Deanship of Graduate Studies
Al-Quds University

Dynamic and Efficient Protocol for Detection and Mitigation of Multiple Black Hole Attacks in MANETs

Abdul-Rahman M. Salem

M.Sc. Thesis

Jerusalem-Palestine

1437 – 2016

Dynamic and Efficient Protocol for Detection and Mitigation of Multiple Black Hole Attacks in MANETs

Prepared By:
Abdul-Rahman M. Salem

B.Sc.: Electrical Engineering, Birzeit University, Palestine, 2000

Supervisor: Dr. Rushdi Hamamreh

A thesis Submitted to Faculty of Engineering, Al-Quds University in partial fulfilment of the requirements for the degree of Master of Electronic and Computer Engineering.

1437 – 2016

Al-Quds University
Deanship of Graduate Studies
Master of Electronics and Computer Engineering

Thesis Approval

Dynamic and Efficient Protocol for Detection and Mitigation of Multiple Black Hole Attacks in MANETs

Prepared By: Abdul-Rahman Mohammad Abdul-Aziz Salem
Registration No: 21210058

Supervisor: Dr. Rushdi Hamamreh

Master thesis submitted and accepted. Date: / 1 / 2016
The names and signatures of the examining committee members are as follows:

1- Head of Committee:	Dr. Rushdi Hamamreh	Signature: ……..…..
2- Internal Examiner:	Dr. Raid Al-Zaghal	Signature: ……..……..
3- External Examiner:	Dr. Mousa Farajallah	Signature: ……..……..

Jerusalem – Palestine

1437 – 2016

Dedication

To the loving memory of my mother as she had brought me up when I was an orphan baby (may Allah grant her His mercy).

To the loving memory of my father (may Allah grant him His mercy).

To my beloved wife, without her caring and support it would not have been possible for me to achieve this.

To my daughters and son.

To my brothers, sisters and friends.

Abdul-Rahman

Declaration

I certify that this thesis submitted for the degree of Master, is the result of my own research, except where otherwise acknowledged, and that this study (or any part of the same) has not been submitted for a higher degree to any other university or institution.

Signed……..

Abdul-Rahman Mohammad Abdul-Aziz Salem

Date: / 1 / 2016

Acknowledgments

All praise belong to ALLAH , the Almighty (swt) , the greatest of all, Lord of all creatures, the Most Gracious, the Most Merciful, for his countless graces and blessings bestowed on me throughout my life.

Peace and blessings of Allah be upon his messenger, Prophet Mohammad (SAAW).

My sincere thanks go for my supervisor Dr. Rushdi Hamamreh, for his appreciated and valuable help; indeed, his continuing directives, guidance and non-stop support motivated and helped me so much in accomplishing this thesis.

I sincerely appreciate the whole hearted cooperation and valuable help rendered by the academic instructions staff of the Faculty of Engineering at Al-Quds University.

Abstract

Mobile Ad Hoc Networks (MANETs) form a promising approach for applications that need fast installation with no infrastructure especially in disaster recovery and emergency operations. On the other hand, many challenges are facing MANETs including security, routing, transmission range, quality of service and dynamically changing topology with high nodes mobility. Many research studies have concluded that security is considered the main obstacle for the widespread adoption of MANET applications.

Security is an important challenge because MANETs are vulnerable to various attacks at all layers due to their distinguished characteristics. One of the severe attacks is the black hole attack. Black hole attack is an active attack that operates in the network layer. It is considered as a type of denial of service (DoS) attack that disrupts the services of routing layer by exploiting the route discovery process of the routing protocol. According to many research studies that focus on studying the effects of malicious attacks on network performance, the black hole attack has the worst malicious impact on network performance specially when the number of malicious nodes increases.

Several mechanisms and protocols have been proposed to detect and mitigate the effects of the black hole attack using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay.

We have proposed "Enhanced RID-AODV" to avoid and mitigate multiple black hole attacks. This protocol, which is an enhanced version of a preceding one "RID-AODV" , is based on creating *dynamic blacklists* for each node in the network. Each node, according to criteria depends on the number of mismatches of hash values of received packets as

compared with some threshold values, can decide to add or remove other nodes to or from its blacklist. The threshold is a function of mobility (*variable threshold*) to cancel the effect of normal link failure.

"Enhanced RID-AODV" was simulated and compared with other protocols for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay and overhead ratio.

بروتوكول ديناميكي لكشف تهديدات الثقوب السوداء المتعددة واستبعادها في الشبكات اللاسلكية الآنية

Dynamic and Efficient Protocol for Detection and Mitigation of Multiple Black Hole Attacks in MANETs

إعداد الطالب: عبد الرحمن سالم

إشراف: د. رشدي حمامرة

المستخلص

تتميز الشبكات اللاسلكية الآنية Mobile Ad Hoc Networks (MANETs) بمزايا فريدة تمنح هذا النوع من الشبكات إمكانيات خاصة، تجعلها الحل المناسب في بيئة لا يمكن (أو يصعب) فيها إنشاء شبكات ببنية تحتية وبشكل سريع. لذلك تستخدم في عمليات الانقاذ وفي حالات الطوارئ عند حدوث الكوارث. لكن في نفس الوقت، هذه الميزات في الشبكات الآنية تضعها أمام تحديات منها أمن المعلومات (Information Security) و بروتوكولات التوجيه (Routing Protocols) لحزم البيانات عبر الشبكة، لأن الشبكات الآنية تتشكل بطوبولوجيا ديناميكية (Dynamic Topology).

يعتبر أمن المعلومات في هذه الشبكات من أهم التحديات لأن خصائصها تجعلها عرضة للكثير من الخروقات وعرضة للتهديدات الالكترونية عليها من خلال جميع الطبقات في الشبكة (Network Layers). وتشير الدراسات والأبحاث بأن سبب عدم الانتشار الواسع لمثل هذه الشبكات يعود إلى ضعف أمن المعلومات فيها.

ومن أنواع التهديدات النشطة (Active Attack) التي تهدد أمن الشبكات الآنية، تهديد الثقب الأسود (Black Hole Attack). الذي يستهدف طبقة الشبكة (network layer)، حيث يستحوذ على عملية توجيه حزم البيانات (routing packets) لتوجيهها إلى العقدة الخبيثة (Malicious Node) وتقوم هذه العقدة بإهمال حزم البيانات التي تصلها بدل

من إعادة إرسالها لتصل إلى هدفها المقصود، مما قد يؤدي إلى حجب الخدمة في الشبكة Denial of Service (DoS). وتزداد خطورة هذا التهديد بزيادة عدد العقد الخبيثة (Malicious Nodes).

البروتوكولات المستخدمة لحل هذه المشكلة تزيد من عدد حزم البيانات التي تصل إلى هدفها ولكنها في نفس الوقت تفرض اجراءات أخرى تزيد من الأعباء على الشبكة (Overhead) وأيضاً تزيد في تأخير وصول هذه الحزم (End-to-End Delay).

تم تصميم وتطوير بروتوكول "Enhanced RID-AODV" يقوم بتحسين نقل حزم البيانات من خلال كشف واستبعاد العقد الخبيثة (Mitigating Black Holes) من مسار حزم البيانات في الشبكة الآنية، عن طريق إنشاء قوائم ديناميكية للعقد السوداء أي الخبيثة، يتم إضافة أو إزالة العقد في أو من القائمة بشكل أوتوماتيكي.

أظهر البروتوكول المقترح مقارنة مع البروتوكولات الأخرى – من خلال المحاكاة (simulation) – تفوق في زيادة Throughput، Packet Delivery Ratio وتقليل End-to-End Delay و Overhead Ratio.

Table of Contents

List of Tables

List of Figures

List of Algorithms

Chapter One

Introduction

1.1 Introduction:

Mobile Ad Hoc Network (MANET) is a self-configuring network formed by co-operating and independent nodes that connect and communicate with each other wirelessly without pre-existing infrastructure. If two mobile nodes are within each other's transmission range, they can communicate with each other directly; otherwise, the nodes in between have to forward the packet for them. So, mobile nodes are not only functioning as hosts but they are also functioning as routers [1][2]. Figure 1.1 shows a mobile ad hoc network.

Figure 1.1: Mobile Ad Hoc Network

Because MANETs are infrastructure-less networks with no centralized administration, they can be self deployed in short time. The easy deployment of nodes, self-organizing nature and freedom of mobility make MANETs suitable for a broad range of applications. They can be useful in disaster recovery and emergency operations where there is not enough time or resources to install and configure an infrastructure. They are also used in other applications; for example, in military services, maritime

communications, vehicle networks, casual meetings, campus networks, robot networks… etc [3].

On the other hand, MANETs are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network [4].

This study addresses one of the most severe attacks in MANETs, which is multiple black hole attack [5]. We propose an enhanced and modified routing protocol that is able to avoid and mitigate the effects that may come due to the existence of multiple malicious nodes that are acting as black hole nodes.

1.2 Overview of Mobile Ad Hoc Networks (MANETs):

A mobile ad hoc network (MANET) is a network of mobile nodes that are able to move arbitrarily and are connected by wireless links. It is a self-configuring network that does not require any pre-existent infrastructure such as centralized management or base stations. Because the nodes in MANET are free to move, leave, and join the network randomly due to mobility; the network topology is changing continuously [1][2].

This kind of network has the advantage of being able to be set up and deployed quickly because it has a simple infrastructure set-up and no central administration. These networks are particularly useful to those mobile users who need to communicate in situations where no fixed wired infrastructures are available. However, the salient feature of creating a network '*on the fly*' without requiring any prearranged infrastructure gave mobile ad hoc networks an appreciated interest in both industrial and military systems. The key challenges in MANETs design come from the decentralized nature, self-organization, self-management, and also the fact that all communications are carried over wireless links in short-range communication. In addition to that the topology in the network is

dynamically changed because of the high mobility nature in (MANET). Therefore, all these unique characteristics present appreciable challenges for MANETs [6][7].

In comparison with wired networks where the devices must have physical access to the network medium, MANETs have no apparent secure boundary. Besides, whilst devices used in wired networks get their electrical supply directly through available power grids, in MANET nodes are generally operated by small batteries with a limited lifetime. This makes nodes unable to perform intensive computations over prolonged periods of time. Also, Mobile ad hoc networks are highly dynamic and large scale, and they cannot be easily monitored [8].

1.2.1 Characteristics of MANETs:

MANETs have many characteristics that make them entirely different from other wireless and wired networks. Some of the key characteristics of MANETs are discussed below [2][6][7]:

1. **Dynamic Topology**:

   Nodes in MANETs are free to move arbitrarily; thus, the network topology may change randomly and rapidly at unpredictable times. Thus, the nodes can be dynamically inside and outside the network, constantly changing their links and topology, leading to change in the routing information all the time due to the movement of the nodes. Therefore, the communicated links between nodes in MANET can be bi-directional or unidirectional.

2. **Infrastructure less**:

   MANETs are formed based on the collaboration between autonomous nodes, peer-to-peer nodes that need to communicate with each other for a special purpose, without any base station, central server, or specialized hardware and fixed routers.

3. **Self-Configuring**:

   MANETs have decentralized infrastructure, with all mobile nodes functioning as routers and all wireless devices being interconnected to one another. MANETs are self-configuring networks in which network activities, including the discovery of the topology and delivery of messages, are executed by the nodes themselves.

4. **Fast Deployment**:

   The infrastructure-less nature of MANETs, makes the deployment of these networks fast and easy. This is the most desirable characteristic of MANETs that has made it widely applicable especially in cases where network is needed where no infrastructure is available such as in case of emergencies or for personal networking in remote areas.

5. **Node Mobility**:

   Mobile nodes are autonomous units in network which continuously change their position and topology independently. Due to continuous motion of nodes the topology changes frequently which means tracking down of particular node becomes difficult. The nodes can easily come out of or into the radio range of various other nodes. The routing information of nodes changes continuously as their movement becomes random.

6. **Multi-hop communications**:

   The communication in MANETs between any two remote nodes is performed by numerous intermediary nodes whose functions are to relay data-packets from one point to another. Thus, ad hoc networks require the support of multi-hop communications.

7. **Shared Physical Medium**:

   The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

1.2.2 Limitations of MANETs:

MANETs have many limitations because of their nature. Main limitations of MANETs are described as follows: [6][7][11]

1. **Bandwidth Constraints**:

   Mobile ad hoc networks are more susceptible to external noise, interference, fading and signal attenuation effects. Therefore, their bandwidth is limited because of the significantly low capacity wireless links as compared to fixed networks.

2. **Energy constraints**:

   Nodes in MANETs are generally battery-operated. The power of these small batteries is limited resulting in a limited lifetime of the nodes. The nodes may behave in a selfish manner because of the limited power supply.

3. **Resources constraints**:

   Most MANET devices are small hand-held devices. These devices indeed have limitations because of their restricted nature; they are often have small processing and storage facilities.

4. **Limited physical security**:

   Mobility implies higher security risks such as peer-to-peer network architecture or a shared wireless medium accessible by both legitimate network users and malicious attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.

5. **Lack of Centralized Management**:

   Nodes in MANETs operate in a distributed manner without any centralized control by a network administrator. Lack of centralized control in MAENTs can influence several operational aspects of the network. This property leads to the issues of organizing and managing these networks. Lack of centralized control makes monitoring and detection of attacks a challenging issue.

1.2.3 Applications of MANETs:

All nodes in MANETs are mobile and the topology is dynamic. These self-configuring networks that do not require a fixed infrastructure can be applied anywhere where there is no communication infrastructure or installing infrastructure is expensive or inconvenient [2][7].

The following are the main domains for mobile ad hoc network applications: [2][6][7][9]

1. **Emergency services**:

   A mobile ad hoc network is most suitable to provide emergency services applications, such as search and rescue operations in disaster recovery, where the entire communication infrastructure is destroyed and establishing a network for communication quickly is crucial. Using a mobile ad hoc networking technology, where a network could be set up in hours instead of weeks. In emergencies caused by natural disasters such as earthquakes, fires and floods ad hoc networking technology provides a quick and easy way to connect police, firemen, ambulance, medical staff and other independent teams to perform rescue operations.

2. **Commercial Applications**:

   Possible application scenarios of MANETs in commercial areas include e-banking, e-commerce and business applications. For example, Electronic payments from

anywhere such as communication dispatch systems for taxi in a town are used to inform individual taxis about passenger pickups, route directions, weather conditions etc. Although taxi networks has central point from where the communications to individual taxis takes place, this communication dispatch system of taxis works in an ad hoc manner.

3. **Educational Applications**:

   MANETS can be used to setup virtual classrooms or conference rooms. Also, they can be used to setup ad hoc communication during conferences, meetings, or lectures.

4. **Collaborative Applications**:

   For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a certain given project.

5. **Entertainment**:

   MANETs help a lot in entertainment, for example, multi-user gaming, robotic pets, and theme parks.

6. **Military battlefield**:

   MANETs can be used in the military to maintain an information network between the soldiers, vehicles and their headquarters.

7. **Personal Area Networking (PAN)**:

   It is a communication network of personal devices such as computers, personal digital assistant (PDAs), telephones and notepads. These devices can form an ad hoc network to communicate and achieve other networking facilities using either WLAN or Bluetooth.

1.2.4 Security Requirements in MANETs:

The major security requirements of MANETs are secure linking, secure routing and secure data transmission or secure data packet forwarding. The task of providing security in the MANET network is a key matter in order to protect the data that are exchanged between the nodes. It is necessary to find security solutions for MANET network where security services exist. These *security services* are a fundamental requirement in security solutions in MANET network [10][11][12]:

1. **Confidentiality:** Confidentiality means that Information access is possible only for nodes that have been authorized to access it. Any information or data should never be disclosed to any unauthorized parties.
2. **Integrity:** Integrity provides protection of message data during transmission. Integrity can be compromised mainly in two ways: malicious altering and accidental altering. A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering. On the other hand, accidental altering may happen when the message is lost or its content is changed due to some benign failures, which might be transmission errors in communication or hardware errors such as hard disk failure.
3. **Availability:** A node should maintain its ability to provide all the designed services regardless of its security state. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service.
4. **Non-repudiation:** Non repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. This is

useful especially when it's needed to discriminate if a node with some abnormal behavior is compromised or not.

5. **Authentication:** Authentication is an essential assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.
6. **Authorization:** Authorization is a mechanism for defining the powers to gain access to certain resources, that is, control over how to access the network. Authorization is generally used to assign different access rights to different levels of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore, there should be an authorization process before the network administrator accesses the network management functions.
7. **Anonymity:** Anonymity means that all the personal information that can be used to identify the owner or the current user of the node should by default be kept private and not to be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

1.2.5 MANETs Vulnerabilities:

Vulnerability is a weakness in security system. MANETs suffer from all the vulnerabilities that their wired counterparts encountered. Some of these vulnerabilities are aggravated in a wireless context due to the characteristics of MANETs, such as the lack of a clear line of

defense and the in-the-air communications. Besides, ad hoc networks are susceptible to vulnerabilities that are inherent to wireless networks, which reside in their routing and auto-configuration mechanisms [13].

Some of the vulnerabilities on ad hoc networks are [11][14]:

1. **Lack of centralized management:** The absence of centralized management in MANETs makes the detection of attacks difficult; because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network.
2. **Resource availability:** Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad hoc environments also allow implementation of self-organized security mechanism.
3. **Scalability:** Due to mobility of nodes, scale of ad hoc network is changing all the time. So, scalability is a major issue concerning security. Security mechanism should be capable of handling large networks as well as small ones.
4. **Cooperativeness:** Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.
5. **Dynamic topology:** Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.
6. **Limited power supply:** The nodes in mobile ad hoc networks need to consider restricted power supply, which will cause several problems. A node in a mobile ad

hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

7. **Bandwidth constraint:** Variable low capacity links exist as compared to wireless networks which are more susceptible to external noise, interference and signal attenuation effects.
8. **Adversary inside the Network:** The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus, this attack is more dangerous than the external attack. Those nodes are called compromised nodes.
9. **No predefined Boundary:** In mobile ad- hoc networks, a physical boundary of the network cannot be precisely defined. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.
10. **Wireless Links:** As the nodes in such networks are interconnected through wireless interface that makes it highly susceptible to link attacks. The bandwidths of wireless networks are less as compared to wired networks, which attracts many attackers to prevent normal communication among nodes.

1.2.6 Security Challenges in MANETs:

The unique characteristics of MANETs, such as absence of infrastructure, rapid and unpredictable change of topology, open and shared wireless medium, and stringent resource constraints, have posed nontrivial challenges to security designs. Table 1.1 summarizes those challenges [13]:

Table 1.1: Security Challenges in MANETs

Characteristics	Security Challenges
Open shared medium	Makes an ad hoc network susceptible to attacks such as eavesdropping, signal jamming, impersonation, message distortion and message injection.
Absence of infrastructure and frequent change of topology and membership	Raises the probability of a network to be compromised. MANETs don't have dedicated routers to form a clear line of defense where traffic monitoring or access control mechanisms can be deployed. In addition, each mobile node is functioning as a router and participating in routing and packet forwarding processes; so, a malicious node en route can tamper the routing and data packets.
Constraints of resources (such as power, bandwidth, CPU capacity and memory)	Security mechanisms must be lightweight in terms of communication overhead, computation complexity and storage overhead. Asymmetric cryptography is usually considered too expensive for MANETs. Therefore, symmetric cryptographic algorithms and one-way functions are commonly used to protect data integrity and confidentiality.
An ad hoc network may consist of a great number of nodes	Renders scalability

The security mechanisms or approaches should be adapted to the characteristics of MANETs. The security solutions for MANETs should accommodate the following needs [15][16]:

1. The security solution should spread across many individual components and rely on their collective protection power to secure the entire network. The security scheme adopted by each device has to work within its own resource limitations in terms of computation capability, memory, communication capacity and energy supply.

2. The security solution should span different layers of the protocol stack, with each layer contributing to a line of defense. No single-layer solution is possible to thwart all potential attacks.
3. The security solution should thwart threats from both outsiders who launch attacks on the wireless channel and network topology, and insiders who sneak into the system through compromised devices and gain access to certain system knowledge.
4. The security solution should encompass all three components of prevention, detection and reaction, that work in concert to guard the system from collapse.
5. The security solution should be practical and affordable in a highly dynamic and resource constrained networking scenario.

1.3 Research Methodology:

This research depends on studying previous work and examining the existing used mechanisms by checking their effectiveness in mitigating the effects of the malicious nodes and in preventing the denial of service by checking the performance metrics. Then, the proposed protocol was implemented and developed to be tested and compared with other protocols with the similar purposes.

In this research, we adopted the ns-2 simulator because it is considered in many research studies in the field; it is an open source simulator and does not require any licenses.

1.4 Motivation:

Mobile Ad Hoc Networks (MANETs) have special characteristics that make them distinguished from other wireless and wired networks. These characteristics make MANETs a promising technology in a wide range of applications in many domains. However, in the same time, these characteristics also make MANETs vulnerable to several attacks making security a major challenge in MANETs. Researcher found that security is

the main obstacle for the widespread adoption of MANET applications as in [4][17][18]. One of the severe attacks in MANETs is the black hole attack which is an active attack that operates in the network layer. This attack becomes more severe when multiple nodes in the network are acting together as black hole nodes.

In multiple black hole attacks, the malicious nodes provide fresh routes that make other legitimate nodes use these malicious nodes in their routes, and then they drop the legitimate traffic of the network resulting in a very low throughput and packet delivery ratio.

Many Several mechanisms and protocols have been proposed to detect and mitigate its effect using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay.

This motivates us to try to provide a solution to multiple black hole attacks in MANET. In this study, we propose an enhanced and modified routing protocol that is dynamic and able to avoid these multiple malicious nodes and mitigate its effects. This dynamic and efficient protocol provides not only an increase in throughput and packet delivery ratio but also a decrease in end-to-end delay and overhead ratio, which are very important performance metrics in MANETs.

1.5 Black Hole Threat Model:

The black hole attack is considered as:

- Active attack: it has modification and dropping behavior.
- Operates in the network layer.
- Interrupts the route discovery process.

- Kind of denial of service attack where it will disrupt the network and the result affects the whole performance of the network.

The attack is made by malicious node which attacks the control message of the routing protocols such as AODV. The diagram in Figure 1.2 is the attack model on how the malicious node M pretends to be a node with attractive route to the destination node D. Upon receiving the RREQ message from node 3, node M immediately generates RREP message and sends it to source node S. In large networks, there is a possibility to have more than one reply of RREP massage.

In order to be favoured against others, the destination sequence number sent by node M is normally higher and it is sent ahead of the rest. Characteristic of AODV will make node S to believe that the first RREP received (through node 3) is the shortest and most up-to-date path to destination node D. As a result, node S updates its routing table by taking node 3 as its next hop to send out data to node D. Node 3 with infected route entry forwards the data packet to node M. Node M either keeps or drops the packet without forwarding it to the destination node D as if the packet is disappeared in a black hole as the attack name implies.

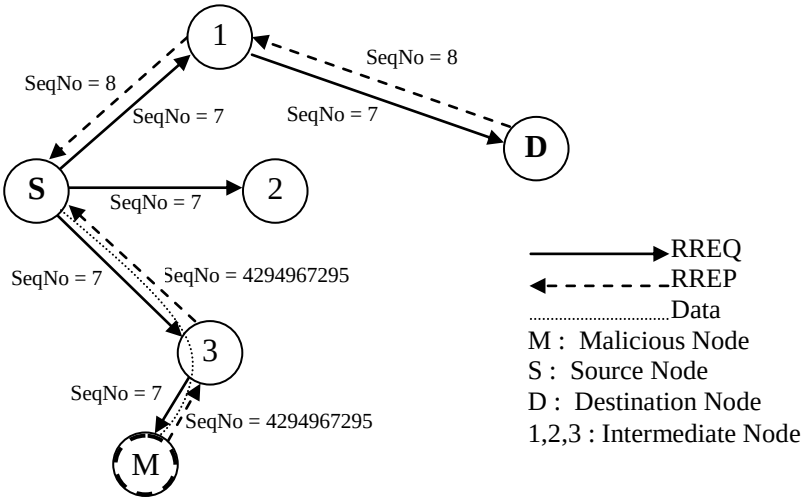

Figure 1.2: Black Hole Attack Model in AODV

1.6 Problem Statement:

The participating nodes of MANETs are independent, mobile and don't have a centralized and organized network infrastructure. Hence, nodes act as routers and are free to move randomly; thus, the network topology changes rapidly and unpredictably. Therefore, MANETs use a peer-to-peer multi-hop routing instead of a static network infrastructure to provide network connectivity.

