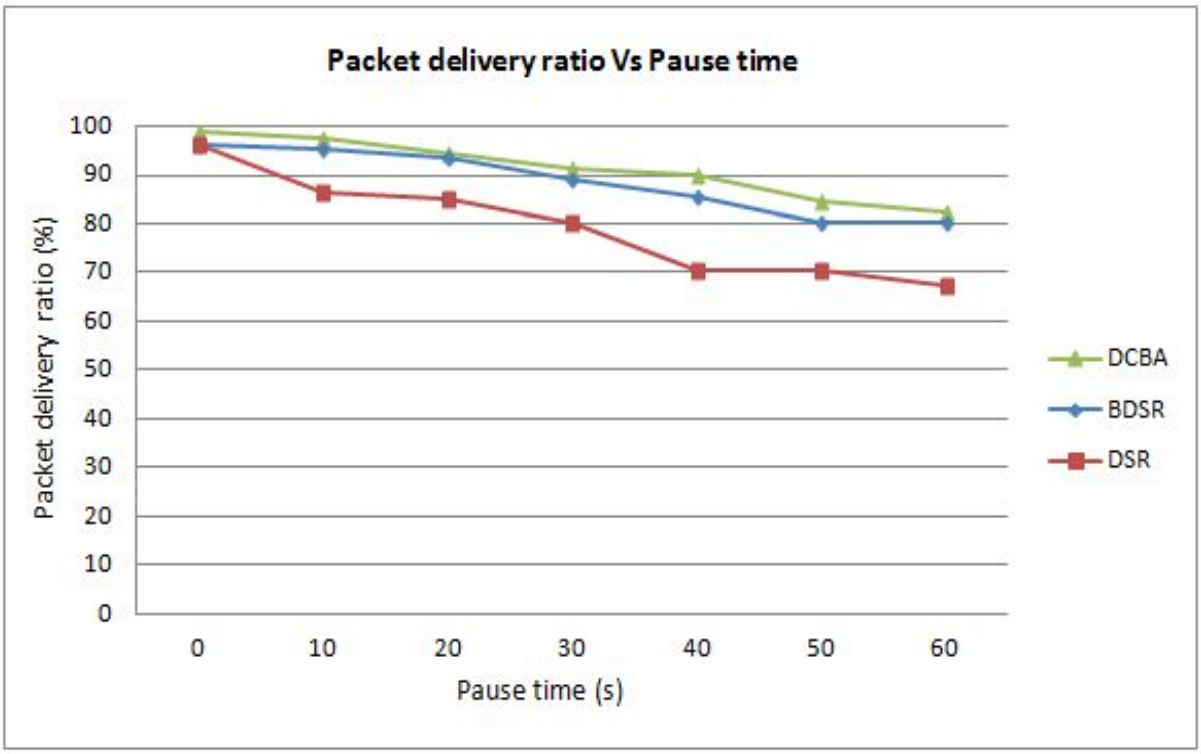

Figure 4.12: DCBA algorithm - Packet delivery ratio Vs Pause time

The second performance metric used in the analysis of our solution is the network throughput. The impact on the network throughput when the percentage of malicious nodes in the network increases is investigated. The results are captured in Figure. 4.13.

First, it can be observed that, DSR heavily suffers from the collaborative blackhole attacks since the protocol does not have any mechanism to prevent these attacks. Moreover, the throughput of DSR goes down under 300bps as the number of blackhole nodes in the network increases from 0% to 40%. Second, the throughput for the BDSR scheme ranges between 520bps and 480bps as the number of malicious nodes increases. Thirdly, our protocol generates a higher throughput than the other two protocols. This is due to the fact that our scheme prevents packet drops by malicious nodes using the proactive mechanism. Even with 40% of blackhole nodes, our protocol produces a throughput of 590bps. Furthermore, it can be observed that the normal DSR protocol under collaborative blackhole attack has the lowest throughput and BDSR also has less throughput when compared to that of the

DCBA scheme under blackhole/collaborative blackhole attacks.