Routing protocols in Mobile Ad Hoc Networks by their nature are distributed routing protocols with the assumption that all nodes in the network will cooperate truly and participate honestly. However, the existence of malicious nodes makes this assumption untrue. Such nodes may drop the packets, if they are not the destination, without forwarding them or may disrupt the routing discovery and maintenance processes resulting in abnormal network operation that affects the performance of the network and may cause denial of service [5].

A black hole attack is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them (drop all packets) without forwarding them to the destination [19].

In reactive routing protocols such as AODV, the destination sequence number (*dest_seq*) is used to describe the freshness of the route. A higher value of *dest_seq* means a fresher route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new *dest_seq* number larger than the current *dest_seq* number. In this way the intruder becomes part of the route to that destination [20].

The problem of a black hole has two properties: First, the node exploits the ad hoc routing protocol to advertise itself as having a valid route to a destination, even though the

route is spurious with the intention of intercepting packets. Second, the node consumes the intercepted packets; a black hole node absorbs the network traffic and drops all packets.

As a result, the black hole attack has a severe impact in decreasing the network throughput and packet delivery ratio. Besides, the existence of multiple black hole nodes increases the severity of this attack resulting in a denial of service problem.

1.7 Research Objectives:

The objective of this thesis is to provide security for mobile ad hoc networks (MANETs). There are two main security needs in MANETs: First is to protect the data transmission and second to make the routing protocol secure. The second one may be not an issue in the centralized networks; but in MANETs, this issue arises because the nodes are not only hosts but also routers. In this research, we are focusing on making routing protocols more secure to prevent malicious nodes from disrupting the routing process and dropping the packets resulting in denial of service (DoS) attack.

1.8 Research Hypothesis:

- In this research, we assume that the intermediate nodes are moving randomly and sending packets among them randomly too.
- Malicious nodes (the black hole nodes) are part of the intermediate nodes that were compromised with malicious software making them to behave abnormally but they carry out the black hole tasks.
- Any intermediate node in the MANET can be a black hole node.
- The normal nodes are using the Ad hoc On-demand Distance Vector (AODV) routing protocol.
- AODV was adopted in this research because of several reasons:

- It is a reactive (on-demand) routing protocol. AODV doesn't maintain network topology at each node and no periodic route updates like proactive routing protocols. However, It finds route whenever needed.
- It is table-based routing not a source-based like DSR, in which each packet carries the complete routing information for its destination in its header.
- AODV is robust since it uses flooding for route discovery; thus, it does not require mobility to be synchronized [21].

1.9 Thesis Contributions:

Information security is one of the most important challenges in MANETs, especially securing the routing processes; because the nodes themselves are responsible for routing and forwarding data packets traversing across the network. Malicious nodes can misroute or drop packets to decrease the performance of the network and increase the delay in delivering these packets, resulting in a denial of service. We have done the following:

- We have designed and developed an enhanced protocol "Enhanced RID-AODV" that is able to detect and mitigate multiple malicious nodes that are acting as black hole nodes in MANETs.
- We have designed and developed a *dynamic* mechanism to automatically blacklist or delist malicious nodes with threshold as function of mobility (*variable threshold)* to cancel the effect of normal link failure (which is not a malicious behavior).
- "Enhanced RID-AODV" also provides a full path (bi-directional) integrity check for the routing control packets.
- "Enhanced RID-AODV" is *lightweight* because it maintains only a limited number of counters and requires minimum processing requirements.

- We verified the performance of "Enhanced RID-AODV" by simulation and comparing with RID-AODV, RAODV, IDSAODV and AODV.

1.10 Literature Review:

Some research studies in the literature have focused on studying the effect of malicious nodes on network performance only without providing any solutions. However, several mechanisms and protocols using different strategies have been proposed to protect MANETs against black hole attacks. Ashok Kanthe et al. studied the effect of malicious attacks in mobile ad hoc networks including black hole attack, packet drop attack and gray hole attack on AODV protocol under different performance metrics: throughput, packet drop rate and end-to-end delay. It was found that the black hole attack is more dangerous than other attacks mentioned in this paper [22].

Imad Aad et al. provided a quantitative study of the performance impact and scalability of DoS attacks in ad hoc networks. They have also considered the black hole attack, as its impact in ad hoc networks. The authors considered the following as critical performance measures for a system under attack: total system throughput and probability of interception in addition to the system fairness measures and the mean number of hops for a received packet. The simulation results for the impact of black hole node showed that the system has high fairness index with no black hole in the network [23].

Dinesh Mishra et al. analyzed the effects of black hole attack in mobile ad hoc network using AODV and DSR routing protocols. The authors considered the throughput as the main performance measure. Simulation results, by NS-2 simulator, showed that a higher data packet loss when using DSR as compared to AODV. The observation and results showed that DSR data loss is around 55%- 60% in the presence of black hole attack, while 45%-50% in the AODV routing. AODV protocol provides better

performance than the DSR in the presence of black holes with minimal additional delay and overhead [24].

Elmar Gerhards-Padilla et al present a novel centralized intrusion detection approach for detecting routing attacks in tactical MANETs called Topology Graph based Anomaly Detection (TOGBAD). It was developed against the Optimized Link State Routing protocol (OLSR) protocol. Firstly, a topology graph is created and the number of neighbors of a node according to this topology graph is calculated. Secondly, the number of neighbors a node claims to have in its HELLO messages is determined. Finally, the originator's number of neighbors according to the message is checked for plausibility against the number of neighbors according to the topology graph. A significant difference between the two values triggers an alarm. With this approach, it is possible to detect the attempt to create a black hole before the actual impact occurs [25].

Sonja Buchegger and Jean-Yves Le Boudec proposed a robust reputation system for misbehaviour detection in mobile ad hoc networks. Nodes have a monitor for observations, reputation records for first-hand and trusted second-hand observations about routing and forwarding behaviour of other nodes, trust records to control trust given to received warnings, and a path manager to adapt their behaviour according to reputation and to take action against misbehaved nodes. Nodes monitor their neighbours and change the reputation accordingly. When the reputation rating is bad, they take action in routing and forwarding. The routes containing the misbehaved node are either reranked or deleted from the path cache. In addition, once a node has detected a misbehaved node, it informs other nodes by sending an ALARM message [26].

Hongmei Deng et al. proposed a method to solve the black hole problem. This method is to disable the ability of an intermediate node to reply in a RREP message, so all

reply messages should be sent out only by the destination node. This method increases the routing delay, especially for a large network. Besides, a malicious node can take advantage by fabricating a reply message claiming it was sent from the destination node. Another solution was proposed in this paper that depends on using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it's not exists, the reply message from the intermediate node is discarded and an alarm message to the network is sent out. Using this method, the black hole problem was avoided, and further malicious behavior was also prevented. This method can't prevent multiple black hole attacks [27].

Seungjoon Lee et al. proposed a method to avoid Black Hole attack based on introducing additional route confirmation messages: Route Confirmation Request (CREQ) and Route Confirmation Reply (CREP). In the proposed method, the intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and confirmation message, the source determines the validity of path according to its policy. Simulation results show remarkable improvement in 30% higher delivery ratio. Its drawback is that it can't detect multiple Black Hole attacks and the control messages have been increased [28].

Satoshi Kurosawa et al. proposed an anomaly detection scheme for black hole nodes using dynamic training method in which the training data is updated at regular time intervals. The considered the destination sequence number in order to detect this attack. In normal state, sequence number changes depending on its traffic conditions and the destination sequence number tends to rise monotonically when the number of connections increases. However, during the attack, the sequence number is increased largely. A statistical method is applied for detection of black hole that is based on the difference between destination sequence numbers of received RREPs. The simulation results of this

method showed significant effectiveness in detecting the black hole attack as compared with conventional scheme. Through the simulation, our method shows significant effectiveness in detecting the black hole attack [20].

The solution proposed by Arun Raj Kumar and S. Selvakumar, focuses on the requirement of a source node to wait unless there is arrival of RREP packet from more than two nodes. When it receives multiple RREPs the source node checks that there is any share hops or not. The source node will consider the route safe if it finds the share hops. Its drawback is the introduction of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of node [29].

Durgesh Wadbude and Vineet Richariya proposed an approach that uses improved security mechanisms to be introduced in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. The performance of these two protocols (SAODV and ARAN) was tested in simulation and their communication costs were measured using the ns-2 simulator, which is suitable for the present purpose. The evaluation metrics used in this study were overhead and end-to-end delay. The results show good performance [30].

Lalit Himral et al. introduced a method to find the secured routes and prevent the malicious nodes (black hole nodes) in the MANETs by checking whether there is a large difference between the sequence number of source node or intermediate node that has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the Route Reply Table (RR-Table). Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, then it

is surely from the malicious node, immediately removes that entry from the RR-Table. The proposed method cannot find multiple black hole nodes [31].

Elhadi Shakshuki et al. proposed and implemented a new intrusion detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to modern approaches, EAACK demonstrates privileged malicious behavior detection rates in definite situations while it does not greatly affect the network performances. The demonstrated results show positive performances [32].

A lightweight routing protocol IDSAODV was proposed by S. Dokurer et al. in [33] as a solution for black hole attack problem in MANETs. The authors manually analyzed the output file obtained from simulation and found out very soon after the first RREP from the destination node a second RREP arrived at the source node. Through simulation, they found out that the first RREP was from the black hole node and the second RREP was from the intended destination. At this point, for future simulations, they assumed that the first RREP would always be from black hole node and modified the AODV protocol to ignore the first RREP and send using second RREP route. A RREP caching mechanism to count the second RREP message was added to aodv.cc file in NS-2 [33].

The simulation results demonstrate that IDSAODV improved the PDR in a MANET with a single black hole node; thus, proving the successful implementation of the route caching mechanism [33].

Many of the proposed solutions that make the route establishment process longer while the nodes are moving are facing from the link failure problem. Om Shree and Francis Ogwu in [34] addressed this issue by getting advantage of the reverse AODV (RAODV) routing protocol proposed by Chonggun Kim et al. in [35]. RAODV discovers route using

reverse route discovery procedure where the destination node sends reverse-route request (R-RREQ) messages to its neighbors to find a valid route to the source node after receiving RREQ from source node. Their simulation results of RAODV show that it does improve the performance of AODV in metrics such as packet delivery ratio (PDR), end-to-end delay, and energy consumption [34][35].

Although RAODV has not been designed to prevent black hole attacks and it was developed with the aim of solving path failure problem, Om Shree and Francis Ogwu proposed in [34] to use it in mitigating the effects of black hole attacks in ad hoc networks. Therefore, they proposed RID-AODV protocol that combines RAODV (proposed in [35]) and IDSAODV (proposed in [33]) to withstand multiple black hole attacks in client-based WMNs [34].

1.11 Thesis Organization:

The rest of the thesis is organized as follows:

This thesis addresses a network layer attack that exploits the routing discovery process. Hence, in chapter 2 routing protocols in MANETs are discussed in details. This includes the classifications of the routing protocols in MANETs. In addition to description of the main protocols and a performance comparison is provided in this chapter.

Chapter 3 is about security attacks in MANETs. It provides classification of security attacks and classification of security attackers in MANETs. A special section in this chapter has been added to address the black hole attack in details and to provide a behavioural analysis of this attack.

In chapter 4, we present the proposed protocol (Enhanced RID-AODV). It is an enhanced version of a preceding one, so we provide how we got advantages from that

preceding protocol and what are the enhancements in this protocol. The chapter ends with pseudocodes for the proposed protocol.

Chapter 5 is about the simulation and results. It starts with introducing the used simulation tools in this research and a description of the network environment considered for simulation. Then the performance metrics that were considered in this research are provided. After that, the results of the simulation for all scenarios are provided and finishing with analysis of these results.

Chapter 6 provides the conclusion of this thesis and suggests future work in the same field.

Chapter Two

Routing Protocols in MANETs

2.1 Introduction:

Wireless networking paradigms can be classified into two classes: wireless ad hoc and cellular networking according to their dependence on fixed infrastructures. In an infrastructure mobile network, mobile nodes have wired access points (or base stations) within their transmission range. The access points compose the backbone for an infrastructure network. In contrast, in the ad hoc networking paradigm there is no fixed infrastructure and packets are delivered to their destinations through wireless multi-hop connectivity. In a mobile ad hoc network, nodes move arbitrarily; therefore, the network topology changes unpredictably. Every node in mobile ad hoc networks has the responsibility to act not only as hosts but also as routers. [37][60].

Routing protocols for wired networks assume stable topology and link state; this makes them not suitable for MANETs. Therefore, research efforts have been made to develop efficient routing protocols for MANETs [43].

The following section addresses the routing protocols and their classifications. Then a comparison between these routing protocols is discussed.

2.2 Classifications of Routing Protocols in MANETs:

Appropriate Classification methods for routing protocols are required to help researchers and designers to study, compare and analyze mobile ad hoc routing protocols in order to understand distinct characteristics of a routing protocol and find its relationship with others. These characteristics mainly are related to the information exploited for routing, when this information is acquired, and the roles that nodes may take in the routing process [36].

There are several methods to distinguish mobile ad hoc network routing protocols in order to classify them. One of the most popular methods of them is based on how routing information is acquired and maintained by mobile nodes. Using this method, mobile ad hoc network routing protocols can be divided into *proactive* routing, *reactive* routing, and *hybrid* routing.

Another classification method is based on the roles which nodes may have in a routing scheme. In a uniform routing protocol, where the network structure is *flat*, all mobile nodes have the same role, importance, and functionality. However, in nonuniform routing protocols, some nodes carry out some management or routing functions. Normally, distributed algorithms are exploited to select those special nodes. Nonuniform routing approaches are related to *hierarchical* network structures to facilitate node organization and management.

According to the abovementioned methods that distinguish routing protocols in MANETS, figure 2.1 shows the classification of the routing protocols according to network structure in MANETs [38][39][40].

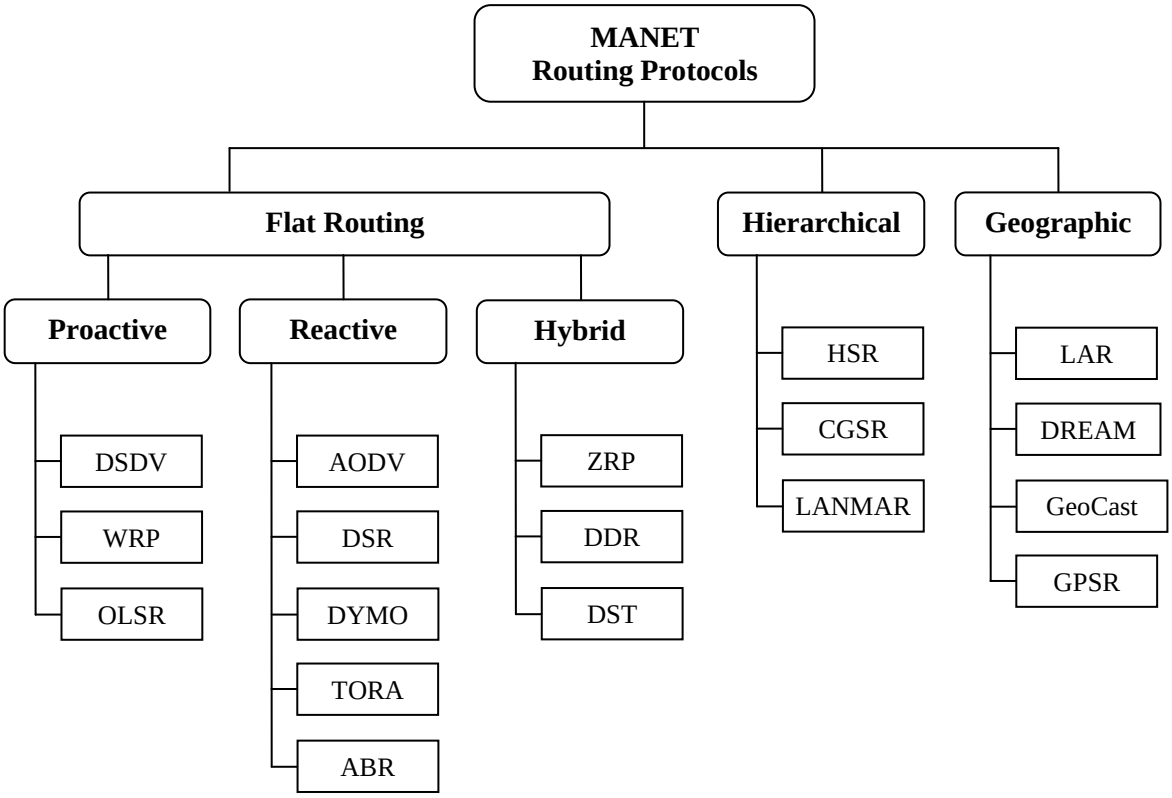

Figure 2.1: Classification of the routing protocols in MANETs

2.2.1 Proactive Routing Protocols:

Proactive routing protocols are also known as *table driven* routing protocols. They are conventional routing protocols based on either link-state or distance vector principles. In this routing protocol every node maintains complete information about the network topology. Whenever the network topology changes the routing table is updated automatically. Periodic route updates are exchanged in order to synchronize the tables. Thus, when there is a need for a route to a destination, such route information is available immediately. As they need to keep node entries for each and every node in the routing table of every node therefore these protocols are not appropriate for usage in large networks. Proactive routing protocols maintain different number of routing tables varying

from protocol to protocol. Some popular proactive routing protocols are: DSDV, GSR, OLSR, WRP etc [39][41].

2.2.2 Reactive Routing Protocols:

Reactive Routing Protocols are also known as *on-demand* routing protocols. The major goal of reactive routing protocols is to minimize the network traffic overhead. These protocols are based on Query-Reply topology in which they do not attempt to continuously maintain the up-to-date topology of the network. When a route is desired, a procedure is invoked to find a route to the destination node by initiating route discovery process. The route request packets are flooded by using flooding technique throughout the network for route discovery. These protocols require a route discovery and route maintenance process [39][42].

The common element in reactive protocols is the mechanism used for discovering routes. The source node emits a request message, requesting a route to the destination node. This message is flooded, i.e. relayed by all nodes in the network, until it reaches the destination. The path followed by the request message is recorded in the message, and returned to the sender by the destination, or by intermediate nodes with sufficient topological information, in a reply message. Thus multiple reply messages may result, yielding multiple paths of which the shortest is to be used [41].

2.2.3 Hybrid Routing Protocols:

Hybrid routing protocols are protocols that are both proactive and reactive in nature. These protocols are designed to increase scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads. In hybrid routing protocols, a proactive method is employed to maintain routes for nearby nodes; a reactive or route discovery method is used for faraway nodes. Most hybrid

protocols are zone based, which means that the network is partitioned or seen as a number of zones by each node [36].

2.2.4 Hierarchical Routing Protocol:

Hierarchical Routing is multilevel clustering of mobile nodes. Routing protocols for mobile ad hoc networks utilize hierarchical network architectures. The proper proactive routing and reactive routing approach are dominated in different hierarchical levels. In case of a route failure the entire route does not need to be recalculated. These networks address the scalability [39].

The most popular way of building hierarchy is to group nodes that are close to each other into explicit clusters. Each cluster has a leading node (*clusterhead*) to communicate to other nodes on behalf of the cluster. An alternate way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. More efficient overall routing performance can be achieved through this flexibility [40].

2.2.5 Geographical Routing Protocols:

The availability of global positioning system (GPS) or similar locating systems allows mobile nodes to access *geographical* information easily. During forwarding operations, geographical Routing Protocols (also known as *location-aware* routing protocols) use the nodes position provided by GPS systems or other mechanisms. In location-based routing protocols, the distance between a packet forwarding node and the destination, along with the node mobility, can be used in both route discovery and packet forwarding. Specifically, a node selects the next hop for packets forwarding by using the physical position of its one-hop neighbours and the physical position of the destination node [36][42].

2.3 Main Routing Protocols in MANETs:

In this section, we discuss the main and common used routing protocols in MANETs. It includes the following protocols: Destination-Sequenced Distance-Vector Routing (DSDV), Optimized Link State Routing Protocol (OLSR), Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Dynamic MANET On-demand (DYMO).

2.3.1 Destination-Sequenced Distance-Vector Routing (DSDV):

The DSDV protocol is a table driven algorithm. In routing tables of DSDV, an entry stores the next hop toward a destination, the cost metric for the routing path to the destination, and a destination sequence number that is created by the destination. Sequence numbers are used in DSDV to distinguish stale routes from fresh ones and avoid the formation of route loops [36][38].

The route updates of DSDV can be either time driven or event driven. In order to keep the routing table completely updated at all the time each device periodically broadcasts routing message to its neighbor devices. When a neighbor device receives the broadcasted routing message and knows the current link cost to the device, it compares this value and the corresponding value stored in its routing table. If changes were found, it updates the value and re-computes the distance of the route which includes this link in the routing table. On the other hand, when a significant change occurs from the last update, a node can transmit its changed routing table in an event-triggered style [36][41].

Advantages of DSDV:

- DSDV is an efficient protocol for route discovery.
- Route discovery latency is very low.

- Loop-free paths are guaranteed in DSDV.

Disadvantages of DSDV:

- To maintain network topology at each node, DSDV needs to send a lot of control messages.
- DSDV generates a high volume of traffic for high-density and highly mobile networks.

2.3.2 Optimized Link State Routing Protocol (OLSR):

Optimized Link State Protocol is a point-to-point table-driven, proactive protocol developed for mobile ad hoc networks, that is, it exchanges topology information with other nodes of the network regularly. OLSR employs an efficient link state packet forwarding mechanism called multipoint relaying. It optimizes the pure link state routing protocol. Each node maintains the topology information about the network by periodically exchanging link-state messages among the other nodes. Each node selects a set of its neighbor nodes as "multipoint relays" (MPR). A node selects MPRs from among its one-hop neighbors with "symmetrical" (i.e., bidirectional) linkages. Therefore, selecting the route through MPRs automatically avoids the problems associated with data packet transfer over unidirectional links. In OLSR, only nodes, selected as such MPRs, are responsible for forwarding control traffic, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required [36][41].

Optimizations in OLSR are done in two ways:

- By reducing the size of the control packets.
- Reducing the number of links used for forwarding the link state packets [41].

Advantages of OLSR:

- OLSR makes routes immediately available when needed due to its proactive nature.
- Best suitable for high density network and does not allows long delays in the transmission of the packets.

Disadvantages of OLSR:

- OLSR needs more time rediscovering a broken link.
- OLSR needs that each node periodically sends the updated topology information throughout the entire network, this increase the protocols bandwidth usage. But the flooding is minimized by the MPR's.

2.3.3 Ad Hoc On-Demand Distance Vector (AODV):

Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol which initiates a route discovery process only when it has data packets to transmit and it does not have any route path towards the destination node, that is, route discovery in AODV is called as on-demand [44][45].

AODV routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols [46].

The protocol consists of two phases: Route Discovery and Route Maintenance. AODV nodes can send four types of messages to communicate among each other. Route Request

(RREQ) and Route Reply (RREP) messages are used for route discovery. Route Error (RERR) messages and HELLO messages are used for route maintenance [47].

A. Route Discovery in AODV:

AODV discovers routes as needed basis via a similar route discovery process. AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers [45].

Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks whether it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. The route discovery process is shown in figure 2.2 below [48].

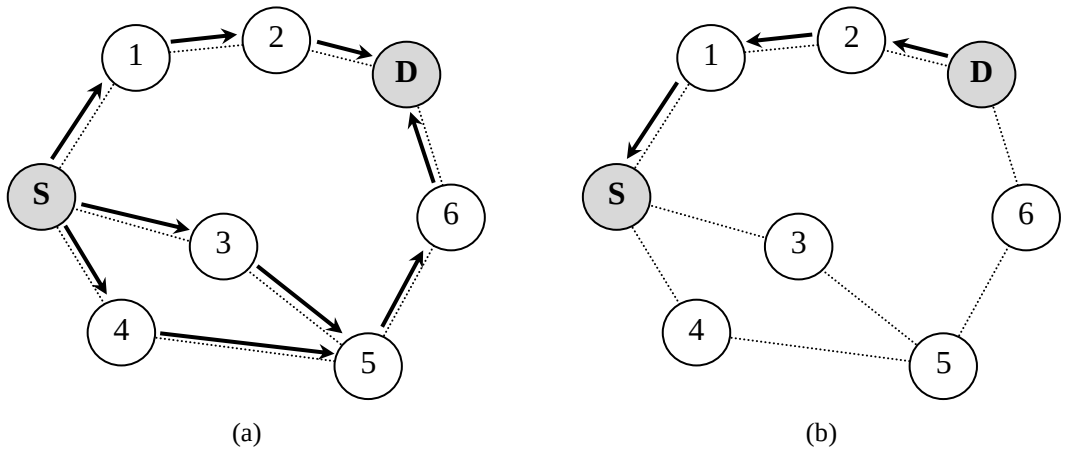

Figure 2.2: AODV route discovery process. (a) Propagation of the RREQ (b) Path of the RREP to the source

The RREQ contains the following fields:

<source_addr, source sequence#, broadcast id, dest_addr, dest sequence#, hop cnt>

The pair *<source_addr, broadcast_id>* uniquely identifies an RREQ. *broadcast_id* is incremented whenever the source issues a new RREQ. Each neighbor either satisfies the RREQ by sending a Route REPly (RREP) back to the source, or broadcasts the RREQ to its own neighbors after increasing the *hop_cnt*. Notice that a node may receive multiple copies of the same route broadcast packet from various neighbors. When an intermediate node receives an RREQ, if it has already received an RREQ with the same *broadcast_id* and source address, it drops the redundant RREQ and does not rebroadcast it [36].