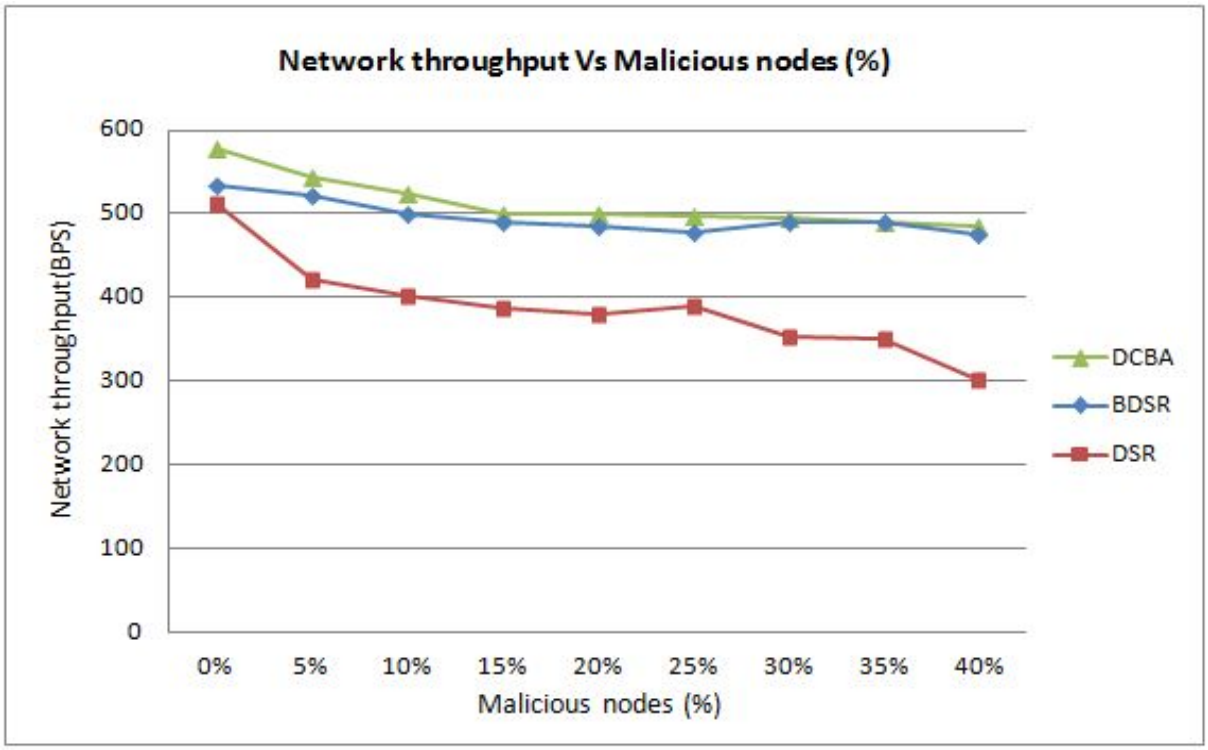

Figure 4.13: DCBA algorithm - Network throughput Vs Malicious nodes(%)

Next the effect of the pause time on the network throughput is also investigated, and the results are depicted in Figure. 4.14. As the pause time increases, the paths between the source node and the destination node last longer and becomes more stable. Therefore, the data packets transmitted along transient routes (resulting from quick node movement) decreases, thus reducing the overall throughput. First, it can be observed that the network throughput under normal DSR protocol decreases as the pause time increases. Secondly, it can be observed that the throughput under the BDSR scheme is higher than that obtained with the normal DSR scheme and our DCBA protocol has the higher throughput compared to that of DSR and BDSR. This can be justified by the fact that DCBA protocol is capable of mitigating the blackhole attacks in the network.