B. Route Maintenance in AODV:

The second phase of the protocol is called route maintenance. It is performed by the source node and can be subdivided into: i) source node moves: source node initiates a new route discovery process, ii) destination or an intermediate node moves: a route error message (RERR) is sent to the source node. Intermediate nodes receiving a RERR update their routing table by setting the distance of the destination to infinity. If the source node receives a RERR it will initiate a new route discovery. To prevent global broadcast messages AODV introduces a local connectivity management. This is done by periodical exchanges of so called HELLO messages which are small RREP packets containing a node's address and additional information [47]. Route maintenance process is shown in figure 2.3 below [45].

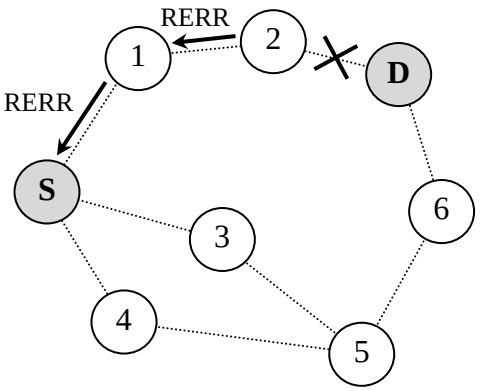

Figure 2.3: AODV route maintenance process

Advantages of AODV:

- AODV is adaptable to dynamic networks
- AODV creates routes only on demand, which greatly reduces the periodic control message overhead associated with proactive routing protocols.
- AODV is a loop free protocol and avoids the counting-to-infinity problem

Disadvantages of AODV:

- There is route setup latency when a new route is needed.

2.3.4 Dynamic Source Routing (DSR):

Dynamic Source Routing (DSR) is an Ad Hoc routing protocol based on the theory of source-based routing rather than table-based. This protocol uses source routing in which each packet carries the complete routing information for its destination in its header. This protocol is source initiated. This is particularly designed for use in multi hop wireless ad hoc networks of mobile nodes. Basically, DSR protocol does not need any existing network infrastructure or administration. This allows the network to be completely self-organizing and self-configuring [49][54].

This protocol is composed of two essential parts of route discovery and route maintenance.

A. Route Discovery in DSR:

During the route discovery mechanism the DSR accumulate the address of each device coming between the source and the destination. The process of route discovery is work as follow. If a source has route of the destination in its cache it utilize that route otherwise a route discovery protocol starts. The source node sends a Route Request packet by flooding the network. If the node receive the Route request is intended destination it returns Route reply to the source. The Route reply contains the list of best path form the source to destination. When the source receives this route reply packet it updates its route cache for sending further data. However if the node that receive the Route request is not a intended receiver it again forward the route request to its neighbor except the source also adding its address in the Route Request packet as illustrated in figure 2.4 [38].

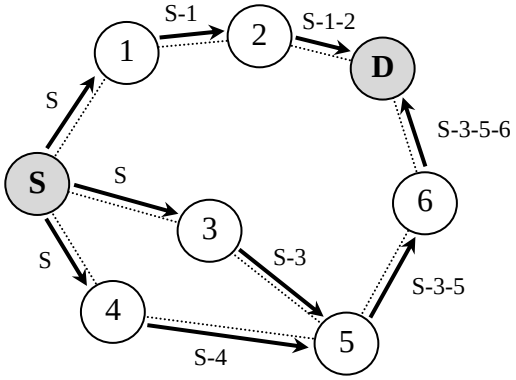

Figure 2.4: Route discovery in DSR

During the route discovery process, the route record field is used to contain the sequence of hops which already taken. Initially, all senders initiate the route record as a list with a single node containing itself. The next intermediate node attaches itself to the list and so on. Each route request packet also contains a unique identification number called as *request_id* which is a simple counter increased whenever a new route request packet is being sent by the source node. So each route request packet can be uniquely identified through its initiator's address and *request_id*. When a node receives a route request packet,

it is important to process the request in the following given order. This way we can make sure that no loops will occur during the broadcasting of the packets [44].

- If the pair < *source node address, request_id* > is found in the list of recent route requests, the packet is discarded.
- If the host's address is already listed in the request's route record, the packet is also discarded. This indicates removal of same request that arrive by using a loop.
- If the destination address in the route request matches the host's address, the route record field contains the route by which the request reached this host from the source node. A route reply packet is sent back to the source node with a copy of this route.
- Otherwise, add this node's address to the route record field and re-broadcast this packet.

A route reply is sent back either if the request packet reaches the destination node itself, or if the request reaches an intermediate node which has an active route to the destination in its route cache. The route record field in the request packet indicates the sequence of hops which was considered. If the destination node is generating the route reply, it just takes the route record field of the route request and puts it into the route reply. If the responding node is an intermediate node, it attaches the cached route to the route record and then generates the route reply as shown in figure 2.5 [41][54].

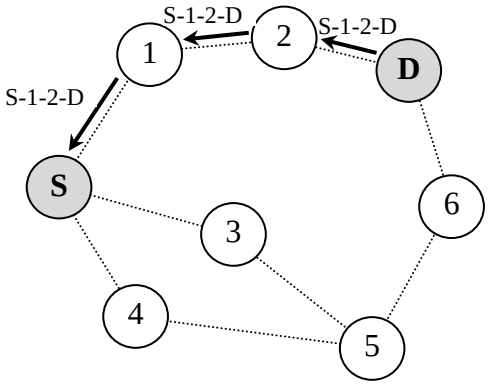

Figure 2.5: Propagation of the route reply in DSR

B. Route Maintenance in DSR:

Route maintenance can be accomplished by two different processes:

- Hop-by-hop acknowledgement at the data link layer.
- End-to-end acknowledgements.

Hop-by-hop acknowledgement is the process at the data link layer which allows an early detection and re-transmission of lost packets. If the data link layer determines a fatal transmission error, a route error packet is being sent back to the sender of the packet. The route error packet contains the information about the address of the node detecting the error and the host's address which was trying to transmit the packet. Whenever a node receives a route error packet, the hop is removed from the route cache and all routes containing this hop are truncated at that point [44].

DSR maintain multiple routes to a destination in its cache. If by some reason a route is broken to some destination then it check its cache for another valid route to the same destination and does not re invoke the route reconstruction process. That's how the route recovery process is faster in DSR than any other on demand routing protocol. However if it does not have an alternative route to the destination then it must reinitiate the route discover process. Placing the entire route information in both reply packet and data packet

create extra bandwidth and processing overhead. DSR is not scalable to large networks because it assumes that the diameter of the network is not more than 10 hops. Route discovery and route maintenances create extra bandwidth overhead [38][54].

Advantages of DSR:

- A route is established only when it is required.
- Supports multipath routing.
- Loop-free routing.

Disadvantages of DSR:

- Not effective in large networks because of route overheads.
- Suffers from the high latency encountered in route discovery.
- The route maintenance mechanism is poor

2.3.5 Dynamic MANET On-demand (DYMO):

Dynamic MANET On-demand (DYMO) is a successor of the Ad hoc On-Demand Distance Vector (AODV) routing protocol, it's known as AODVv2, defined in Internet Engineering Task Force (IETF) Internet-Draft [50]. It operates similarly to AODV. DYMO does not add extra features or extend the AODV protocol, but rather simplifies it, while retaining the basic mode of operation. DYMO is a purely reactive protocol in which routes are computed on demand i.e. as and when required and it employs sequence numbers which guarantees the orderly delivery of packets to the destination and maintains loop-free routes. Like AODV, DYMO implements three messages during the routing operation namely Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). As DYMO uses AODV as the basis, it borrows "Path Accumulation" from Dynamic Source Routing (DSR) [51][52].

DYMO protocol has two basic operations: Route Discovery and Rout Maintenance.

A. DYMO Route Discovery:

The DYMO route discovery is very similar to that of AODV except for the path accumulation feature. The originating node initiates flooding of Route Requests (RREQ) throughout the network to find the target node, where each intermediate node records the route to the originating node. On receiving the RREQ, the target node responds with a Route Reply (RREP) which is sent in a unicast, hop-by-hop fashion towards the originating node. On receipt of RREP by originating node from the target node, the routes between the originating node and the target node are established in both directions as illustrated in figure 2.6. [53]

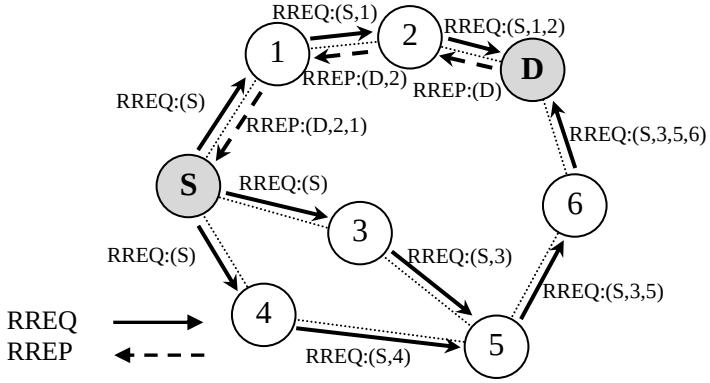

Figure 2.6: DYMO Route Discovery

B. DYMO Route Maintenance:

In order to respond to the changes in network topology, nodes maintain their routes and monitor the links over which the network traffic flows. When a received data packet is to be forwarded to some other node where the route is unknown or broken, the source of the packet is notified by sending Route Error (RERR) that indicates the current route is broken. The RERR generating node multicasts the RERR message to only those nodes

which are concerned with the link failure as shown in figure 2.7. Upon reception of a RERR message, the routing table is updated and the entry with the broken link is deleted. After deletion of the route entry, if any of the nodes face a packet to the same destination a new route discovery process needs to be initiated again [52][53].

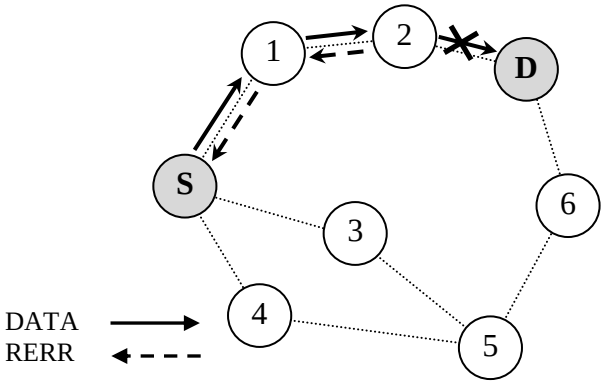

Figure 2.7: RERR messages generation and propagation in DYMO

Features of DYMO protocol:

One of the special features of DYMO is that it is energy efficient. If a node is low on energy, it has the option to not participate in the route discovery process. In such a case, the node will not forward any of the incoming RREQ messages. It however will analyze the incoming RREP messages and update its routing tables for future use. In addition, the routing table of DYMO is comparatively less memory consuming than AODV even with "Path Accumulation" feature. Also the overhead for the protocol decreases with increased network sizes and high mobility. The performance evaluation shows that DYMO outperforms AODV as a MANET routing protocol [51].

Advantages of DYMO:

- DYMO is energy efficient when the network is large and shows a high mobility.

- The routing table of DYMO is comparatively less memory consuming than AODV even with Path Accumulation feature.
- The overhead for the protocol decreases with increased network sizes and high mobility.

Disadvantages of DYMO:

- DYMO does not perform well with low mobility; which the control message overhead is rather high and unnecessary.
- DYMO performs well when traffic is directed from one part of the network to another. However, it shows a degraded performance when there is very low traffic random and routing overhead outruns the actual traffic.

2.4 Performance Comparison of Routing Protocols in MANETs:

There are many research studies that provide comparisons of the routing protocols in terms of performance indexes. Simulation results of many research studies shows that AODV has the highest throughput followed by OLSR and GRP protocol, and the AODV protocol shows low data drop for 30 nodes according to [55]. In the simulation experiment of [56], AODV shows to have the overall best performance. It has an improvement of DSR and DSDV and has advantages of the both [55][56].

Simulation results of [57] verified that AODV gives better performance as compared to DSR and DSDV. Figure 2.8 shows the packet delivery fraction versus number of nodes. It is obvious that the AODV routing protocol performance is better than DSDV and DSR as the number of nodes increases [57].

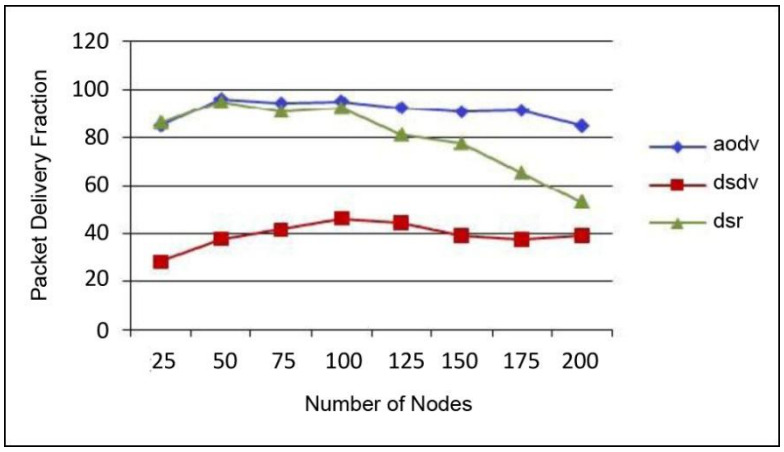

Figure 2.8: Packet Delivery Fraction vs. Number of Nodes [57]

Figure 2.9 shows that AODV provides the highest throughput as compared with DSDV and DSR [57].

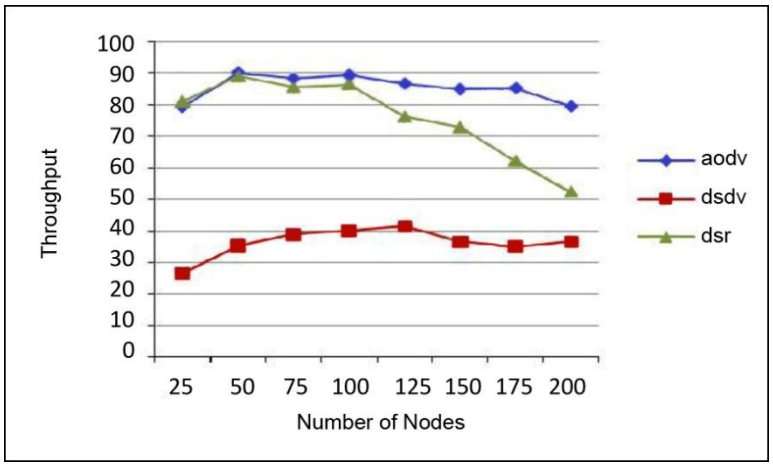

Figure 2.9: Throughput Vs. Number of Nodes [57]

2.5 Summary:

Due to high degree of node mobility in MANETs; network topology is frequently changing, which makes routing in MANETs a challenging task. As a result, conventional routing algorithms are not suitable for these networks. Several routing protocols have been designed for ad hoc networks. Classifications of MANET routing protocols are discussed in this chapter. They are proactive, reactive, hybrid, hierarchical and geographical routing protocols Proactive routing protocols such as OLSR have high overhead traffic caused by

periodic exchange of control messages. Reactive routing protocols suffer from high initial delay. By studying some examples of reactive and proactive protocols, AODV gives better performance as compared to DSR and DSDV in terms of packet deliver ratio and throughput.

Chapter Three

Security Attacks in MANETs

3.1 Introduction:

The distinguishing characteristics of MANETs give the space for malicious attackers to find vulnerabilities that are not available in other types of wireless networks. MANETs are vulnerable to various attacks at all layers. So, much research has been conducted on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality: intruders can compromise the operation of the network by attacking any of the physical, MAC or network layers. The network layer, especially the routing protocol, is vulnerable because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, the lack of clearly defined physical network boundary and the transient nature of services in the network. Standard information security measures such as encryption and authentication do not provide complete protection; thus, intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs [4][58].

Securing MANET is more difficult as channel is accessible to legitimate user and also to malicious attacker. Nodes are free to move arbitrarily due to which the network topology changes frequently and consequently the trust among the nodes creates complexity of routing of data [59].

3.2 Classification of Security Attacks in MANETs:

MANETs are vulnerable to attacks more than other conventional wired and wireless networks due to their special network attributes. Besides, different types of attacker with various motives can carry out the same type of attack. Defense mechanisms may need to be sensitive not only to the type of attack but also the type of attacker. Therefore, in this

section, we discuss taxonomy for security attacks; in the next section we will discuss taxonomy for attackers and their motives [5][10].

Security attacks can be categorized, according to the criteria that whether they disrupt the operation of a routing protocol or not, into two broad classes: passive and active attacks as shown in figure 3.1 below. Passive attacks, where adversaries do not make any emissions, are mainly against data confidentiality. In active attacks, malicious acts are carried out not only against data confidentiality but also data integrity. Active attacks can also aim for unauthorized access and usage of the resources or the disturbance of an opponent's communications. An active attacker makes an emission or action that can be detected [60][61].

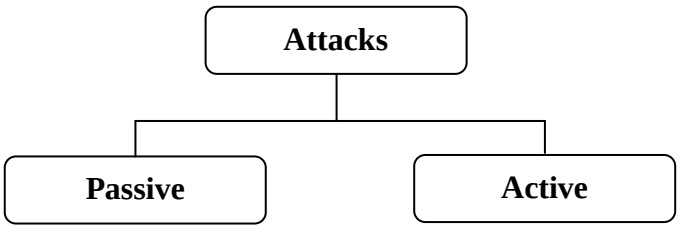

Figure 3.1: Classification of attacks

3.2.1 Passive Attacks:

In passive attacks, the attacker attempts to discover valuable information but does not disrupt the operation of the routing protocol. Passive attacks can be grouped into eavesdropping and traffic analysis types as illustrated in figure 3.2 [62].

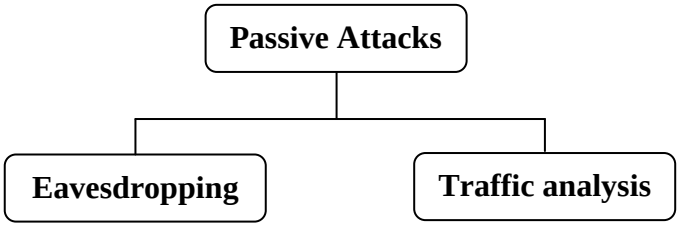

Figure 3.2: Classification of passive attacks

1. **Eavesdropping:**

Classified data can be eavesdropped by tapping communication lines, and wireless links are easier to tap. Therefore, wireless networks are more susceptible to passive attacks. In particular when known standards are used and plain data, i.e. not encrypted, are sent wirelessly, an adversary can easily receive and read the data. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. The information may include encryption keys, credit card numbers, location or passwords of the nodes [14][60].

2. **Traffic Analysis:**

Not only the content of data packets is important for adversaries, but also the traffic pattern may also be very valuable for them. For example, confidential information about network topology can be derived by analyzing traffic patterns. In ad hoc networks the nodes closer to the base station, i.e. the sink, make more transmissions than the other nodes because they relay more packets than the nodes farther from the base station [14].

Traffic analysis in ad hoc networks may reveal the following type of information:

- Location of nodes.
- Network topology used for communication
- Roles played by nodes
- Available source and destination nodes

There are many techniques that may be used for traffic analysis:

- Traffic analysis at the physical layer: in this attack only the carrier is sensed and the traffic rates are analyzed for the nodes at a location.

- Traffic analysis in MAC and higher layers: MAC frames and data packets can be demultiplexed and headers can be analyzed. This can reveal the routing information, topology of the network and friendship trees.
- Traffic analysis by event correlation: events like detection in a sensor network or transmission by an end user can be correlated with the traffic and more detailed information, e.g. routes, etc., can be derived.
- Active traffic analysis: traffic analysis can also be conducted as an active attack. For example, a certain number of nodes can be destroyed, which stimulates self organization in the network, and valuable data about the topology can be gathered [60].

Traffic analysis can also be used to organize attacks against anonymity. Adversaries can aim to detect the source of certain data packets, which may help localizing events and determining the weaknesses, capabilities, functions and owners of transferred data. Moreover, traffic patterns can pertain to the other confidential information such as the actions and the intentions [63].

3.2.2 Active Attacks:

In an active attack an adversary actually affects the operations in the attacked network or information system. It involves actions like modification and deletion of exchanging data to absorb packets destined to other nodes to the attacker for analyzing or disabling the network. So, active attacks are very severe attacks on the network. For example, the networking services may be degraded or terminated as a result of these attacks. Sometimes the adversary tries to stay undetected, aiming to gain unauthorized access to the system resources or threatening confidentiality and/or integrity of the content of the network [62][63].

Active attacks are classified into four classes as shown in figure 3.3 [60][63][64][65].

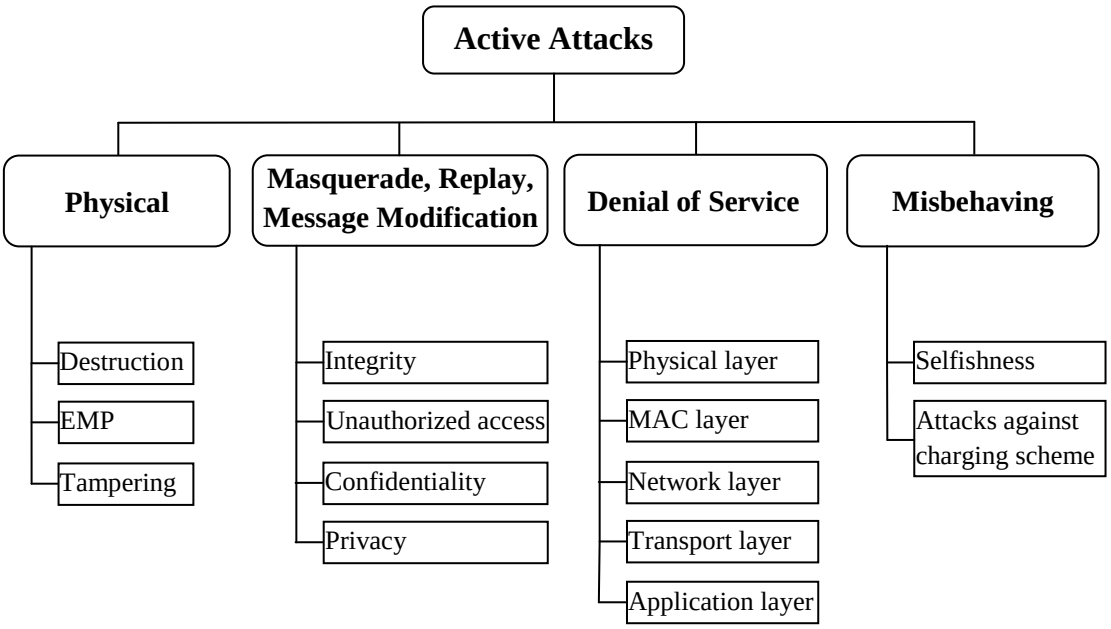

Figure 3.3: Classification of active attacks

3.2.2.1 Physical Attacks:

An adversary may *physically damage hardware* to terminate the nodes. This is a security attack that can also be considered to fall in the domain of fault tolerance, which is the ability to sustain networking functionalities without any interruption due to node failures.

When nodes are unattended and can be reached physically by the adversary, they can be attacked by *tampering* techniques, such as microprobing, laser cutting, focused ion-beam manipulation, glitch attacks and power analysis. Node tampering can help in masquerading and denial-of-service attacks [60][63].

Electromagnetic pulse (EMP) attacks are also among the threats that can be listed within physical security attacks. An EMP is a short-duration burst of high-intensity electromagnetic energy that can produce voltage surges, which can damage electronic devices within range [60][63].

3.2.2.2 Masquerade, Replay and Message Modification:

A *masquerading* node acts as if it is another node. Messages can be captured and *replayed* by masquerading nodes. The content of the captured messages can be *modified* before being replayed. Various scenarios and threats can be developed based on these approaches [60].

Masquerading, message replay and content modification can be used to attack the integrity of the content of messages or services in a network. Attacks against the integrity of services can be considered as denial-of-service (DoS) attacks because they reduce the availability of some services [60].

Masquerading, message replay and content modification can also be used against *confidentiality* by making the other nodes send the confidential data to a malicious node or by accessing the confidential data. They can also be used as techniques for gaining *unauthorized access* to system resources.

An adversary may masquerade for *phishing*, which means deceiving someone in order to make him/her give confidential information voluntarily. A malicious node that masquerades an authorized node can ask another node to give information about passwords, keys, etc.

3.2.2.3 Denial-of-Service Attacks:

A denial-of-service (DoS) attack mainly targets the *availability* of network services. A DoS is defined as any event that diminishes a network's capacity to perform its expected function correctly or in a timely manner. A DoS attack is characterized by the following properties [60][63]:

- **Malicious:** it is carried out to prevent the network from fulfilling its intended functions. It is not accidental. Otherwise it is not in the domain of security but reliability and fault tolerance.
- **Disruptive:** it degrades the quality of services offered by the network.
- **Asymmetric:** the attacker puts in much less effort compared to the scale of the impact made on the network.

A DoS attack can be organized at any networking protocol layer:

A. DoS in the physical layer:

The mentioned physical attacks in this section can also be perceived as DoS attacks because they prevent a network from performing its expected functions.

Jamming attack, which is a DoS in the physical layer, can be performed by a malicious device that jam a wireless carrier by transmitting a signal at that frequency. The jamming signal contributes to the noise in the carrier and its strength is enough to reduce the signal-to-noise ratio below the level that the nodes using that channel need to receive data correctly.

B. DoS in the link layer:

The algorithms in the link layer, especially MAC schemes, present many exploitation opportunities for DoS attacks. A malicious node can continuously jam a channel to create a MAC layer DoS attacks by performing any of the following cases:

- Whenever an RTS signal is received, a signal that collides with the CTS signal is transmitted. Since the nodes cannot start transmitting data before receiving the CTS, they continue sending RTS signals.

- If the MAC scheme is based on sleeping and active periods, jamming only the active periods can continuously block the channel.

- False RTS or CTS signals with long data transmission parameters are continuously sent out, which makes the other nodes that do virtual carrier sensing wait forever.

- Acknowledgement spoofing, where an adversary sends false link layer acknowledgements for overheard packets addressed to neighboring nodes, can also be an effective link layer DoS attack.

C. DoS in the network layer (against Routing Schemes):

Ad hoc networks are infrastructureless and have special routing challenges, as mentioned in chapter 2, which bear additional opportunities for new types of DoS attack against the network layer protocols for such networks. These attacks generally fall into one of two categories: routing disruption attacks or resource consumption attacks as shown in figure 3.4 [60].

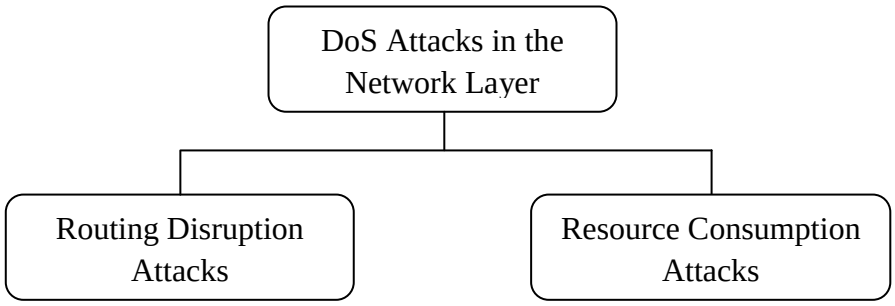

Figure 3.4: Classification of DoS attacks in the network layer

Routing disruption attacks aim to make the routing scheme dysfunction, making it unable to provide the required networking services. The goal of *resource consumption attacks* is to consume network resources such as bandwidth, memory, computational power and energy [60].

Malicious node can disrupt network operations by not following the routing protocol specifications as follows [66]:

a. Modification:

Malicious node may illegally modify the routing information of the received messages before forwarding them, it can alter one or several fields in the message, depends on the goals that it may want to achieve. Such attack compromises the integrity of route discovery. By altering routing information, a malicious node can take control of a route, can cause network traffic to be dropped or redirected, or take a long route to the destination increasing communication delays. Malicious node may increase the destination sequence number to make route appear fresher, decrease the hop count to make it appear shortest or even replace the source (destination) IP address in the IP header with another IP address to impersonate another node [66].

Routing control messages (RREQ, RREP and RERR) can be modified in the following ways:

1- **Modification of RREQ:** The freshness of a RREQ message is represented by the RREQ ID, and based on this field along with the originator IP address, the intermediate node accepts or refuses to forward the RREQ message. Therefore a malicious node may increase the RREQ ID to convince other nodes to accept the modified RREQ message as illustrated in figure 3.5. It may also increase the destination sequence number to make route appear fresher, decrease the hop count to make route appear shortest or even replace the source address in the IP header with non-existent IP address to cause loss of the RREP message.

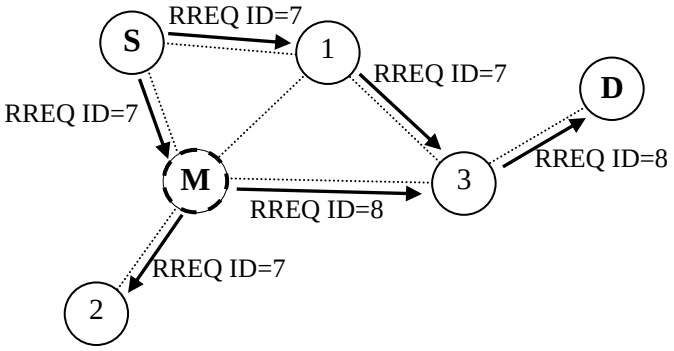

Figure 3.5: Malicious Node Modifies a RREQ message

2- **Modification of RREP:** Nodes use the destination sequence number to determine the freshness of the information received from the source node. When several RREP messages are received by a source node, it chooses the one with a largest Destination Sequence number and accordingly constructs a route to a destination. Therefore, a malicious node may increase the Destination Sequence number of the RREP message to guarantee that its RREP message or the RREP message passing through it as illustrated in figure 3.6. As a result malicious node invades the established route and can carry out other malicious actions.

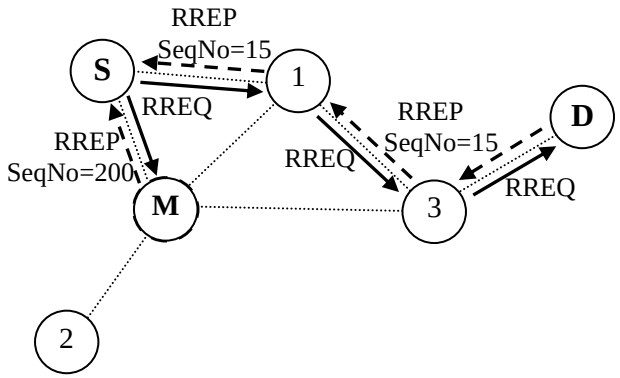

Figure 3.6: Malicious Node Modifies a RREP message

3- **Modification of RERR:** When a malicious node receives a RERR message, it can replace an unreachable destination IP address with another IP address, or append new unreachable destination IP addresses that, in fact, can be reached through the malicious node as illustrated in figure 3.7. It also can send out a faked RERR message without being triggered by the receipt of any RERR message. The

modified RERR message can be send to the neighbors in the precursor list, or even to those that are not in the precursor list of the malicious node, in order to disable active routes and disrupt the routing operation [66].

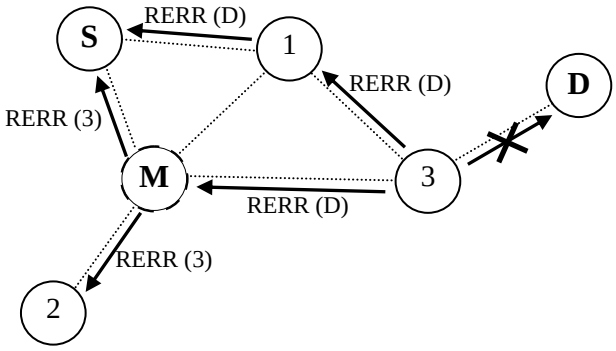

Figure 3.7: Malicious Node Modifies a RERR message

Table 3.1 lists the fields in a RREQ, RREP, and RERR message that the malicious node may manipulate.

Table 3.1: Possible malicious modifications of routing protocols fields messages

Fields	Messages	Modifications
Type	All	Change the message type
Flags	All	Reverse the setting
Hop count	RREQ, RREP	Decrease it to update other nodes reverse route tables, or increase it to suppress its update
RREQ ID	RREQ	Increase it to make the faked RREQ message acceptable, or decrease it to make the RREQ message unacceptable
Dest_IP	RREQ, RREP	Replace it with another IP address
Dest_SEQ	RREQ, RREP	Increase it to update other nodes forward route tables, or decrease it to suppress its update
Orig_IP	RREQ, RREP	Replace it with another IP address
Orig_Seq	RREQ	Increase it to update other nodes reverse route tables, or decrease it to suppress its update
Prefix size	RREP	Increase/Decrease the size of the subnet prefix
Lifetime	RREP	Decrease/increase it to shorten/extend the lifetime of the route entry updated by this RREP message
Dest count	RERR	Modify it according to the number of unreachable destinations included in the

		RERR message
Un_Dest_IP	RERR	Replace it with another IP address
Un_Dest_SEQ	RERR	Increase it to update other nodes routing table, or decrease it to suppress this entry

b. Fabrication Attack:

Fabrication refers to attack performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claims that a neighbor can no longer be contacted [66]. In AODV there are two kinds of fabrication:

1- **Forge reply:** The malicious node sends forged routing control message in response to legitimate routing message. Forge Reply is mainly related to the generation of faked RREP and RREP-ACK messages, trigged respectively by the receipt of legitimate RREQ and RREP messages as illustrated in figure 3.8. Malicious node impersonates destination address in the received RREQ, sends a forge RREP message, and establishes a route with a source node, in order to intercept or to drop data packets.

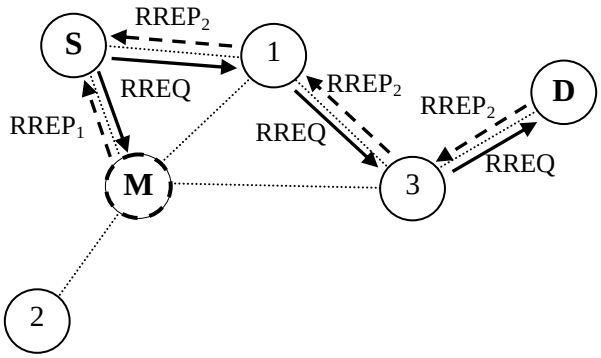

Figure 3.8: Malicious Node Modifies a fake RREP message

2- **Active forge:** In this attack the malicious node sends a forged routing control message without prior reception of any routing message, to achieve malicious

purpose such as; break route or delete route, by using respectively a forge RREQ or forged RERR message. Malicious node may eventually Flood the network with RREQ messages to consume the network resources.

c. Dropping attack:

Dropping control packets might be the greatly benefit for both selfish and malicious nodes. Particularly, once dropping the RREQ packets, a selfish node prevents the established routes from passing through it and consequently it saves its energy for transmitting its own packets. Likewise, a malicious node may directly disrupt the routing operation by dropping routing messages to prevent new route from being established, or isolate a node or a group of nodes from communicating with the rest of the network. Dropping RERR packets extends the duration of use of the broken routes and consequently the network bandwidth falls sharply since no packet reaches its destination. In some cases malicious node may carry out more sophisticated dropping to divert security mechanisms by performing periodic, selective or random dropping.

d. Black Hole Attack:

Black hole attack is a type of active attack that exploits the route reply message (RREP) feature of the ad hoc on-demand distance vector (AODV) routing protocol. This attack involves some modification of the data stream or the creation of a false stream. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. A RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any other RREP messages from other neighboring nodes or even from the actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination

node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them [34]. Black hole attack will be explained in more details in section 3.4 in this chapter.

e. Gray Hole Attack:

This attack is more sophisticated than the black hole attack, instead of dropping all data packets a malicious node selectively drops packets. It may drop packets originating from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes, which limits the suspicion of its wrongdoing. It can also alternate by interval of time between malicious behavior (dropping packets) and honest behavior (forwarding packets). To render the attack more difficult to detect malicious node can combines selective drop, and periodic or random dropping [61][66].

f. Wormhole Attack:

Also called tunneling attack, is composed of two (or group of) colluding malicious nodes directly linked to each other through wormhole tunnel established by means of a wired link, a high quality wireless out-of-band link or a logical link via packet encapsulation. One malicious node forwards received RREQ control messages from one point in the network to the second malicious node in another point many hops away in the network through the wormhole tunnel as illustrated in figure 3.9. When the second malicious node receives these tunneled packets it replays them in its neighborhood. Therefore the malicious nodes are included in the established route and may now intercept or drop data packets instead of forwarding. [66].

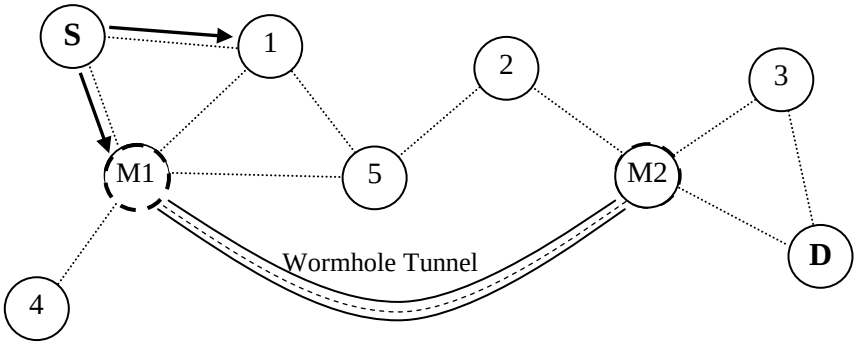

Figure 3.9: Wormhole Attack

Wormhole attack is difficult to detect, and can be launched even against communications that provide authenticity and confidentiality. Detection of wormhole attack requires the use of an unalterable and independent physical metric, such as time delay or geographical location [61][67].

g. Rushing Attack:

This attack can be carried out against on-demand routing protocols that use duplicate suppression in their operations. In order to reduce the route discovery overhead, each intermediate node processes only the first received route request packets and rejects any duplicate packets that arrive later. Rushing node exploits this mechanism by quickly disseminating route request packets in order to be included in the discovered routes, as illustrated in figure 3.10. Rushing attack can be performed in many ways: by transmitting at a higher wireless transmission power level, by ignoring delays at MAC or routing layers, by keeping other nodes' transmission queues full or by using a wormhole tunnel [67].

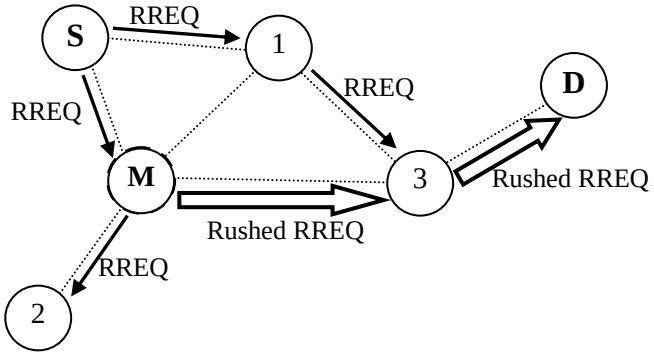

Figure 3.10: Rushing attack

h. Resource depletion:

Also known as the sleep deprivation attack, it can be achieved by constantly generating fake routing packets and flooding it through the whole network, creating routing loops or injecting unnecessary data flows in some parts of the network. Hence, the malicious node may effectively consume the network bandwidth, power energy, and the processing time of the legitimate nodes. To achieve this end, the malicious node applies the strategies illustrated below [66]:

1- **RREQ flooding:** The malicious node floods the network either by modify incoming RREQ messages to make them appear fresh by increasing their RREQ ID or by continuously fabricate a large number of fake RREQ packets as in figure 3.11. In both cases the fake RREQ packets will be rebroadcast by the malicious node's neighbors and propagated to the rest of the network.

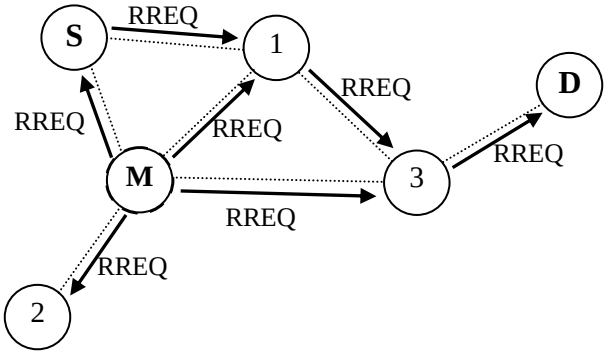

Figure 3.11: RREQ flooding

2- **Routing loop:** The malicious node creates a loop(s) between forwarding nodes within a real route by sending a fake RREP, therefore the nodes involved in the loop(s) consume about 10 times more energy than the normal cases. Furthermore, the data packets transmitted in the loop will be dropped in the end and some nodes will be isolating from the rest of the network.

3- **Data flow injection:** In this attack malicious node injects large volumes of data flows on the network to congest existing routes and set up unnecessarily data flows to any point in the network up to its extreme transmission bandwidth. This type of attack is difficult to defend against, because it is hard to differentiate between legitimate and malicious data flows.

i. Impersonation Attack:

Impersonation also known in the literature as spoofing or masquerading attack is launched by using other node's identity (IP address) in outgoing routing packets. The malicious node may impersonate source node to communicate with destination node, or the destination node to reply the source node, as illustrated in figure 3.12, or even announce new route with high destination sequence number or reduced hop count to the others nodes. Therefore

the attacker can read, alter the received packets or even totally (entirely) isolate the real (authentic node (the real owner of the address) from the network. Impersonation attack sometimes is the first step for more sophisticated attacks [66].

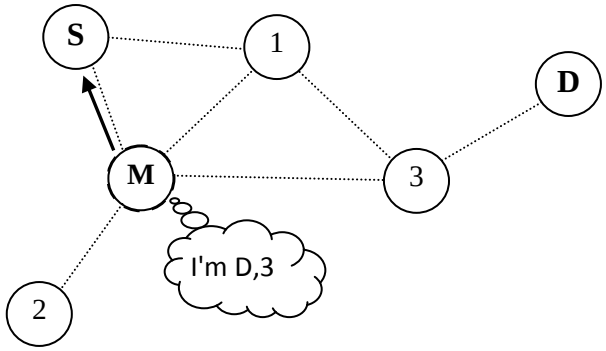

Figure 3.12: Impersonation Attack

j. Sybil Attack:

A Sybil attack is an improved version of impersonation, in which a single node pretends to be many different nodes at the same time, by using multiple distinct addresses while transmitting. An attacker can obtain (acquire) an address through two manners; it can usurp an existing address or forging (fabricate) one if the network has no restriction to the allowed. This reduces the effectiveness of fault-tolerance schemes and poses a significant threat to geographic routing protocols. Apart from these services it may also affect the performance of other schemes such as misbehavior detection, voting-based algorithms, data aggregation and fusion and distributed storage [60][66].

D. DoS in The Transport Layer:

Transport layer protocols are also susceptible to security threats. Some attack scenarios applicable at this layer are listed below:

a. SYN Flooding Attack:

The SYN flooding attacks are the type of Denial of Service (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node. These half opened connection are never completes the handshake to fully open the connection [14].

b. Session Hijacking

Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc) and other information from nodes. Session hijacking attacks are also known as address attack which make affect on OLSR protocol. The TCP-ACK storm problem may occur when malicious node launches a TCP session hijacking attack. The attacker "X" injects session data, and node "1" sends acknowledgement packet to node "2". Packet will not contain any sequence number that node 2 is expecting. It results in, when node "2" receive the packet and tries to resynchronize the TCP session with node "1". This process is repeated over and over that leads to ACK storm. Hijacking a session in a connectionless transport protocols such as User Datagram Protocol (UDP) is even easier than connection oriented protocols [14].

c. Transport layer acknowledgement spoofing:

False acknowledgement or acknowledgement with large receiver windows may make the source node generate more segments than the network can handle, causing congestion and degrading the network capacity.

d. Replaying acknowledgement:

In some transport layer protocols, such as TCP-Reno, acknowledging the same segment multiple times indicates negative acknowledgement. A malicious node can replay an acknowledgement multiple times to make the source node believe that the message was not delivered successfully.

e. Jamming acknowledgements:

A malicious node can jam the segments that convey acknowledgements. This may lead to the termination of a connection.

f. Changing sequence number:

In protocols like RMST and PSFQ, a malicious node may change the sequence number of a fragment and make the destination believe that some fragments have been lost.

g. Connection request spoofing:

A malicious node can send many connection requests to a node, using up its resources such that it cannot accept any other connection request [60].

E. DoS in The Application Layer:

Application layer protocols can also be exploited in DoS attacks. Many of them were mentioned in the previous section. Protocols like node localization, time synchronization, data aggregation, association and fusion can be cheated or hindered, as explained in that section. For example, a malicious node that impersonates a beacon node and gives false

location information or cheats with regard to its transmission power, i.e. transmitting with less or more power than it is supposed to do, may hamper the node localization scheme. Since these kinds of attack diminish the related network service, they can also be categorized as DoS attacks [14][60].

Other attacks in the application layer are:

a. **Repudiation Attacks:** Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services.

b. **Malicious Code Attacks:** Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

3.2.2.4 Misbehaving:

Misbehaving can also count as a cyber threat. Some nodes within the network may misbehave to gain unfair shares of the limited networking resources, i.e. they may employ *selfishness*. For example, by using the MAC scheme, a misbehaving node can force the other nodes into longer back offs and free the network resources for its own use. Nodes may also be selfish by refusing to relay others' messages. If every node acts like this, then selfishness may have an impact similar to a DoS attack [60][63].

Another means of misbehaving may be *aimed at a charging scheme* by denying payment for services received. Not always Ad hoc networks are free-of-charge environments where everybody collaborates to communicate with each other through a license-free channel. For example, Mesh networks provide wireless multihop access to broadband services. Similarly, there can be multihop cellular networks where nodes are allowed to access the network through ad hoc multihop wireless links when they are out of the coverage area provided by the infrastructure, as shown in Figure 3.13. In both of these cases nodes reach a service provider and are supposed to pay for the services they get from the provider [60][63].

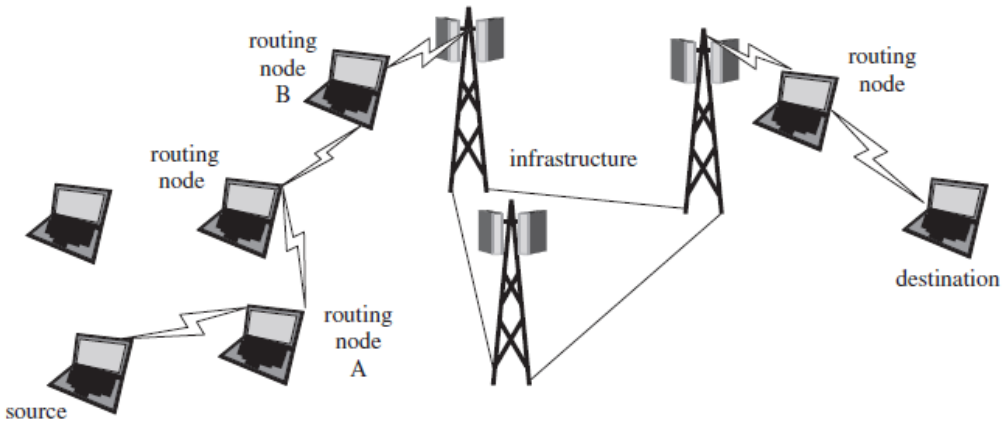

Figure 3.13: Multihop cellular networks

Several attacks are envisaged against the charging schemes in these kinds of network:

- **Refusal to pay:** The source node may deny that it carried out communications specified on a bill.
- **Dishonest rewards:** In multihop networking, intermediate nodes should relay the packets of others. To motivate intermediate nodes to forward the packets of others instead of being selfish, rewarding mechanisms, such as paying them, can be

designed. In this case, a misbehaving node may want to appear that it was involved in forwarding some packets, even though it was not.

- **Free riding:** Intermediate nodes on the route between the source and destination can piggyback their packets on to ongoing communications to avoid paying the bill. For example, routing node A can piggyback its packet to routing node B onto packets from the source to the destination in Figure 3.13.