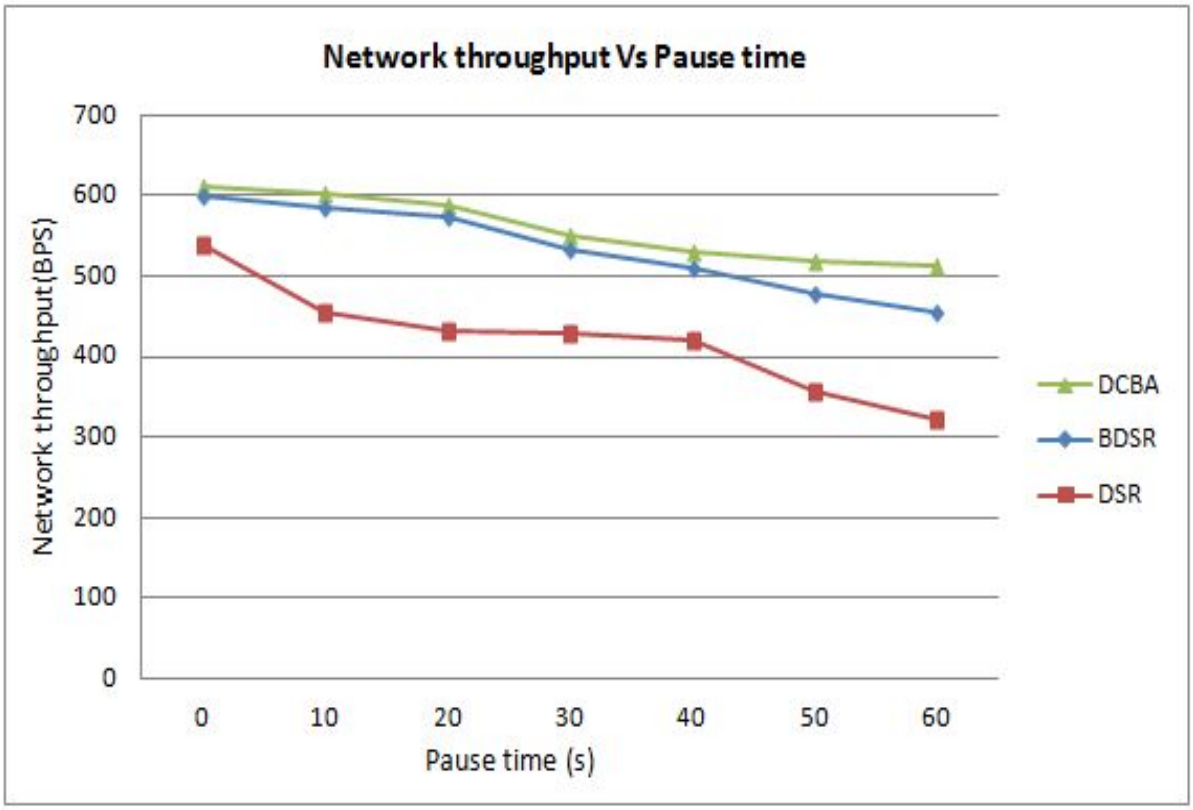

Figure 4.14: DCBA algorithm - Network throughput Vs Pause time

The third performance metric used in the analysis of our solution is the routing overhead ratio in the network. The effect of the pause time on the routing overhead ratio is depicted in Figure. 4.15. First, it can be observed that the DSR protocol routing overhead decreases as the pause time increases. This is due to the fact that the increase in pause time causes the attacker to establish a more stable path between the source and destination. As paths become more stable, the required number of routing related packets reduces. Secondly, the routing overhead ratio for the BDSR protocol is higher than that of the DSR protocol because the BDSR scheme uses more RREQ packets to find the secure route in the presence of blackhole nodes. Thirdly, DCBA's routing overhead is greater than that of the DSR scheme and less then that of the BDSR scheme because our protocol does not need the use of fake RREQ packets as the BDSR does.

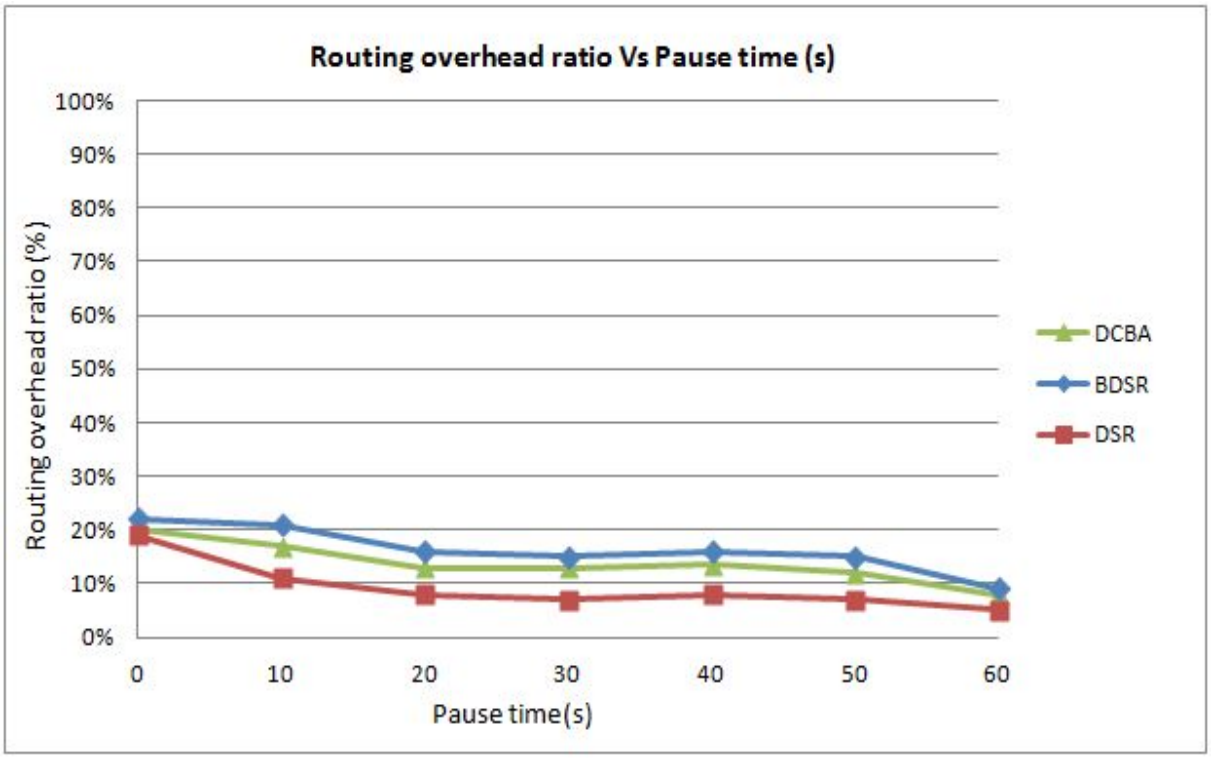

Figure 4.15: DCBA algorithm- Routing overhead(%) Vs Pause time

The effect of the percentage of malicious nodes on the routing overhead ratio is depicted in Figure. 4.16. First, the DSR protocol introduces the lowest overhead due to the fact that it does not use any additional requests for finding secure routes. Also the routing overhead ratio for DSR decreases as the number of malicious node increases. This is due to the fact that the presence of more malicious node in network causes immediate reply to the route requests, which in turn causes less overhead. Second, the routing overhead of the BDSR protocol is greater than that of the DSR protocol since BDSR uses the extra RREQ packets to bait the blackhole nodes.Third, DCBA introduces a lower overhead compared to BDSR and more overhead compared to DSR. This might be due to the fact that our solution uses normal RREP packets header to check the suspicious value of the node.