3.3 Classification of Security Attackers in MANETs:

Similar to attacks, attackers can also be categorized according to many criteria. According to [60], attackers are classified based on the characteristics shown in figure 3.14.

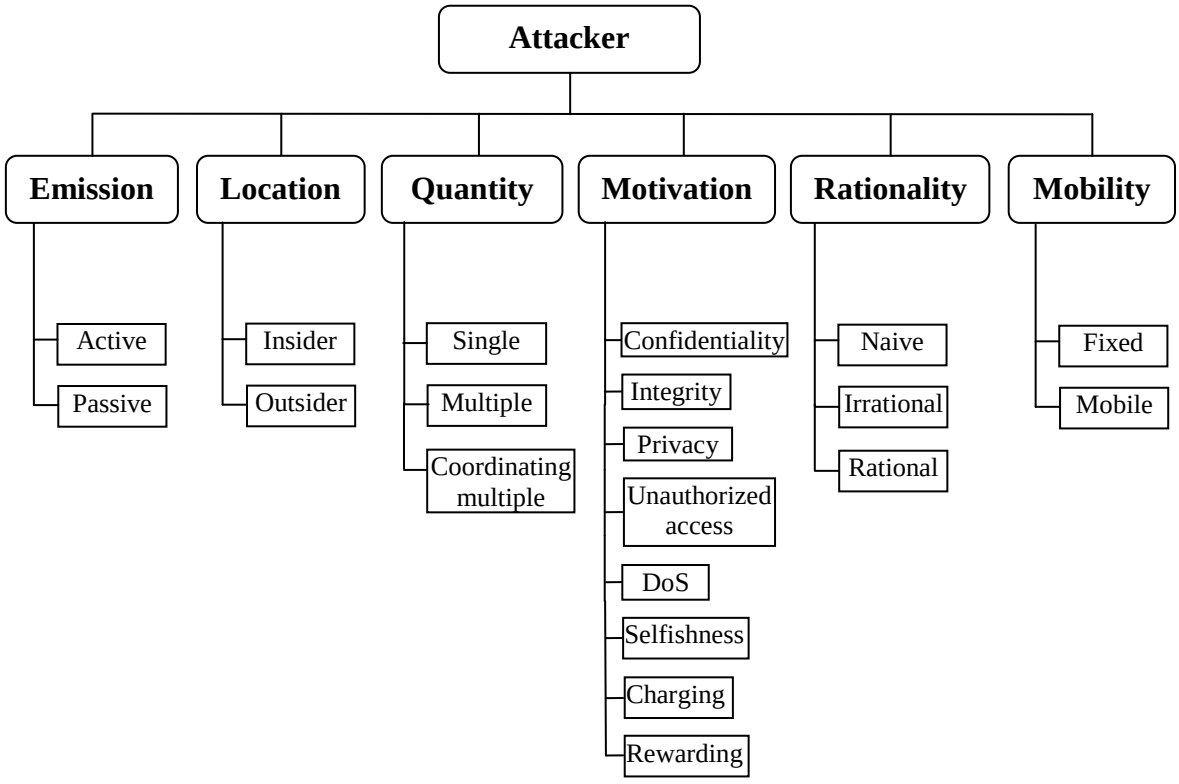

Figure 3.14: Classification of attackers

1. **Emission:** An attacker can be passive or active; this matches the classification of attacks. Active attacks are carried out by active attackers and passive attacks by passive attackers.

2. **Location:** An attacker can be an insider or an outsider. An insider is a node that has been compromised or tampered with, and it is a part of the attacked network. The attacker may learn all the cryptographic information owned by the compromised node when it is an insider. Therefore, stealthy active attacks can be organized by insider attackers. Outsider attacks can be either passive or active. In other words, an insider can be perceived as a legal entity inside the network such as a node that has been registered or a node that is allowed to access the network. An outsider is typically a node that is not welcome on the network.

3. **Quantity:** There may be a single attacker or more than one. When there are multiple attackers, they can collaborate with each other, which can be considered a more difficult case to defend against.

4. **Motivation:** An adversary carries out attacks with a certain motivation, such as breaking confidentiality, integrity and privacy. This may also be done to gain access to unauthorized resources. An attacker may also attack to hinder the operations of the other side. Selfishness, avoiding payment or getting unearned rewards may be other motives.

5. **Rationality:** Needlessness, malfunctioning nodes and naïve users may also become threats to a network. However, needlessness is not the only reason for ‘irrational’ attacks – those where the results of the attack may not be worth the cost of attacking. An attacker may attack simply in order to attack and break a security system, perceiving this as a challenge to prove himself/herself. Therefore, some

attacks are irrational where the results of these attacks may not be worth their cost. Rational attackers carry out their attacks to obtain something which is worth more than the cost of the attack.

6. **Mobility:** Attackers can be fixed or mobile. Detecting mobile attackers and defending against them is generally more difficult than defending against a fixed adversary [60][63].

3.4 Black Hole Attack in MANETs:

Routing protocols in Mobile Ad Hoc Networks by their nature are distributed routing protocols with the assumption that all nodes in the network will cooperate truly and participate honestly. However, the existence of malicious nodes makes this assumption not true. Such nodes may drop the packets, if they are not the destination, without forwarding them or may disrupt the routing discovery and maintenance processes resulting in abnormal network operation that affects the performance of the network and may cause denial of service [23].

A black hole attack is a kind of denial of service (DoS) where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them (drop all packets) without forwarding them to the destination [24].

In reactive routing protocols such as AODV, the destination sequence number (*dest_seq*) is used to describe the freshness of the route. A higher value of *dest_seq* means a fresher route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new *dest_seq* number larger than the current *dest_seq* number. In this way the intruder becomes part of the route to that destination [25].

Figure 3.15 illustrates the black hole attack where nodes S and D are the source and destination respectively and node B is the black hole.

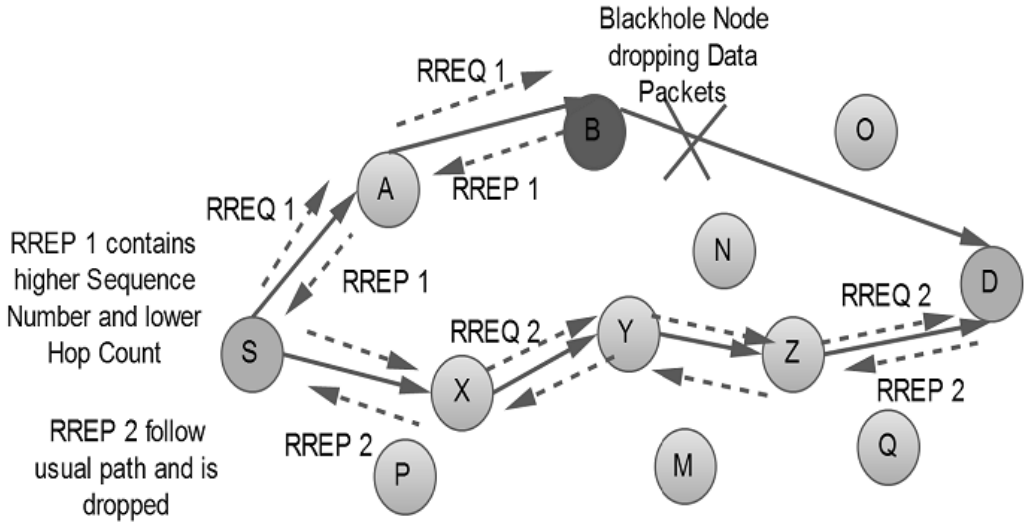

Figure 3.15: Black Hole Attack Illustration

A black hole has two properties: First, the node exploits the ad hoc routing protocol to advertise itself as having a valid route to a destination, even though the route is spurious with the intention of intercepting packets. Second, the node consumes the intercepted packets. In an ad hoc network that uses the AODV protocol, a black hole node absorbs the network traffic and drops all packets [24].

3.4.1 Behavioral Analysis of the Black Hole Node:

The black hole node is a strange malicious node joins the network with the intention of dropping the transmitted data packets instead of delivering them to the desired destination.

The following are the main behavioral characteristics of the black hole node [68]:

1. It snoops on its neighbors to discover which node is preparing to send an RREQ.
2. For any received RREQ, the black hole node propagates an RREP claiming that it has a direct link to the destination.

3. It constantly attempts to locate itself within the transmission range of any source node in order to reply as quickly as possible. This requires a continual movement of the black hole node in the network. Moreover, its movement speed may be higher than the normal nodes.

Analyzing these characteristics, there are two main key points from the behavior of the black hole node. First, it never contributes in the operation of route discovery (i.e. never broadcasts the received RREQs). Moreover, for any route including a black hole, the black hole always appears as the last hop before the destination. Second, it's expected that the number of the routes that the black hole contributes in them is greater than the number of routes that the normal node contributes in them [68].

3.5 Summary:

The characteristics of mobile ad hoc networks make them vulnerable to many attacks in all layers. This chapter provided classifications of attacks in MANETs. Different types of attacker with various motives can carry out the same type of attack. So, a classification of attackers also provided in this chapter.

In the network layer, attacks may be routing disruption attacks or resource consumption attacks. Malicious node may modify, fabricate or drop packets. Black hole attack is a modification and dropping attack in the network layer. It is very severe attack because it can make a denial of service (DoS) in the network. To mitigate its effect and to avoide the malicious nodes, we have to protect the integrity of the routing control messages during route discovery process.

Chapter Four

The Proposed Protocol (Enhanced RID-AODV)

4.1 Introduction:

Routing is an essential operation in all network types and it has special importance in ad hoc networks; because in such networks, nodes are operating not only as hosts but they are also operating as routers. Therefore, any breakthrough in the routing process has a direct impact to the performance of the whole network. This is the reason why routing is targeted in many kinds of attacks in MANETs especially black hole attack.

In this chapter an enhanced and modified routing protocol "Enhanced RID-AODV" is presented. The goal of this protocol is to avoid malicious nodes to be used as malicious nodes in the routing processes.

4.2 Evolution of the Proposed Protocol:

In this section we provide an enhanced and modified protocol based on previous one to provide a solution for the black hole attack problem when multiple nodes are acting as malicious black hole nodes.

The proposed protocol, "Enhanced RID-AODV" or "ERID-AODV ", is a modification and enhancement of the RID-AODV protocol proposed in [34]. RID-AODV protocol was proposed as combination of previous two protocols, namely IDSAODV (which is proposed in [33]) and RAODV (proposed in [35]). Figure 4.1 illustrates the evolution of ERID-AODV protocol.

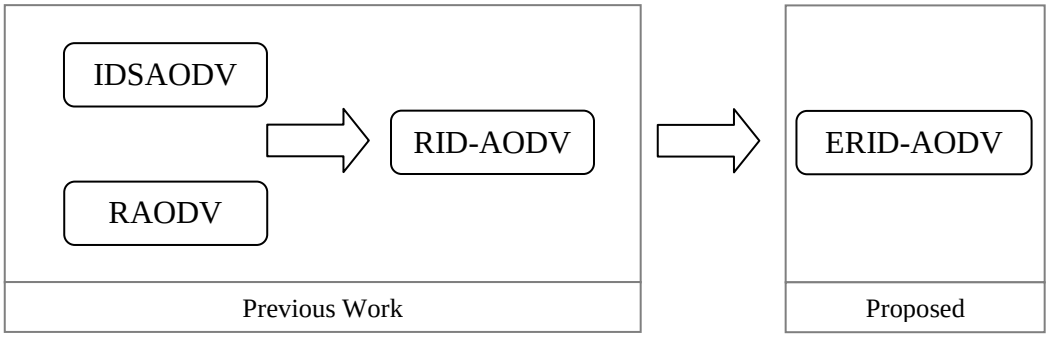

Figure 4.1: Evolution of the proposed protocol (Enhanced RID-AODV)

4.2.1 Getting advantages of the preceding protocols

The proposed protocol (Enhanced RID-AODV) provides a modification and enhancements to preceding protocol RID-AODV, which is combination of two protocols: IDSAODV and RAODV. Therefore, we got all advantages of the preceding protocols in mitigating the bad impact of the existing of malicious black hole nodes in the ad hoc network. The benefits of the preceding protocols together with the proposed enhancements, we got better results in terms of performance metrics as will be shown in the next chapter.

1. **Getting advantages of Intrusion Detection System AODV (IDSAODV) protocol:**

By analyzing the output file obtained from the simulation, it was found that there were always a second route between the nodes which are communicating. RREP message arrived from different possible routes, for example one arrived at the source on average at t= 1.2765 seconds as opposed to the RREP message arriving from the black hole node on average at t= 0.2059 seconds. It is reasonable to assume that an RREP message will arrive from the black hole earlier than the actual destination with a higher probability as the black hole does not waste any time. While the second RREP is from the intended destination. However, in some cases, this idea may not work. For instance the second RREP can be received at the source node from an intermediate node which has stale information about

the destination node or the second RREP message may come from the black hole node if the real destination node is nearer than the black hole node.

Based on the above arguments and observations, the IDSAODV was proposed to use the second route for message delivery and it was investigated by simulation that this approach improves the network performance under the black hole attacks in an ad hoc network. Actually IDSAODV improved the packet deliver ratio (PDR) in MANET with a single black hole node.

2. Reverse AODV (RAODV):

Although RAODV has not been designed to prevent black hole attacks and it was developed with the aim of solving path failure problem, authors of [34] proposed to use it in mitigating the effects of black hole attacks in ad hoc networks.

On demand routing protocols, including AODV, is based on single route reply RREP message. The lost of RREP message may cause a significant waste of performance.

For example, consider the case in figure 4.2 below where S is a source node, D is a destination node and others are intermediate nodes. When route request message RREQ is broadcasted by node S and each node on a path builds reverse path to the previous node, finally the reverse path D→3→2→1→S is built. This reverse path is used to deliver RREP message from node D to the source node S. If node 1 moves towards the arrow direction shown in the figure and goes out of transmission range of node 2, RREP missing will occur and the route discovery process will be useless. However, there are several alternative paths built by the RREQ message are ignored.

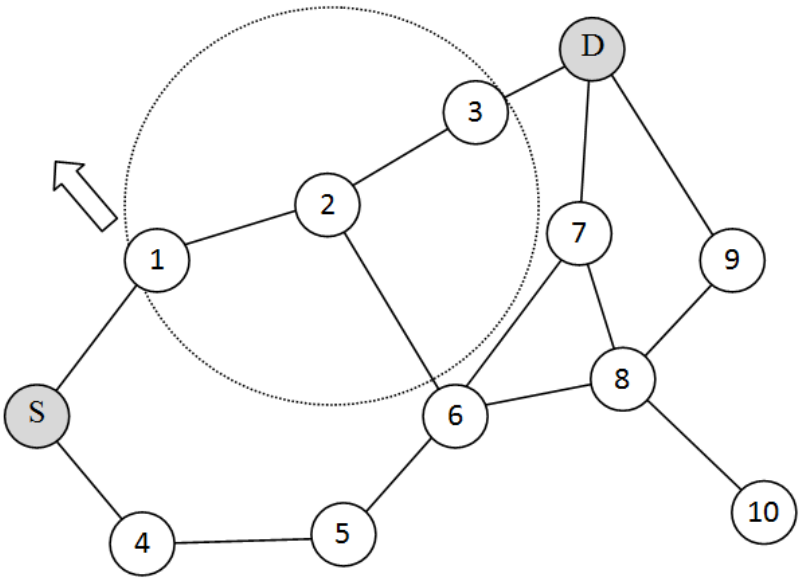

Figure 4.2: RREP Delivery Fail

Thus, R-AODV was proposed to avoid RREP loss and improve the performance of routing in MANET. In R-AODV, route reply message is not unicast, rather, destination node uses reverse RREQ (R-RREQ) to find source node. R-AODV protocol discovers routes on-demand using a reverse route discovery procedure. During route discovery procedure source node and destination node plays same role from the point of sending control messages. Thus, after receiving RREQ message, destination node floods reverse request (R-RREQ), to find source node. When source node receives an R-RREQ message, data packet transmission is started immediately. Figure 4.3 shows that when the when node 1 has moved and went outside the transmission range of node 2, when using RAODV, destination does not unicast reply along pre-decided shortest reverse path. Rather, it floods R-RREQ to find source node S. And forwarding path to destination is built through this R-RREQ.

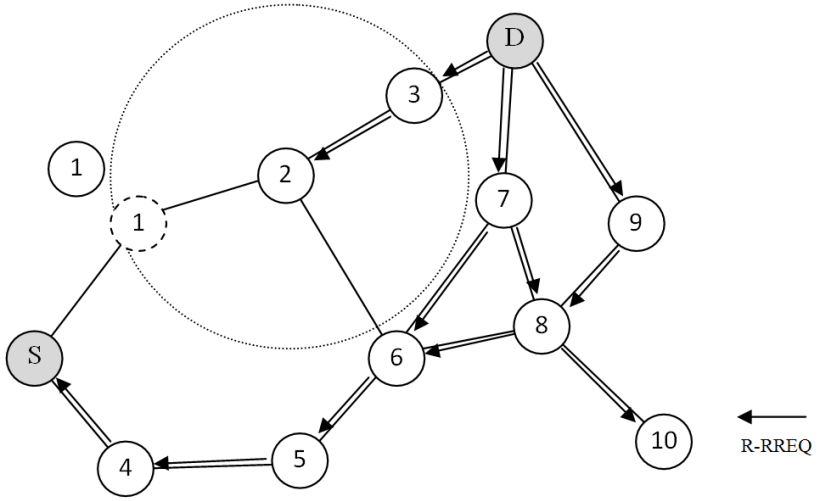

Figure 4.3: Reverse RREQ (R-RREQ) from destination to source node

R-AODV uses absolutely same procedure of RREQ of AODV to deliver route reply message to source node. R-AODV protocol can reply from destination to source if there is at least one path to source node. In this manner, R-AODV prevents a large number of retransmissions of route request messages, and hence diminishes the congestion in the network. Moreover, R-AODV improves the routing performance such as packet delivery ratio and end-to-end delay. Therefore, success rate of route discovery may be increased even though high node mobility situation.

4.3 The enhancements in the proposed protocol

The detection of the malicious nodes and mitigation their effects can be achieved by creating and maintaining *dynamic blacklist* in each node according to some criteria. Then each non malicious node will prevent sending or forwarding to the neighboring nodes that exist in its own blacklist either in the forward or reverse path In other words, each node will not use blacklisted nodes as intermediate nodes. Dynamic blacklist means that each node adds and removes nodes to or from its blacklist automatically according to specific criteria as will be explained in this section.

The criteria for each node to add another node's address in its blacklist is the repetitive mismatch in the hash value of the receiving frames (layer 2 frame) from the same neighboring node. So, each node keeps a counter for each other node that receives a frame from the neighboring nodes. If there is a mismatch between the received hash value and the calculated value, the corresponding counter for the sending (or forwarding) node will be incremented. When the counter reaches some threshold value ***malPcktThreshold***, then the corresponding neighboring node will be blacklisted.

Each node keeps small number of counters. If node n_i has p neighboring nodes (**p** is ⊆ of all nodes) and $\mathbf{n_i}$ is receiving from **q** nodes (**q** is ⊆ of **p**), then $\mathbf{n_i}$will keep only **q** counters for this purpose. For example, for the network in figure 4.4, the node 9 will maintain less than or equal to 5 counters.

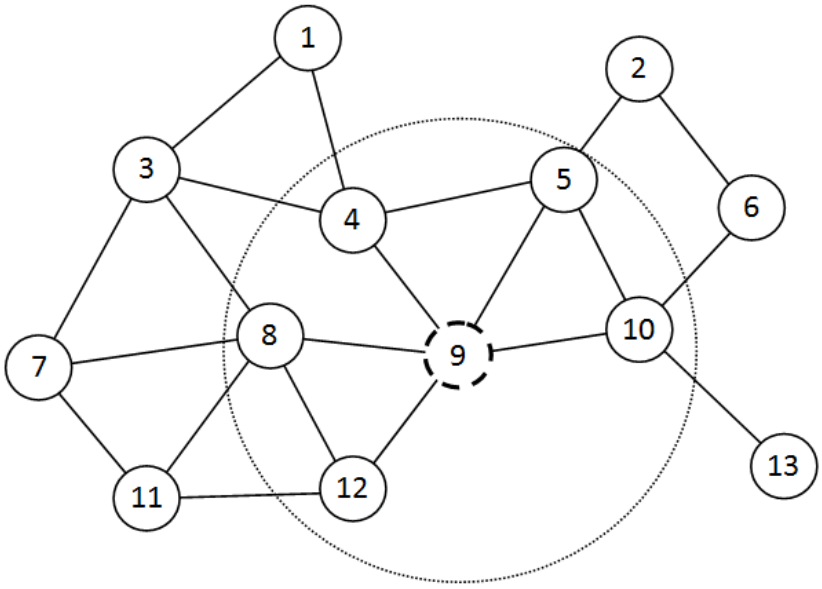

Figure 4.4: Each node maintains a small number of counters

In addition, we can get another advantage of the nature of the reverse route discovery procedure in RAODV to create *full path (bidirectional) integrity check implemented in hop-by-hop basis* to detect any modifications on the traversing packets and to detect the causing nodes.

To distinguish between hash value mismatch that may occur as a result of normal link failure, which is from the nature of MANETs due to mobility of nodes that communicate wirelessly, or from the existence of malicious nodes, the threshold value $\boldsymbol{malPcktThreshold}$ should be considered as a function of mobility (variable threshold). If the node is moving with relatively high speed the mismatch of hash values is most likely due to normal link failure, and so the threshold should be high. On the other hand, if there are many hash value mismatches while the node is moving slowly, there is most likely a malicious node. So, the value of $\boldsymbol{malPcktThreshold}$ is directly proportional to the node speed and it was implemented by using equation (5.1):

$$\boldsymbol{malPcktThreshold = NodeSpeed + C} \qquad \textbf{(4.1)}$$

Where $\mathbf{C}$ is the threshold value when the node speed is zero.

The malicious node may not act as a black hole all the time, it may become benign for some period of time, then it may (or may not) resume its malicious activities. So, when a node adds another node's address to its blacklist, the blacklisted node will not stay in its blacklist forever. However, it will be blacklisted for a previously specified period of time. So, when a node is added to another node's blacklist, not only the address of the blacklist is added but also the expiry time for that node to be released from that blacklist. The blacklisted node expiry time is computed using equation (5.2):

$$\boldsymbol{blkListedNodeExpTime = CURRENT\_TIME + blocking\ Period} \qquad \textbf{(4.2)}$$

Each time the node wants to send (or forward) a packet to a neighbouring node, it will check if it is blacklisted, and if so it will also check the expiry time for that node. If it's expired, it will be removed from the blacklist of that node and its corresponding counter and expiry timer will be reset. Because of that it is dynamic blacklist. Figure 4.5 illustrates the idea of the using counters to create blacklist with expiration time for the blacklisted nodes. In this figure, because the counter in node 2 that is associated to node 3 has exceeded the threshold value, node 2 added node 3 to its blacklist. So, node 2 will not forward to node 3 until the time exceeds the blacklist expiry time for node 3 which is 37 in this example.

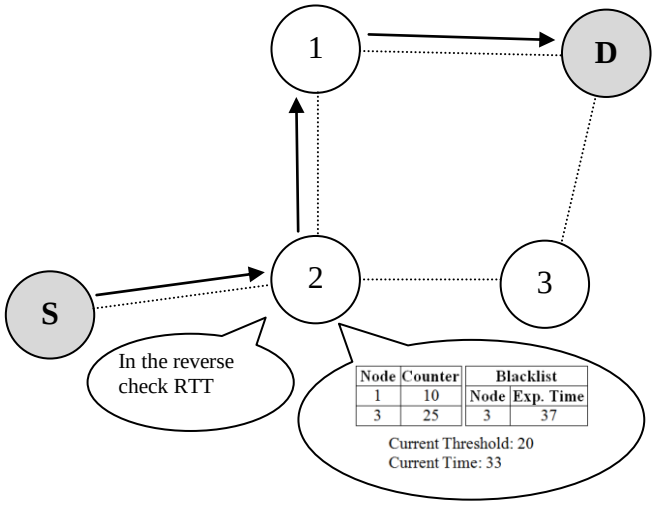

Figure 4.5: Using blacklist to avoid forwarding to blacklisted nodes for a pre-specified period

Now when a node wants to send (or forward) a packet, in either the forward path or reverse path, it will check the routing table to decide what is the next hop. Then it will check if the next hop is blacklisted or not, if it's blacklisted, it will check the blacklist expiry time. If the next hop node is still blacklisted, then the node will remove that node from its neighbour list and run the handle link failure procedure. Then the node will try to send (or forward) the packet by using another path.

As a result, we can get a secure path that avoids the black hole malicious nodes during routing packet as shown in figure 4.6.