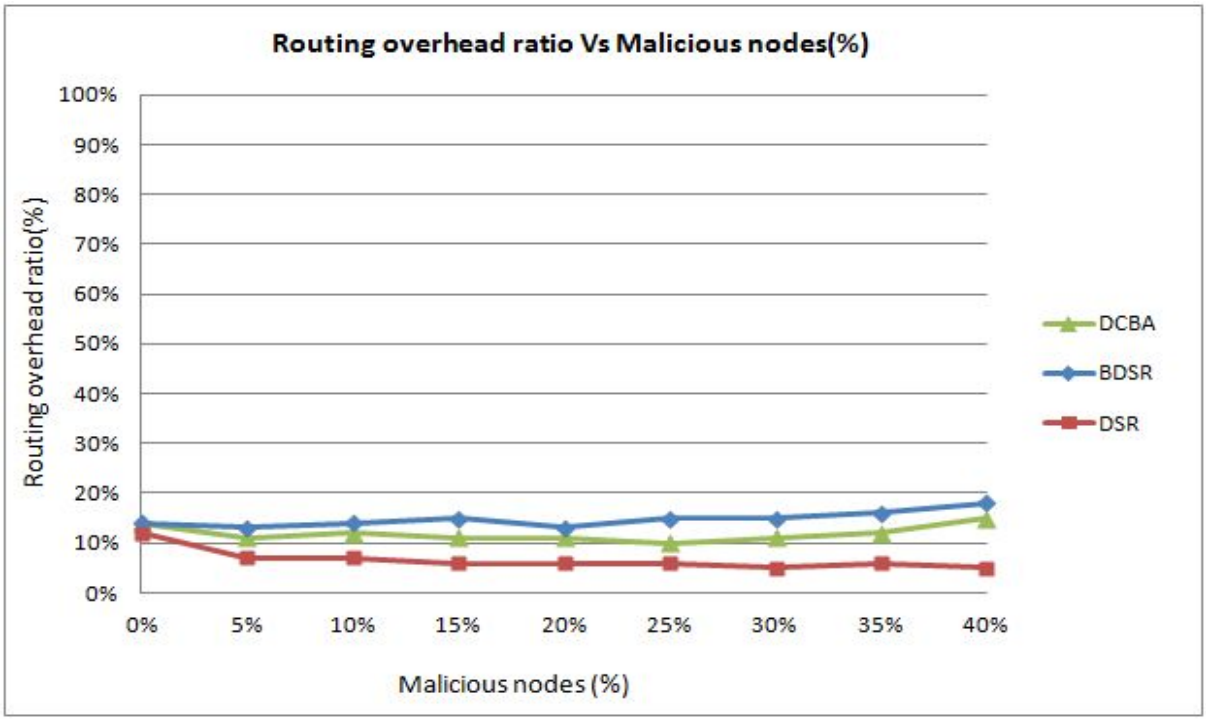

Figure 4.16: DCBA algorithm- Routing overhead(%) Vs Malicious nodes(%)

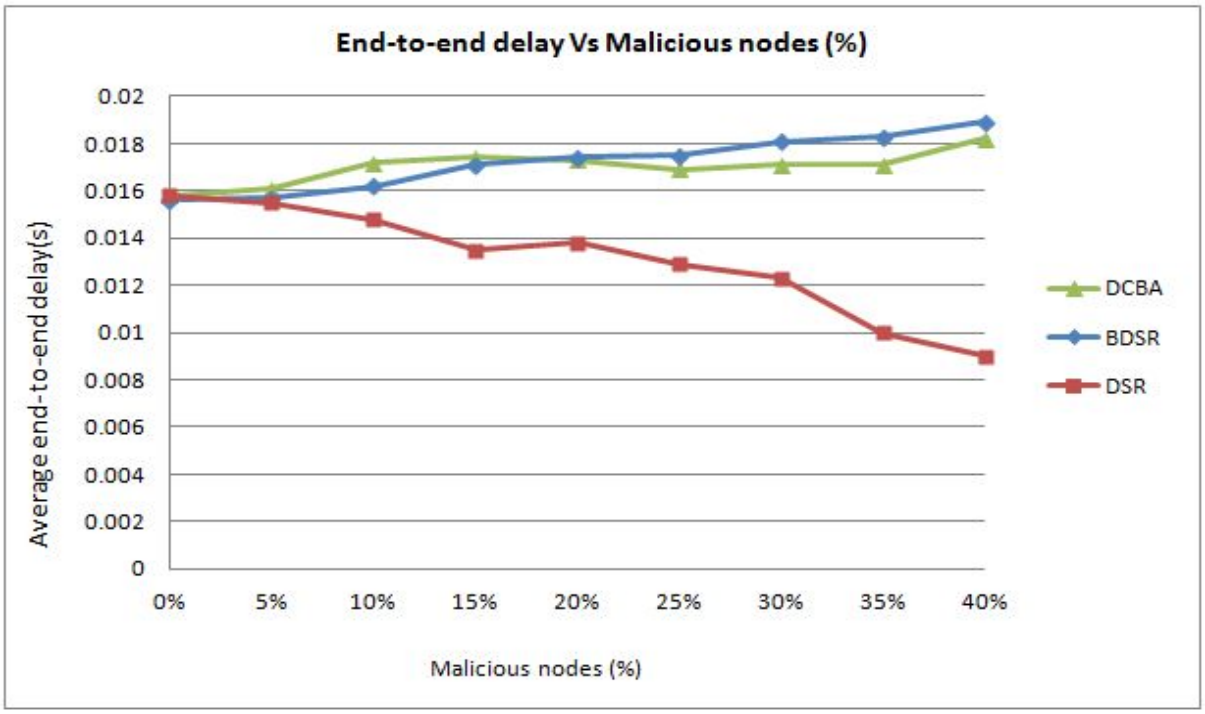

Figure 4.17: DCBA algorithm- End-to-end delay Vs Malicious nodes(%)

The impact of the number of malicious black hole nodes on end-to-end delay is depicted in Figure. 4.17 . It can be observed that the delay in DSR decreases when the percentage of blackhole nodes increases. This is justified by the fact that an increase in number of malicious nodes means that the source will have to find more routes between source to destination in less time because more blackholes reply quickly for the route requests. Secondly, the delay for the BDSR protocol and DCBA protocol increases with the increase in malicious nodes since it has to avoid more malicious nodes when it tries to find out secure route from source to destination.

Chapter 5

Conclusions

5.1 Conclusion and Future Work

The main goal of our thesis was to help improve the security in MANETs against collaborative blackhole attacks. Firstly, we have analyzed the behavior and challenges of security threats in mobile ad hoc networks as well as how blackhole attacks affect the performance and security for such networks. After some extensive research on many recent ideas of blackhole attack prevention in MANETs, we were able to brainstorm ideas to address the problem of collaborative blackhole attacks in MANETs.

Although many solutions have been proposed to mitigate the blackhole attacks in MANETs, most of the solutions proposed were reactive in nature i.e. they can identify the malicious node only after the attack has been carried out by the malicious node. Many of these solutions are also only capable of mitigating single blackhole attack and are not capable of avoiding collaborative blackhole attack.

For mitigation of blackhole attack in MANETs, firstly, we proposed the DBA-DSR scheme, a feasible DSR-based solution to mitigate blackhole attacks in MANETs. The BDA-DSR scheme is proactive in nature and is capable of finding malicious node before the actual routing process is initiated and before the attack has been carried out. Simulation

results showed that (1) the original DSR heavily suffers from blackhole attack in terms of network throughput and packet delivery ratio, (2) the proposed DBA-DSR scheme performs better than the DSR scheme in terms of network throughput rate and minimum packet loss percentage.

Secondly, we proposed a scheme (so-called DCBA) to identify and mitigate blackhole/collaborative blackhole attacks in MANETs. The proposed DCBA scheme merges the advantage of proactive detection in the initial stage and reactive mechanism at later stages if the proactive detection approach fails to identify the malicious blackhole nodes. Simulation results showed that the proposed scheme outperforms both the DSR and BDSR schemes in terms of network throughput rate and minimum packet loss percentage.

As part of future work, we intend to strengthen our DCBA by introducing cryptographic schemes into it. In our scheme it was assumed that only the source node had the right to update the suspicious value table and broadcast the information about the suspicious value table to other nodes in the network. We intend to secure the suspicious value information sent by the source node so that the malicious node cannot tamper with the valuable information.

Bibliography

[1] A. M. R. H. Khokhar, A. N. Ngadi, "A review of current routing attacks in mobile ad hoc networks," *International Journal of Computer Science and Security*, vol. 3, no. 5, pp. 18—-29, 2008.

[2] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the 2nd ACM workshop on Wireless security*, WiSe '03, (New York, NY, USA), pp. 30–40, ACM, 2003.