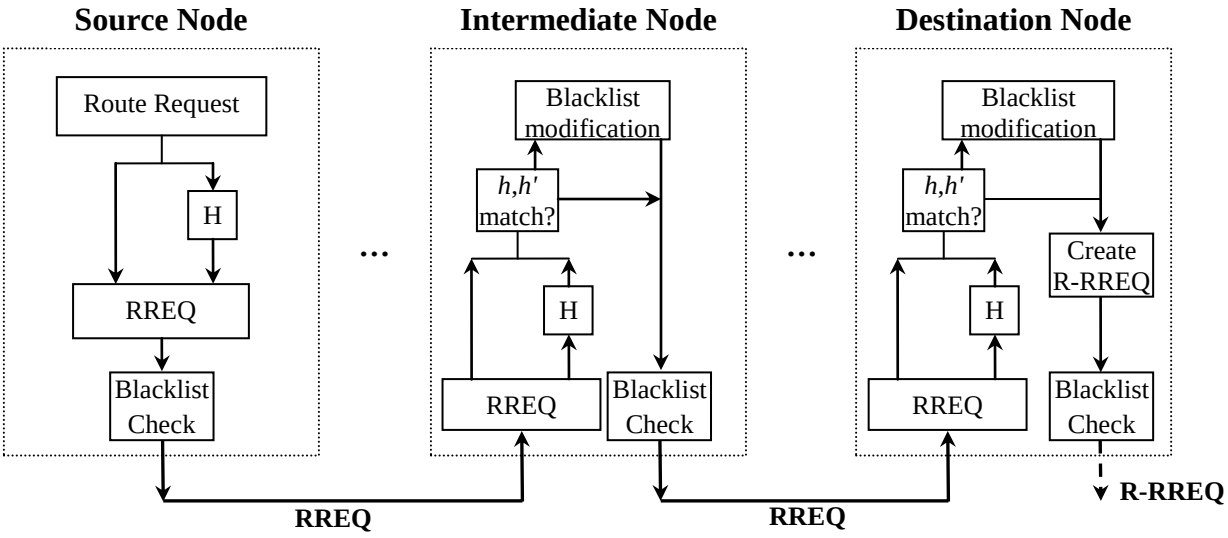

Figure 4.6: Secure Routing Path

The criterion for the reverse path is the round trip time (***RTT***). ***RTT*** is the length of time it takes the RREQ to be sent (or forwarded) plus the length of time it takes for the R-RREQ to be received by the node. As we assumed that all the nodes are trusted, we can measure ***RTT*** in the normal behaviour, and use it as a reference. Any change in this value indicates that the reply was not from the original destination; so, this value can be used to detect the malicious node.

The node will first measure Round Trip Time (***RTT***). Then it will calculate the average hop-to-hop time ($\boldsymbol{T_{h-h}}$) using the following equation:

$$\boldsymbol{T_{h-h} = \frac{RTT}{2 * hop\ count}} \qquad \textbf{(4.3)}$$

Now, the New *RTT* ($\boldsymbol{RTT_{next}}$) should satisfy the following condition:

$$\boldsymbol{RTT - \frac{T_{h-h}}{2}} < \boldsymbol{RTT_{next}} < RTT + \boldsymbol{\frac{T_{h-h}}{2}} \qquad \textbf{(4.4)}$$

The sequence diagram of the Enhanced RID-AODV protocol is shown in figure 4.7. ***RTT*** values are shown in normal behaviour and in malicious behaviour.

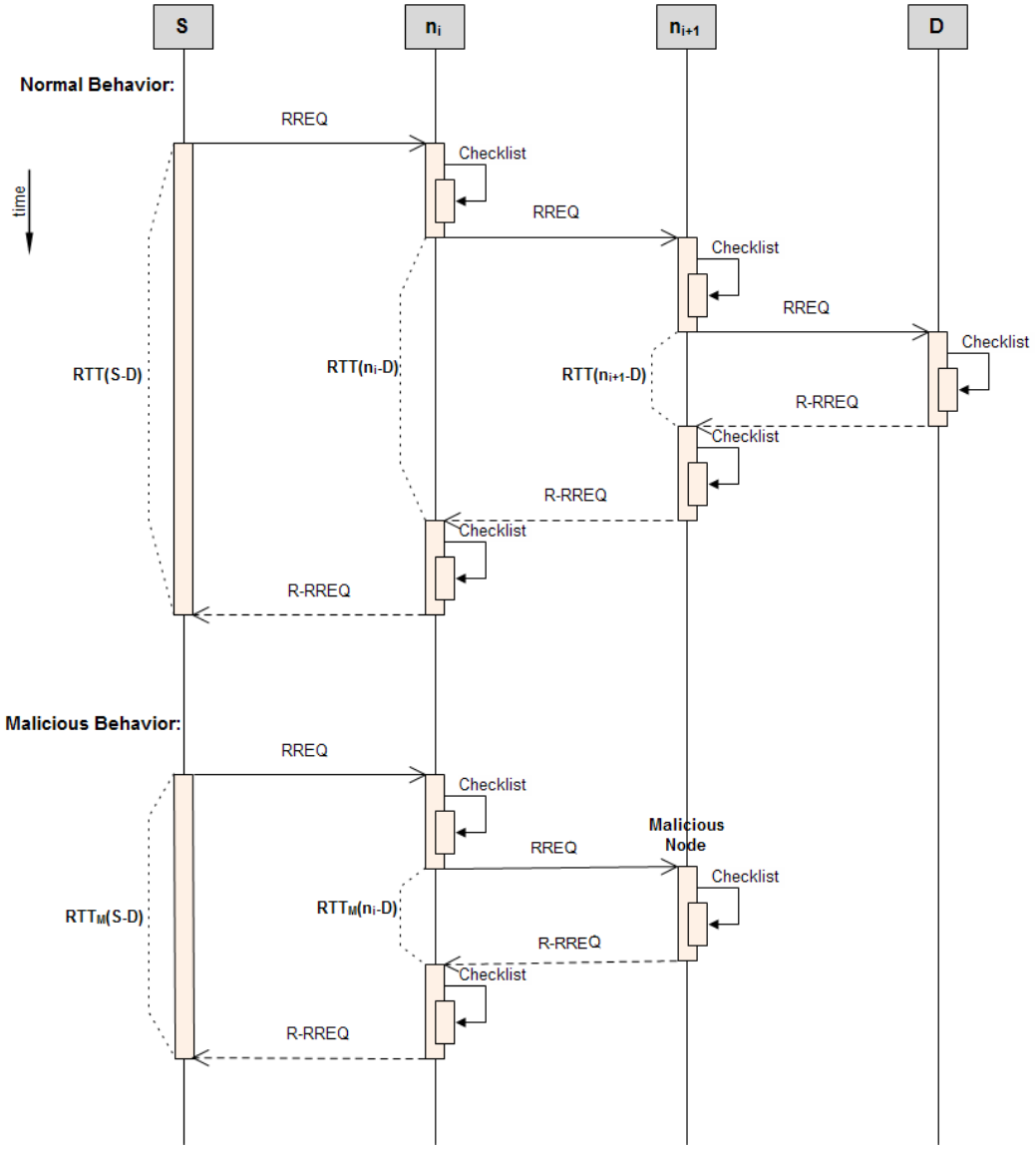

Figure 4.7: Sequence Diagram for the Enhanced RID-AODV

4.3.1 Hashing Function:

To implement the Enhanced RID-AODV protocol a new field was added in the route request (RREQ) and reverse route request (R-RREQ). The original and modified RREQ message formats are shown in figure 4.8 and figure 4.9 respectively.

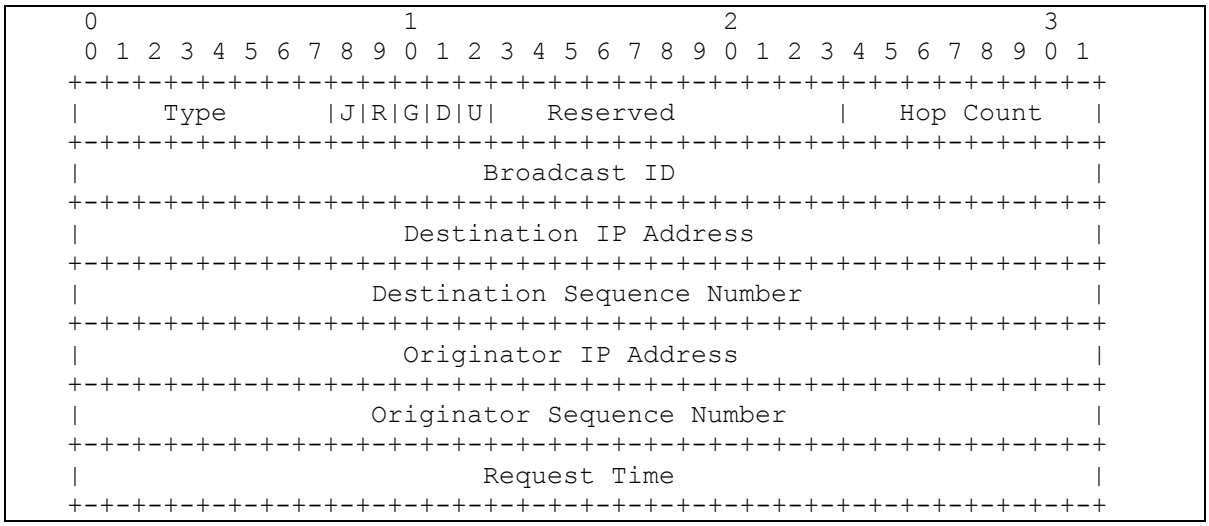

Figure 4.8: Original Route Request (RREQ) Message Format [46]

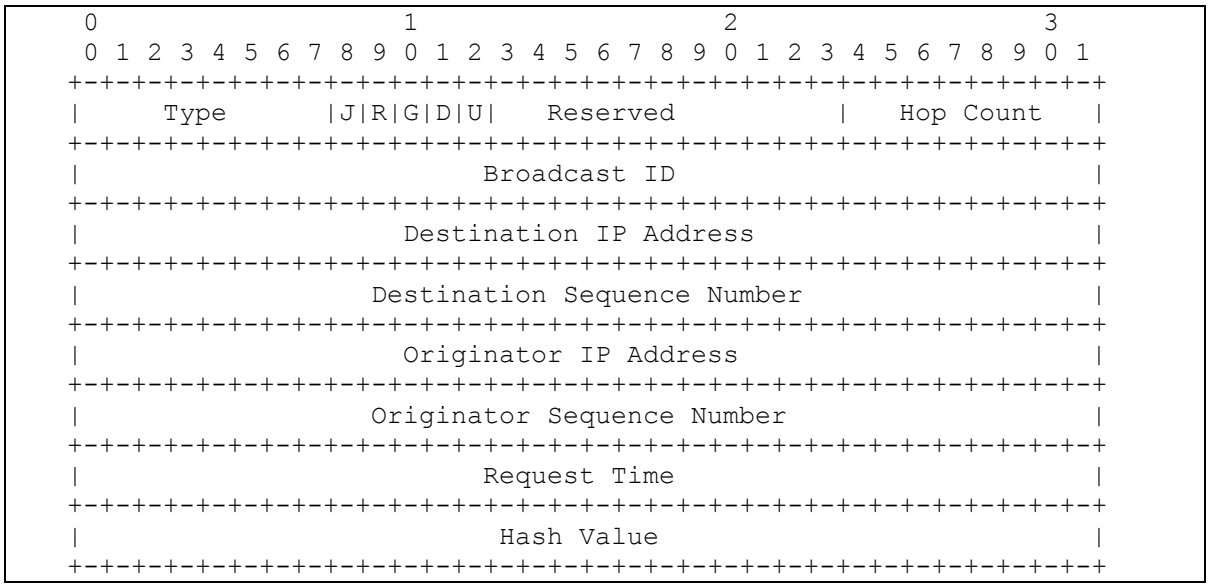

Figure 4.9: Modified Route Request (RREQ) Message Format

Because we adopt the Reverse-AODV, we also modified the reverse route request (R-RREQ) message format to handle the hash value.

The original R-RREQ message format as proposed in [35] is shown in figure 4.10 and the modified one in the Enhanced RID-AIDV protocol is shown in figure 4.11 below.

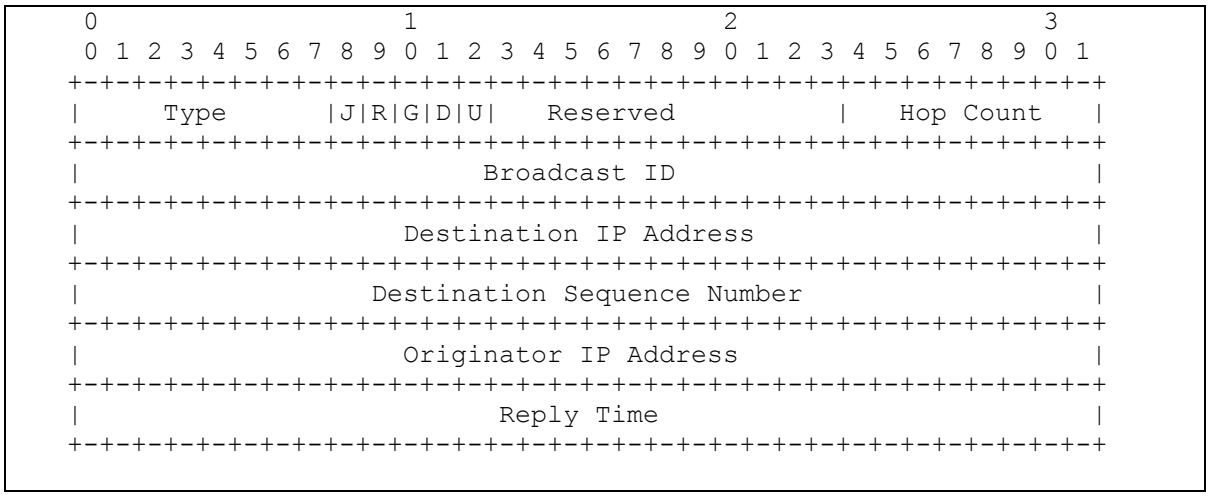

Figure 4.10: Reverse Route Request (R-RREQ) Message Format

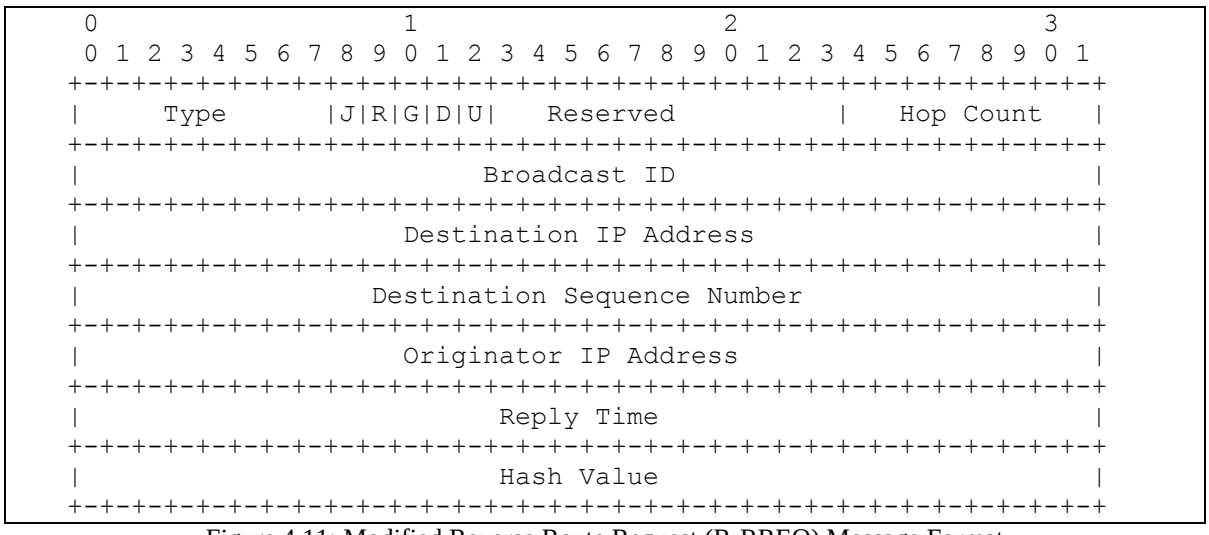

Figure 4.11: Modified Reverse Route Request (R-RREQ) Message Format

In our protocol we used one-way hashing function on the level of packets in the routing discovery control messages. The purpose of using a hash function is to produce a "fingerprint" of the message. This fingerprint will be used for route request (RREQ) *packet authentication* and *integrity check* in each hop while traversing from source node to the destination node and for reverse route request (R-RREQ) from destination to source; resulting in a two-way (bidirectional) control packet authentication and integrity check.

For our implementation of the "Enhanced RID-AODV" protocol, we used a simple hash function in the purpose of having a small number of arithmetic operations because of the

limitations in recourses and power in the nodes in MANET. Besides, the hash function was applied to three fields of the RREQ and R-RREQ messages only and not to the whole message:

- Destination Sequence Number ($\boldsymbol{DstSeqNo}$).
- Source Address ($\boldsymbol{SAddr}$)
- Broadcast ID ($\boldsymbol{BID}$).

Destination sequence number ($\boldsymbol{DstSeqNo}$) is susceptible to be modified by the malicious node to claim that it has a fresher route than the genuine one. The pair: source address ($\boldsymbol{SAddr}$) and broadcast ID ($\boldsymbol{BID}$) uniquely identify an RREQ, so this combination will form a unique representation of the whole RREQ message. Therefore, we can make the hashing value for these fields instead of taking the hashing value of all message fields.

$$\boldsymbol{h = H(DstSeqNo\,, SAddr\,, BID\,)} \qquad \textbf{(4.5)}$$

where $\boldsymbol{h}$ is the hash value and $\boldsymbol{H(\cdot)}$ is the hash function.

The input of the hashing function was considered as array of blocks each one is an 8-bit integer in array $\boldsymbol{M[\cdot]}$

The hash function was implemented as a recursive sequence according to equation 5.4:

$$\boldsymbol{h(i) = (h(i-1) * s\,) + M[i-1]} \qquad \textbf{(4.6)}$$

Where $\boldsymbol{s}$ is a seed value, the initial value of $\boldsymbol{h}$ (which is $\boldsymbol{h(0)}$) is *zero* and the final value of $\boldsymbol{h}$ (which is $\boldsymbol{h(N-1)}$) is *the hash value*. ($\boldsymbol{N}$ is the array length)

4.3.2 Pseudocodes and Flowchart for the Enhanced RID-AODV protocol

The pseudocodes for the Enhanced RID-AODV protocol are presented in algorithms 4.1, 4.2 and 4.3. Algorithm 4.1 is a pseudocode that describes how the node decides to add other nodes to or from its blacklist. In other words, how the node detects malicious nodes and adds them to its blacklist.

Pseudocode for the proposed protocol: How the node decides to add or remove other nodes in its blacklist:

1. Generate new hash value ($NewHash$).
2. Compare the generated hash value New_Hash with the received hash value with the packet $HashVal$.
3. if($NewHash \neq HashVal$)
   then, $incr\ malNodeCouter(PrevHopAddr)$
4. Check the speed of the node ($NodeSpeed$).
5. Compute the threshold that will be used to consider a node as blacklisted
   $$malPcktThreshold = NodeSpeed + C$$
6. *//To add a node to a blacklist*
   if(isBlacklisted(NextHop) == FALSE &&
   $malNodeCouter(NextHop) > malPcktThreshold$)
   then,
   a. $addBlackList(NextHop)$.
   b. $blkListedNodeExpTime(NextHop) = CURRENT\_TIME + Blocking\ Period$

Algorithm 4.1: Pseudocode for the proposed protocol: How the node decides to add other nodes in its blacklist

Algorithm 4.2 is a pseudocode that describes how the node decides to remove other nodes from its blacklist

Pseudocode for the proposed protocol: How the node decides to add or remove other nodes in its blacklist:

//To remove a node from a blacklist
if(isBlaklisted(NextHop) == TRUE &&
$CURRENT\_TIME > BlkListedNodeExpTime(NextHop)$)
then,
a. $removeBlackList(NextHop)$.
b. $malNodeCouter(NextHop) = 0$
c. $blkListedNodeExpTime(NextHop) = 0$

Algorithm 4.2: Pseudocode for the proposed protocol: How the node decides to remove a node from its blacklist

Algorithm 4.3 is a pseudocode that describes how the node behaves when sending or forwarding a packet.

Pseudocode for the proposed protocol: How the node behaves when sending or forwarding a packet:

```
if(isBlacklisted(NextHop) == TRUE)
then,
    // Generate route error message
        send RERR
```

Algorithm 4.3: Pseudocode for the proposed protocol: how the node behaves when sending or forwarding a packet

Figure 4.12 shows the flowchart for the Enhanced RID-AODV protocol. It includes the RREQ and R-RREQ phases and how each node takes decision of adding or removing nodes to its blacklist.

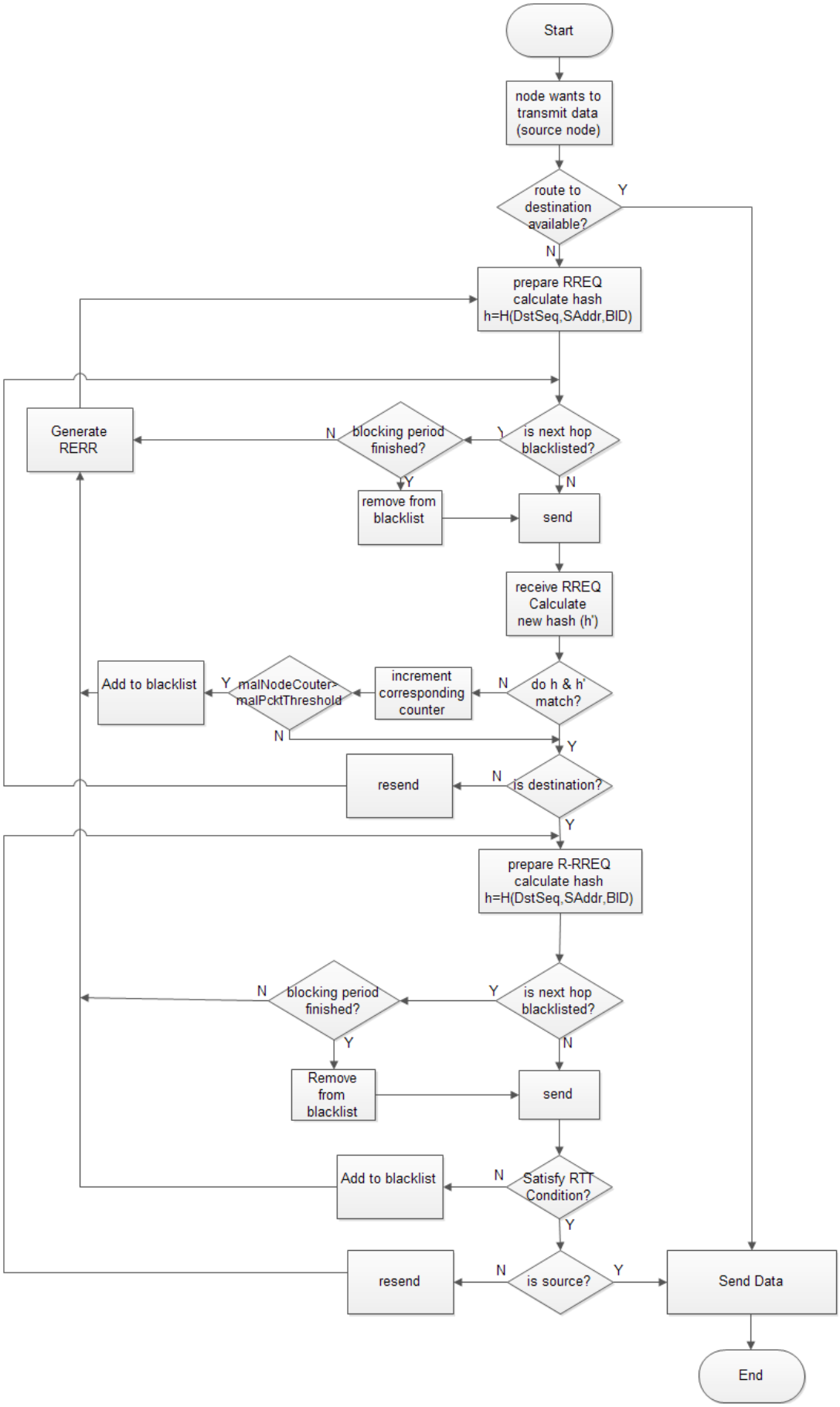

Figure 4.12: Flowchart of the Enhanced RID-AODV protocol

4.4 Summary:

This chapter presented the designed and proposed protocol "Enhanced RID-AODV". This protocol gets advantages of previous works and it was enhanced to overcome the drawbacks of its preceding. The enhancement provides a blacklist for the malicious nodes in each node so that each node will avoid these nodes during routing packets. Besides, using variable thresholds eliminates the effect to normal link failure in deciding to add a node to the blacklist. Using these blacklists can decrease the delay and increase the throughput and packet delivery ratio.