[3] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad-hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, pp. 46–55, 1999.

[4] W. L. Hongmei Deng and D. P.Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine,*, vol. 40, no. 10, pp. 70–75, 2002.

[5] S. Agrawal, S. Jain, and S. Sharma, "A survey of routing attacks and security measures in mobile ad-hoc networks," *Journal of Computing*, 2011.

[6] A.Vani and D. Rao, "Providing of Secure Routing against Attacks in MANETs," *International Journal of Computer Applications*, vol. 24, pp. 16–25, June 2011.

[7] V.K.Taksande and Dr.K.D.Kulat, "Performance Comparison of DSDV, DSR, AODV Protocol with IEEE 802.11 MAC for Chain Topology for Mobile Ad-hoc Network using NS-2," *International Journal of Computer Applications (IJCA) Special Issue on 2nd*

National Conference- Computing, Communication and Sensor Network (CCSN), no. 3, pp. 26–31, 2011.

[8] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-centric Computing and Information Sciences*, vol. 1, no. 1, pp. 4+, 2011.

[9] D. B. Johnson and D. A. Maltzion, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, pp. 153–181, Kluwer Academic Publishers, 1996.

[10] D. B. Johnson, David, and D. A. Maltzion, "Protocols for adaptive wireless and mobile networking," *IEEE Personal Communications*, vol. 3, pp. 34–42, 1996.

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks," in *Proceedings of International Conference on Wireless Networks*, (Las Vegas, Nevada, USA), pp. 570–575, 2003.

[12] L. Tamilselvan and V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET," in *Proceedings of the The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, AUSWIRELESS '07, (Washington, DC, USA), pp. 21–, IEEE Computer Society, 2007.

[13] L. Tamilselvan and V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET," *Journal of Networks (JNW)*, vol. 3, no. 5, pp. 13–20, 2008.

[14] P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao, and J.-L. Chen, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs," in *Proceedings of 13th International Conference on Advanced Communication Technology (ICACT)*, (Phoenix Park Gangwon-Do, Korea (South)), pp. 755 –760, Febraury 2011.

[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, (New York, NY, USA), pp. 255–265, ACM, 2000.

[16] W. Kozma and L. Lazos, "React: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in *proceedings of second ACM conference on Wireless network and Security*, (Zurich, Switzerland), pp. 103–110, 2009.

[17] A. Baadache and A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," *International Journal of Computer Science and Information Security*, vol. 7, pp. 10–16, 2010.

[18] S. Jain, M. Jain, and H. Kandwal, "Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks," *International Journal of Computer Applications*, vol. 1, pp. 37–42, February 2010.

[19] E. A. M. Anita and V. Vasudevan, "Black hole attack prevention in multicast routing protocols for mobile ad hoc networks using certificate chaining," *International Journal of Computer Applications*, vol. 1, pp. 21–28, February 2010.

[20] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "A manet routing protocol that can withstand black hole attack," in *Proceedings of the 2009 International Conference on Computational Intelligence and Security - Volume 02*, CIS '09, (Washington, DC, USA), pp. 421–425, IEEE Computer Society, 2009.

[21] S. Deswal and S. Singh, "Implementation of Routing Security Aspects in AODV," *International Journal of Computer Theory and Engineering*, vol. 2, no. 1, pp. 135–138, 2010.

[22] P. N. Raj and P. B. Swadas, "A Dynamic Learning System Against Blackhole Attack In AODV Based MANET," vol. 2, pp. 54–59, 2009.

[23] N. Jaisankar, R. Saravanan, and K. D. Swamy, "A Novel Security Approach for Detecting Black Hole Attack in MANET," *Information Processing and Management, Communications in Computer and Information Science*, vol. 70, pp. 217–223, 2010.

[24] "GloMoSim." `http://pcl.cs.ucla.edu/projects/glomosim/`. Last accessed: August 8, 2012.

[25] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A Library for Parallel Simulation of Large-scale Wireless Networks," in *Workshop on Parallel and Distributed Simulation*, pp. 154–161, 1998.