Chapter Five

Simulation and Results

5.1 Introduction:

In this chapter, we present our simulation experiments that were carried out to test our protocol and to provide a good comparison between "Enhanced RID-AODV" protocol and other protocols in terms of performance metrics.

5.2 Simulation Tool:

Network Simulator version 2 (NS-2) is one of the most popular network simulators that are appropriate to simulate the wireless networks [69]. In our research we used ns-2 because it is widely adopted in scientific community, an open source simulator and does not require any licenses.

Ns-2 is an open-source discrete event-driven simulator that is written in C++, which is Object Oriented Language (OOL). Ns-2 supports simulation of several routing protocols over wired and wireless networks and supports the ability to develop or modify protocols. It has become the most widely used open source network simulator ant it has many types of mobility models and traffic generators. The results of the simulation that performed based on NS-2 are NAM file (display file) and trace file (analysis file) that differ in storage size according to the network size [70].

To interpret the resulting trace files after each simulation, *AWK* software was used. *AWK* is an interpreted programming language for processing text files; it is very useful when analyzing traces [70].

Figure 5.1 illustrates an overview about the steps of the simulation and analysis using ns-2 simulator.

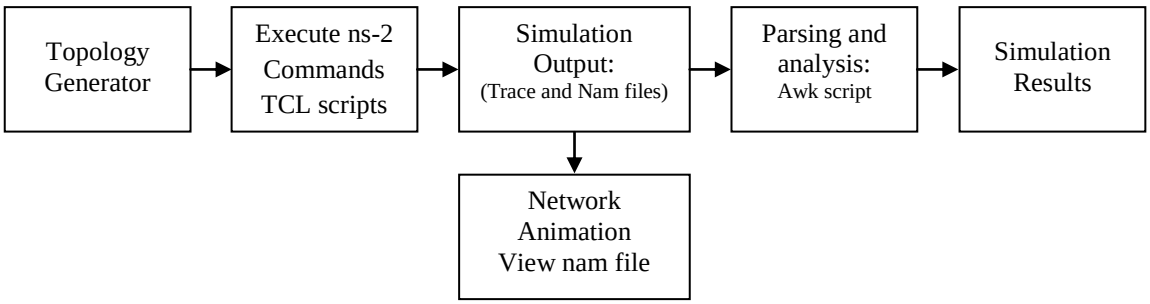

Figure 5.1: Overview of simulation and analysis using ns-2

5.3 Simulation and Network Environment

The simulation was carried out using ns-2 simulator under Ubuntu Linux operating system. During the simulation the packet header (*aodv_packet.h* file) of the AODV route request and route reply (changed to route reverse request) are modified to hold the hash value (***Hash_Val***) with packet. In addition to that, the files *aodv.h* and *aodv.cc* were modified to implement the Enhanced RID-AODV protocol together with previous protocols. Also, files */common/node.h* and */common/node.cc* have been modified to hold the $\boldsymbol{q}$ counters and the blacklists inside each node. Simulation was carried out by referring to many resources including but not limited to references [71][72][73].

The simulation area is a square field of 1000m x 1000m with fixed sender and receiver nodes that communicate using intermediate mobile nodes, which are moving randomly during simulation time (these random movements were generated using '*setdest*' tool) and the intermediate nodes are sending random traffic pattern among each other (created using '*cbrgen.tcl*' command). The sender and receiver were placed in points (200,200) and (800,800) respectively. So they are out of the transmission range of each other and all traffic between them is through the moving intermediate nodes. The parameter considered in this simulation is given in table 5.1 below.

Table 5.1: Parameters used in simulation

Parameter	Value
Simulator	ns-2
Routing protocol	AODV, IDSAODV, R-AODV, RID-AODV, Enhanced RID-AODV
Simulation time	100 sec
Simulation area	1000m x 1000m
Number of nodes	40
Number of malicious nodes	0,1,2,3,4,5,6,7
Sender node	Fixed at point (200,200)
Receiver node	Fixed at point (800,800)
Intermediate nodes	Moving randomly
Maximum speed of mobile nodes	Three scenarios: 20, 30 & 40 m/s
Data Rate	50 Kb/s
Pause time	0 sec
Transport type	UDP, CBR
Data packet size	Default
MAC Protocol	IEEE 802.11

In this research, the Enhanced RID-AODV protocol together with four preceding protocols were implemented and simulated with the same environment parameters to be able to make a comparison among them. That include: the genuine AODV protocol with simulation of black hole malicious nodes, the IDSAODV protocol proposed in [33], RAODV proposed in [35], RID-AODV that was proposed on [34] and our proposed protocol which is Enhanced RID-AODV. For each protocol many scenarios were generated to simulate the existence of different number of malicious nodes in order to study the effect of multiple malicious nodes on network performance and the effectiveness of each protocol to compare among these protocols; we made as many combinations of nodes to act as malicious nodes and then we computed the average of the results.

The simulation was carried out in three scenarios by changing the maximum speed of the nodes. The idea is to test the effectiveness of these protocols as the speed to the nodes increased. The three scenarios are:

1. Scenario 1: maximum speed = 20 m/s.
2. Scenario 2: maximum speed = 30 m/s.
3. Scenario 3: maximum speed = 40 m/s.

5.4 Performance Metrics:

In this simulation, the following four performance metrics were considered and computed as the average of many cases in all scenarios of multiple malicious nodes for all the protocols in the study. Four separate scripts were generated to compute these performance metrics using *awk* command.

1. **Throughput**: The amount of data transferred over the period of time expressed in kilobits per second (kbps). Throughput has been calculated using equation (5.1):

$$Throughput = \frac{\sum Size\ of\ Received\ Data\ Packets}{Simulation\ Time} \qquad (5.1)$$

2. **Packet Delivery Ratio (PDR)**: The percentage ratio of the total number of data packets received by the destination node to the number of data packets sent by the source node as in equation (5.2).

$$PDR = \frac{\sum Number\ of\ Received\ Data\ Packets}{\sum Number\ of\ Sent\ Data\ Packets} * 100\% \qquad (5.2)$$

3. **Average End-to-End Delay**: The average delay between the sending of the data packet by the source node and its receipt at the destination node. This includes all the delays caused during route acquisition, buffering and processing at intermediate

nodes, retransmission delays at the MAC layer, etc. The average end-to-end delay was computed using equation (5.3).

$$Avg\_E2E\_Delay = \frac{\sum_i (Receive\ Time\ of\ P_i - Sent\ Time\ of\ P_i)}{Number\ of\ Received\ Packet} \quad (5.3)$$

4. **Overhead Ratio**: The ratio of the total number of control packets sent at the routing level and the total number of packets sent from the source node as in equation (5.4).

$$Overhead\ Ratio = 1 - \frac{Number\ of\ Data\ Packets\ Sent\ at\ RTR}{Number\ of\ All\ Packets\ Sent\ at\ RTR} \quad (5.4)$$

5.5 Simulation Results

We can investigate the efficiency of the new protocol graphically by using the NAM (network animator) tool to take screenshots for the network traffic for the case of using RID-AODV protocol which is illustrated in figure 5.2, and the case of using the "Enhanced RID-AODV" protocol illustrated in figure 5.3. Both figures were taken for the same network scenarios and screenshots were taken at approximately the same moment of the simulation time as shown in the figures.

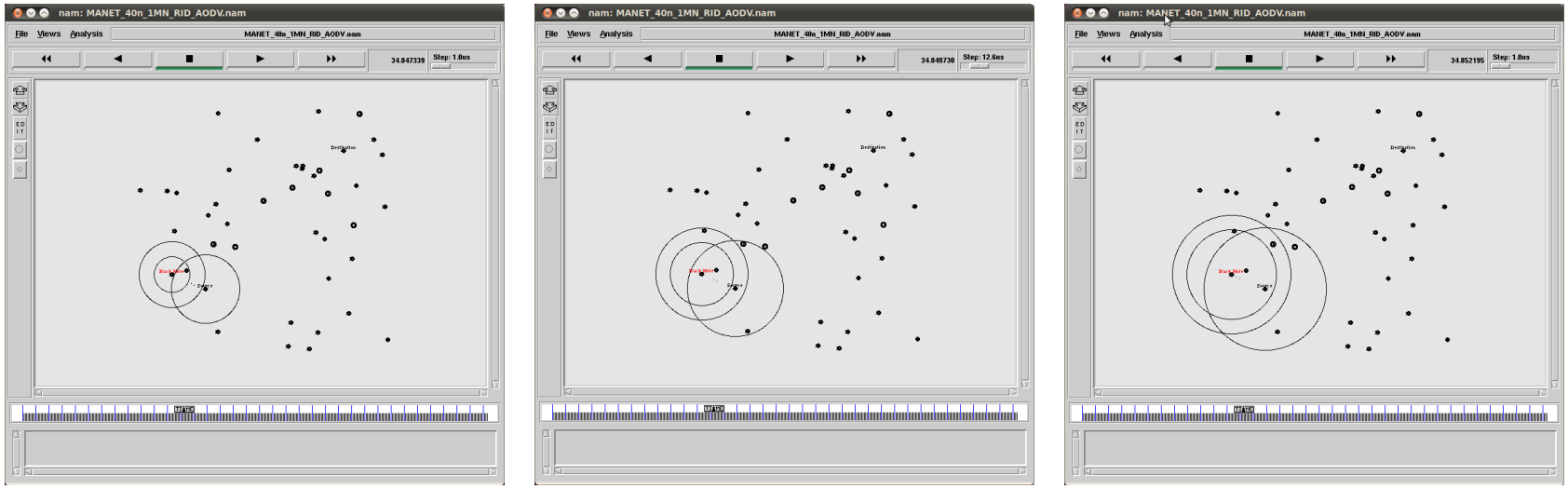

Figure 5.2: Screenshots when using RID-AODV

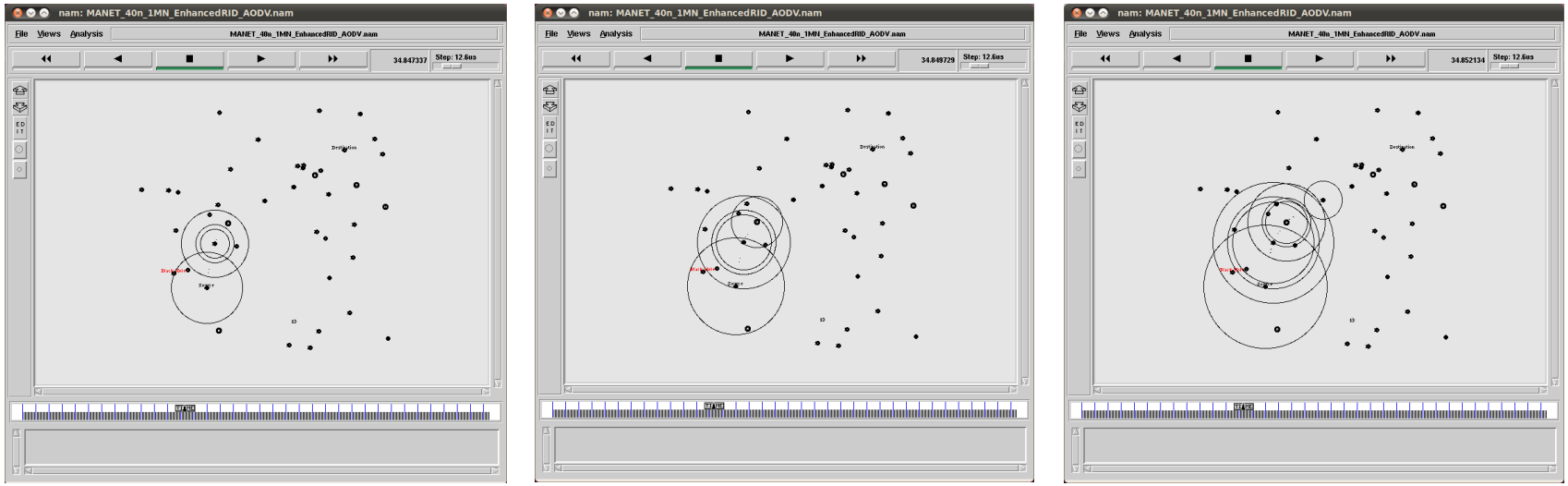

Figure 5.3: Screenshots when using "Enhanced RID-AODV" – traffic is routed to avoid black hole node

It's clear from the figures that the use of blacklists during making decisions of packet forwarding has advantages in avoiding the malicious nodes (black hole nodes) and to use only the legitimate nodes for routing data packets to reach the intended destination.

5.5.1 Results of the First Scenario:

In the first scenario, we made the nodes moving in a maximum speed = 20 m/s. Table 5.2 shows the results of the throughput for the case of the existence of black hole nodes (as the number of black hole nodes increases up to 7 malicious nodes), and these results are illustrated graphically in figure 5.4.

Table 5.2: Effect of number of malicious nodes on throughput for different protocols in first scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	3.98	15.96	25.23	38.05	41.16
2	1.87	8.51	25.85	38.66	40.40
3	2.16	7.86	26.49	37.71	40.58
4	1.08	5.60	26.36	38.80	40.48
5	0.68	4.36	27.30	38.14	40.62
6	0.29	2.79	26.17	37.69	40.84
7	0.00	1.92	26.42	36.55	40.97

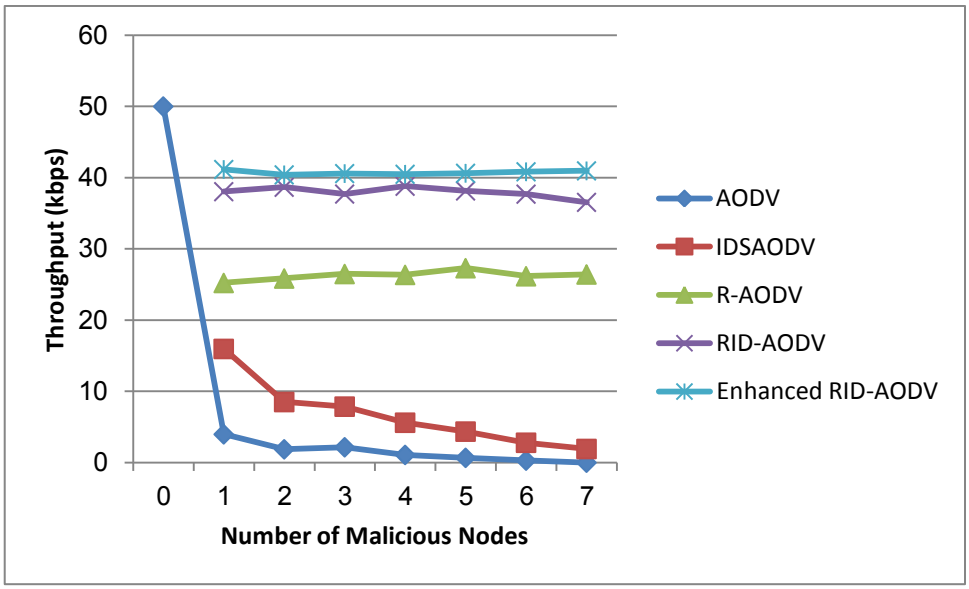

Figure 5.4: Throughput vs. number of malicious nodes for different protocols in first scenario

We can notice, from the figure, the effects of increasing the number of malicious nodes in the network on the throughput. One black hole in the network has a huge impact in decreasing the throughput, and few numbers of malicious nodes are able to prevent all traffic from reaching the destination. IDSAODV provides a small improvement to throughput; but, this is not enough because the throughput is still very low. R-AODV provides more improvement and stability to the throughput as the number of malicious nodes increases. RID-AODV also improved the throughput. The Enhanced RID-AODV protocol provides more improvement to throughput and takes advantages of its preceding in stability and robustness in avoiding multiple black hole nodes.

The packet delivery ratio (PDR) was computed for the using equation (5.2), the results are shown in table 5.3 and graphically in figure 5.5.

Table 5.3: Effect of number of malicious nodes on PDR for different protocols in first scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	7.44	29.84	47.16	71.12	76.94
2	3.50	15.91	48.33	72.27	75.53
3	4.03	14.70	49.52	70.50	75.87
4	2.02	10.47	49.28	72.54	75.68
5	1.26	8.15	51.04	71.30	75.94
6	0.54	5.22	48.92	70.46	76.34
7	0.00	3.59	49.39	68.32	76.58

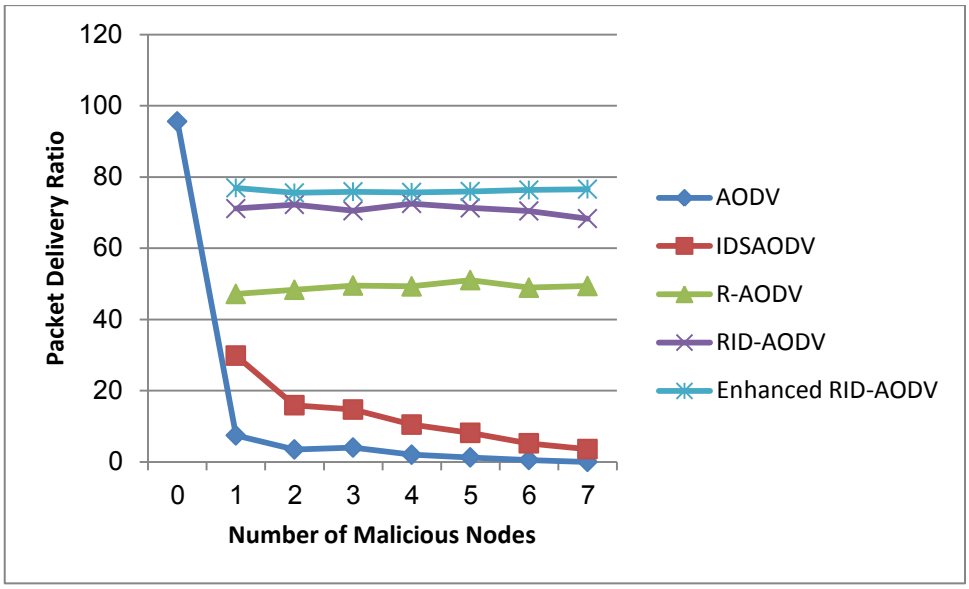

Figure 5.5: PDR vs. number of malicious nodes for different protocols in first scenario

The figure above shows the percentage of the number of receives packets by the destination node to the total number of the sent packets by the source node. It is obvious the impact of malicious nodes in dropping the packets to reduce the received packets. Only one black hole node in the network is able to reduce the PDR to around 10% of the original PDR. We can notice the improvements provided by IDSAODV, R-AODV and RID-AODV protocols. Also, this figure verifies the efficiency of the Enhanced RID-AODV protocol in improving the PDR and in providing stability against increasing the number of malicious nodes.

One of the major improvements of the Enhanced RID-AODV is decreasing the average end-to-end delay. This performance metric was computed for the proposed protocol and the preceding ones, the results are shown in table 5.4 and figure 5.6.

Table 5.4: Effect of number of malicious nodes on Average End-to-End Delay for different protocols in first scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	9.06	29.50	46.61	79.69	44.07
2	0.40	13.28	34.48	72.35	52.24
3	0	8.52	38.87	64.77	51.08
4	0	4.62	30.17	65.94	55.21
5	0	2.57	34.31	64.66	49.95
6	0	1.28	26.84	59.78	49.98
7	0	0	26.60	70.65	45.86

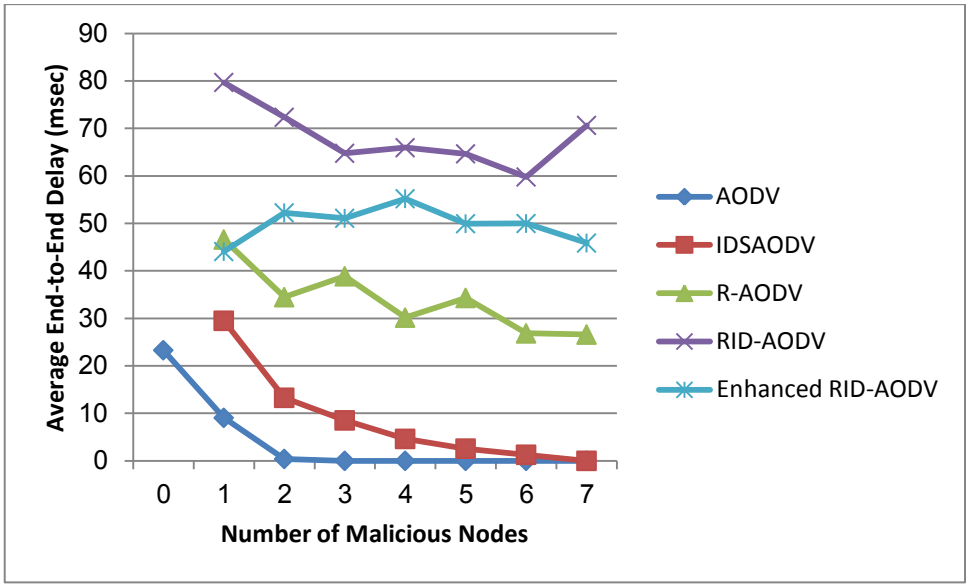

Figure 5.6: Effect of number of malicious nodes on Average End-to-End Delay for different protocols in mitigating multiple black hole attacks.

From the results in the table and the figure, it is clear that the previous protocols have an impact in increasing the average end-to-end delay with the increase in the throughput and PDR. However; the Enhanced RID-AODV, due to the use of blacklists the nodes chooses the optimized path. As a result the average end-to-end delay has decreased as compared to RID-AODV. This is an important improvement because time is a significant factor in ad hoc networks.

Also the overhead ratio has been improved by the proposed protocol. Results of applying Enhanced RID-AODV protocol and the preceding protocols on overhead are shown in table 5.5 and figure 5.7.

Table 5.5: Effect of number of malicious nodes on Overhead Ratio for different protocols in first scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	5.90	5.19	16.55	13.74	12.20
2	5.43	4.92	16.58	13.33	12.13
3	4.59	5.26	16.86	13.43	11.74
4	4.36	5.05	16.68	13.25	11.95
5	3.42	5.01	16.68	13.41	11.91
6	3.08	4.37	16.80	13.12	11.75
7	2.66	4.44	16.41	14.04	11.89

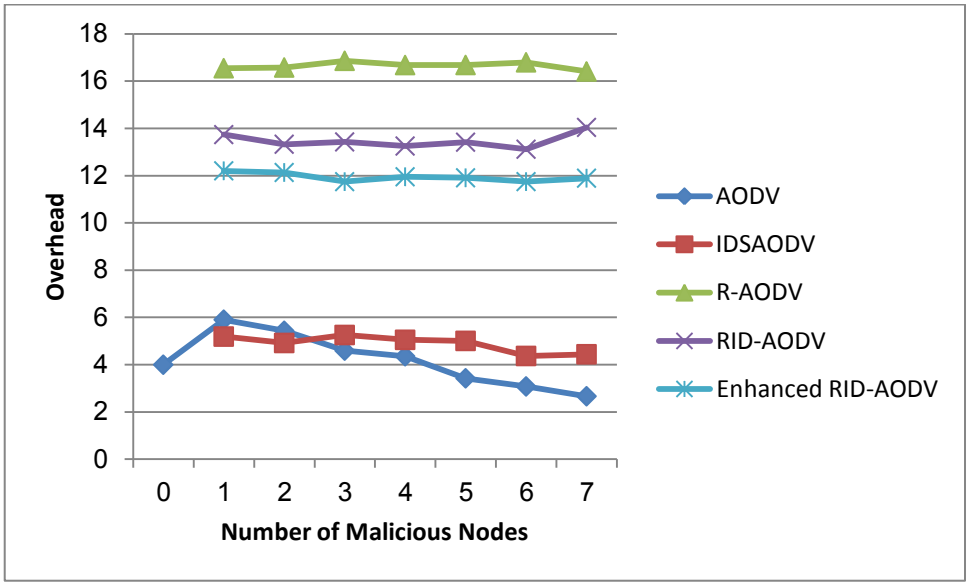

Figure 5.7: Overhead Ratio vs. number of malicious nodes for different protocols in first scenario

The previous protocols not only increase the end-to-end delay but also impose more overhead. The increase of the overhead ratio is mainly due to the new R-RREQ message. However, as a result of applying blacklists in the intermediate nodes, some control packets are prevented to be transmitted across the network. As a result, the overhead ratio decreased.

5.5.2 Results of the Second Scenario:

In the second scenario, the intermediate nodes are moving in a maximum speed of 30 m/s. The four performance metrics have been computed for this scenario. Throughput results for this scenario are presented in table 5.6 and shown in figure 5.8 below.

Table 5.6: Effect of number of malicious nodes on throughput for different protocols in second scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	4.34	17.01	29.14	38.45	41.16
2	0.9	12.73	28.14	38.46	41.98
3	0.41	9.55	28.29	37.98	40.84
4	0.13	4.76	26.92	39.45	41.3
5	0.51	4.73	28.21	39.39	41.66
6	0.29	3.53	28.04	36.76	40.89
7	0	3.01	27.43	38.55	41.9

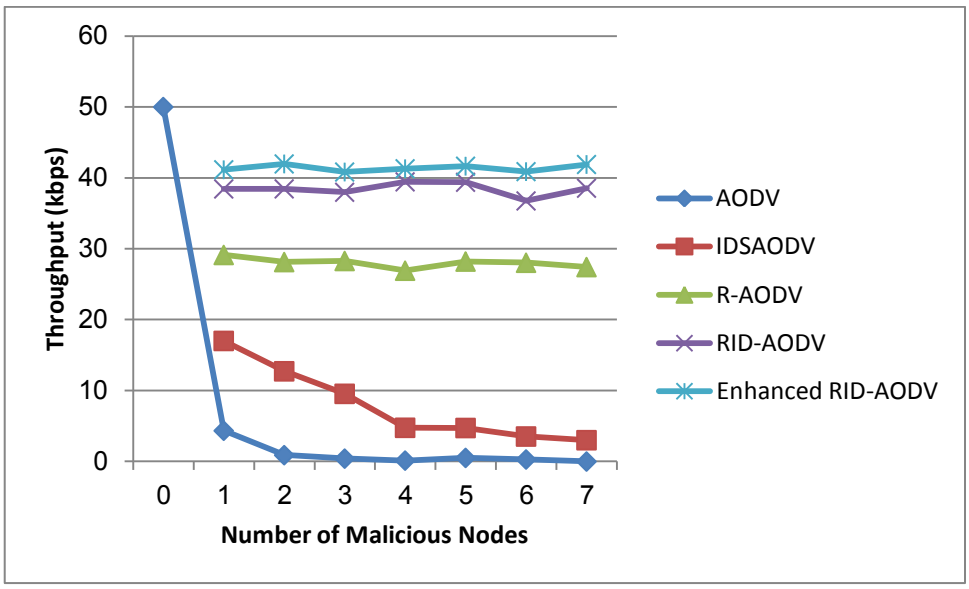

Figure 5.8: Throughput vs. number of malicious nodes for different protocols in second scenario

As shown in the figure, throughput has been improved in this scenario by applying the previous mechanisms. The Enhanced RID-AODV provides an improvement as compared with its preceding RID-AODV.

Packet delivery ratio (PDR) results for the second scenario are shown in table 5.7 and in figure 5.9 below:

Table 5.7: Effect of number of malicious nodes on PDR for different protocols in second scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	8.11	31.8	54.49	71.87	76.94
2	1.68	23.81	52.61	71.89	78.47
3	0.76	17.85	52.88	71	76.34
4	0.24	8.9	50.33	73.75	77.21
5	0.95	8.85	52.75	73.64	77.88
6	0.54	6.6	52.41	68.71	76.44
7	0	5.62	51.27	72.07	78.32

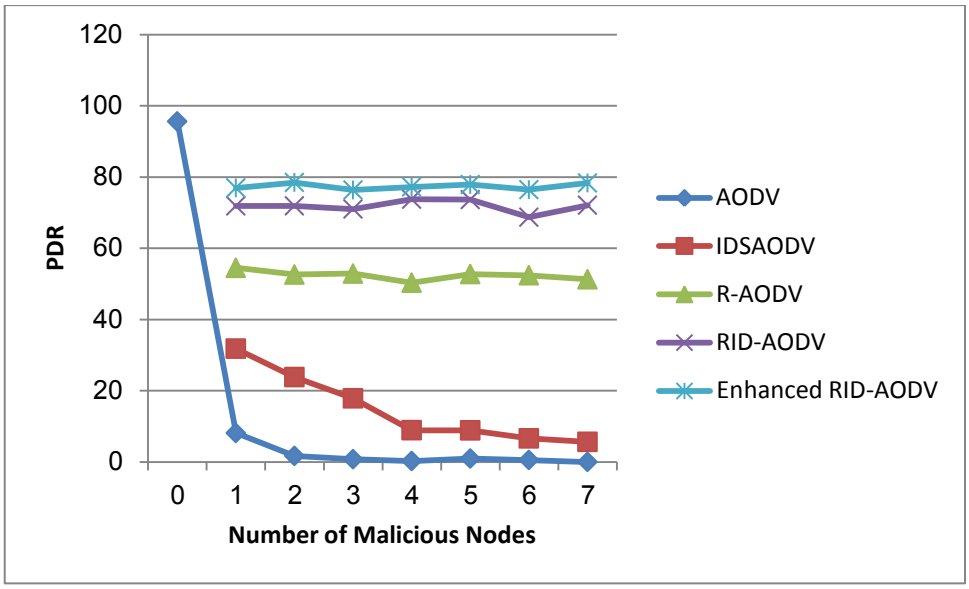

Figure 5.9: PDR vs. number of malicious nodes for different protocols in second scenario

It is obvious that the percentage number of received data by the destination node has been improved by the Enhanced RID-AODV protocol more than with previous protocols. We note also that the PDR value with no malicious nodes does not reach 100%, that because of the effect of the normal link failure due to mobility of the intermediate nodes that communicated wirelessly.

Average end-to-end delay results for the second scenario are shown in table 5.8 and figure 5.10 below:

Table 5.8: Effect of number of malicious nodes on Average End-to-End Delay for different protocols in second scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	20.97	29.57	30.35	87.86	62.91
2	1.4	14.22	28.68	84.18	60.5
3	0	9.64	24.85	72.02	53.9
4	0	1.29	27.46	80.72	56.95
5	0	2.35	27.4	88.63	66.33
6	0	3.7	20.8	87.01	66.43
7	0	1	22.22	74.84	48.1

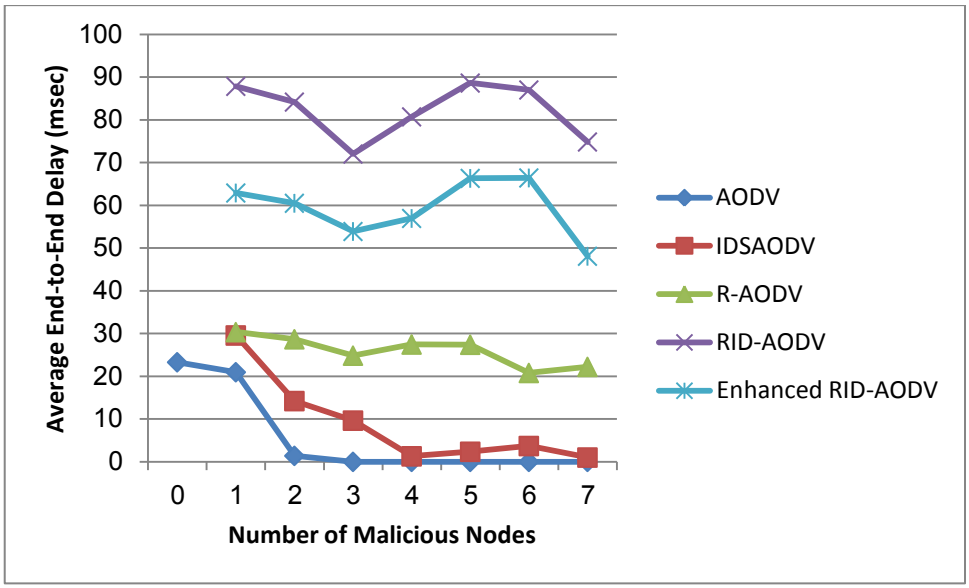

Figure 5.10: Average End-to-End Delay vs. number of malicious nodes for different protocols in second scenario

Also in the second scenario, the results of applying the Enhanced RID-AODV protocol show that the average end-to-end delay has decreased. This prove the efficiency of this protocol.

Overhead ratio results for the second scenario are shown in table 5.9 and figure 5.11 below:

Table 5.9: Effect of number of malicious nodes on Overhead Ratio for different protocols in second scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	6.32	5.92	14.83	12.15	11.9
2	5.52	6.29	15.67	12.43	11.16
3	4.51	5.43	14.97	11.69	10.95
4	4.53	5.59	15.72	12.21	10.83
5	3.73	5.29	15.89	12.1	10.73
6	1.02	5.53	15.33	11.27	10.77
7	2.71	5.45	15.38	11.52	11.13

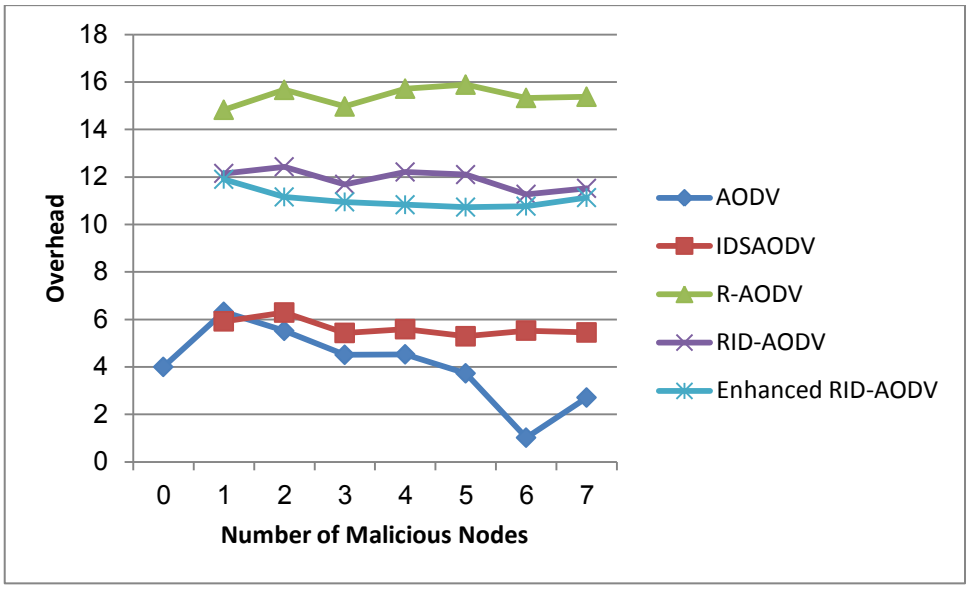

Figure 5.11: Overhead Ratio vs. number of malicious nodes for different protocols in second scenario

Similar to the first scenario, the overhead ratio has decreased as a result of using the Enhanced RID-AODV protocol due to the effect of the blacklists.

5.5.3 Results of the third scenario:

In the third scenario, the nodes are moving in a maximum speed = 40 m/s. Results of the throughput in this scenario are illustrated in Table 5.10 and illustrated in figure 5.12 below.

Table 5.10: Effect of number of malicious nodes on throughput for different protocols in third scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	3.24	13.34	26.18	37.09	41.07
2	0.51	9.9	26.72	37.27	40.42
3	0.24	5.15	26.04	37.31	40.92
4	0.25	4.77	26.35	35.75	39.13
5	0	1.55	27.37	36.93	38.17
6	0	3.04	26.73	35.38	39.74
7	0	3.25	26.29	36.74	38.77

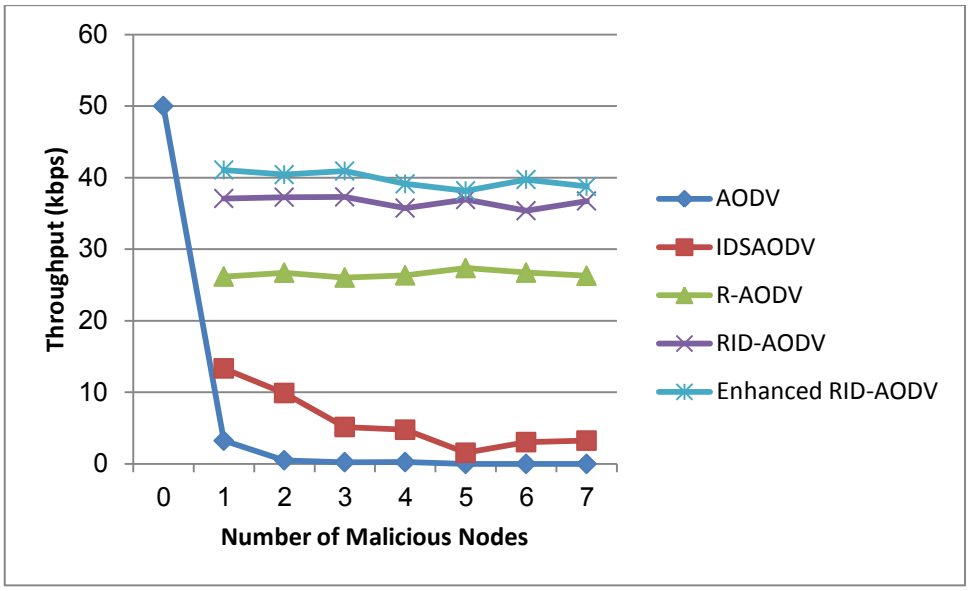

Figure 5.12: Throughput vs. number of malicious nodes for different protocols in third scenario

Also in this scenario, the Enhanced RID-AODV has the highest throughput among other protocols in this study.

Packet delivery ratio (PDR) results for the third scenario are shown in table 5.11 and figure 5.13 below:

Table 5.11: Effect of number of malicious nodes on PDR for different protocols in third scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	6.06	24.94	48.94	69.34	76.77
2	0.95	18.5	49.96	69.67	75.56
3	0.44	9.62	48.67	69.74	76.51
4	0.48	8.91	49.26	66.83	73.15
5	0	2.89	51.16	69.04	71.36
6	0	5.68	49.96	66.14	74.29
7	0	6.08	49.15	68.68	72.47

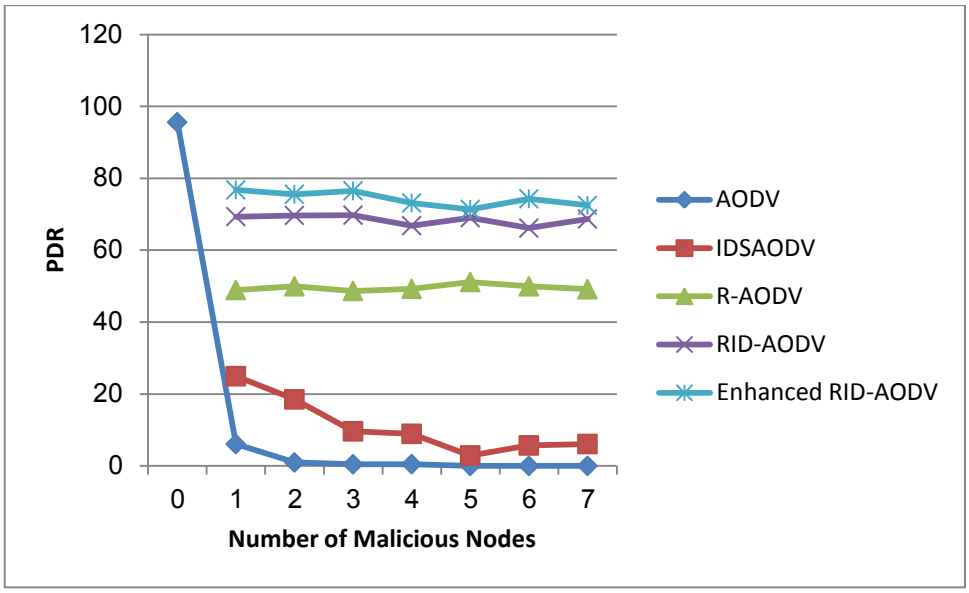

Figure 5.13: PDR vs. number of malicious nodes for different protocols in third scenario

As the maximum speed of the intermediate nodes has increased, using the Enhanced RID-AODV protocol provides the highest packet delivery ratio.

Average end-to-end delay results for the third scenario are shown in table 5.12 and figure 5.14 below:

Table 5.12: Effect of number of malicious nodes on Average End-to-End Delay for different protocols in third scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	7.07	22.68	21.22	87.47	50.65
2	0.22	9.71	22.1	82.32	46.34
3	4.33	2.63	23.76	87.53	64.39
4	0	3.83	24.02	74.31	65.13
5	0	2.69	25.74	82.06	64.67
6	0	2.71	27.15	73.92	58.52
7	0	1.61	32.03	81.86	58.63

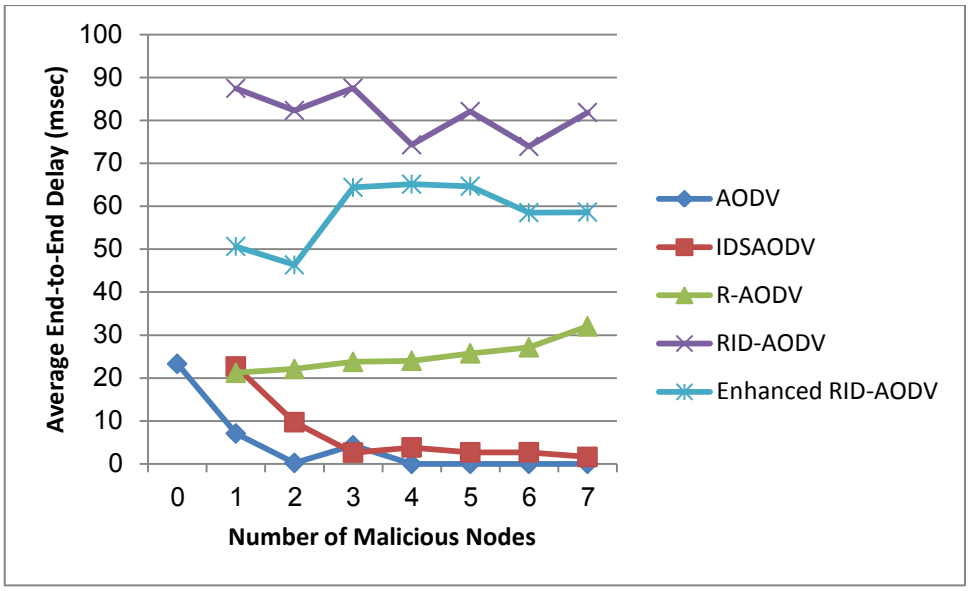

Figure 5.14: Average End-to-End Delay vs. number of malicious nodes for different protocols in third scenario

In this scenario the average end-to-end delay has decreased as compared to RID-AODV providing enhancements in all scenarios.

Overhead ratio results for the third scenario are shown in table 5.13 and figure 5.15 below:

Table 5.13: Effect of number of malicious nodes on Overhead Ratio for different protocols in third scenario

No. of black hole nodes	AODV	IDSAODV	R-AODV	RID-AODV	ERID-AODV
1	5.88	5.85	16.45	11.64	11.21
2	5.1	5.89	16.59	12.07	11.02
3	5.42	5.77	16.77	11.76	10.7
4	4.36	5.46	16.69	12.24	11.04
5	2.78	4.84	16.1	11.89	11.29
6	4.18	4.93	17.06	12.11	10.66
7	2.62	5.59	16.18	12.11	11.24

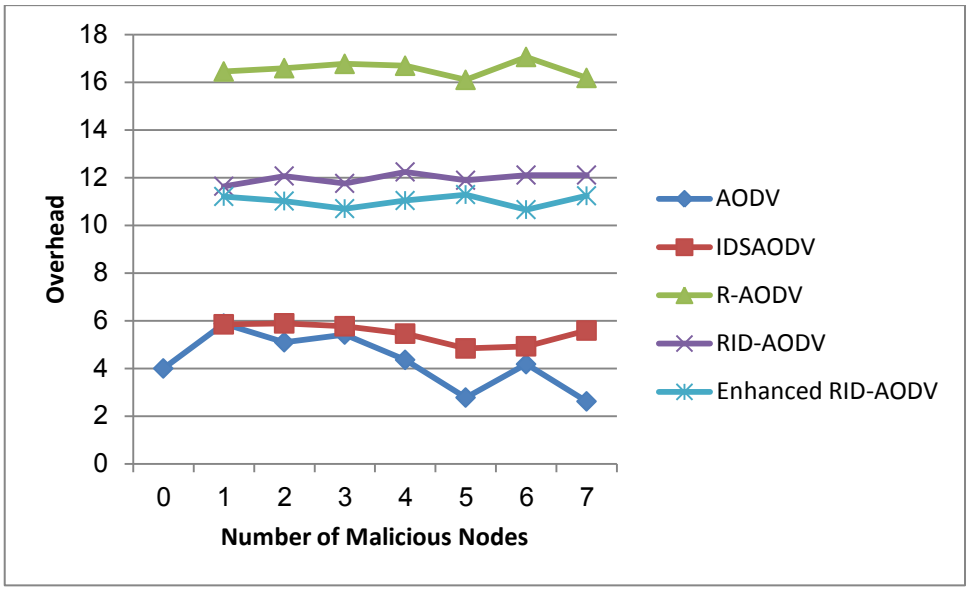

Figure 5.15: Overhead Ratio vs. number of malicious nodes for different protocols in third scenario

The enhanced RID-AODV protocol required less overhead than R-AODV and RID-AODV protocols in this scenario also as shown in the figure.

5.6 Summary of Results Analysis:

1. Simulation results show that only one black hole in the network - without any solution - is able to decrease the PDR to almost 10% of its value without black hole. And only a small number of black holes in the network are able to reduce the throughput and the packet delivery ratio to almost zero resulting in denial of service (DoS) for the legitimate nodes.

2. It is obvious from the figures that the proposed protocol is suitable for mitigating multiple black hole attacks because of the stability in the curves while increasing the number of malicious nodes that are acting the black hole attack.

3. Average *end-to-end delay* has decreased in the proposed protocol as compared to the preceding one in all scenarios with the following rates:

a. In scenario 1 end-to-end delay has decreased by 27.1 % in average.
b. In scenario 2 end-to-end delay has decreased by 27.8 % in average.
c. In scenario 3 end-to-end delay has decreased by 28.3 % in average.
d. For all cases (as an average) end-to-end delay has decreased by 27.7 %

4. There is an increase in *throughput* also in all scenarios:
    a. In scenario 1 throughput has increased by 7.3 %
    b. In scenario 2 throughput has increased by 7.7 %
    c. In scenario 3 throughput has increased by 8.5 %
    d. For all cases (as an average) throughput has increased by 7.8 %

5. Enhancement in *Packet Deliver Ratio (PDR)* in all scenarios as follows:
    a. In scenario 1 PDR has increased by 5.2%.
    b. In scenario 2 PDR has increased by 5.5 %
    c. In scenario 3 PDR has increased by 5.8 %
    d. For all cases (as an average) PDR has increased by 5.5 %

6. *Overhead ratio* also has decreased as compared to the preceding protocol but in small percentage:
    a. In scenario 1 overhead ratio has decreased by 1.53 %
    b. In scenario 2 overhead ratio has decreased by 0.84 %
    c. In scenario 3 overhead ratio has decreased by 0.95 %
    d. For all cases (as an average) overhead has decreased by 1.11 %

As a summery, we can say that the major enhancement in our protocol "Enhanced RID-AODV" was in reducing the average end-to-end delay which is a very important factor in the ad hoc networks because they are used in vital and critical applications that requires fast installation and fast data transfer. In addition we gained an increase the throughput and the packet delivery ratio, also a small decrease in the overhead ratio.

5.7 Summary:

In this chapter, we provide our simulation experiments that were carried out in order to verify the performance of the proposed protocol "Enhanced RID-AODV". Our results and analysis are based on four performance metrics: Throughput, Packet Delivery Ratio (PDR), Average End-to-End Delay and overhead ratio. There were three scenarios for network environment in the simulation process. In each scenario, the intermediate nodes are moving in different speed.

As a summary of the results, "Enhanced RID-AODV" shows a better performance as compared to its proceedings. The use of blacklist in each node makes these nodes to select the optimized path for the traversing packets across the network. The average end-to-end delay and the overhead ratio have been decreased and the throughput and PDR have been increased in all scenarios.

Chapter Six

Conclusion and Future Works

6.1 Thesis Conclusion

6.2 Future Work

6.1 Thesis Conclusion:

MANET has some unique helpful characteristics that make the design of suitable security mechanisms a very challenging and important issue. As security is the main obstacle for adoption of mobile ad hoc networks in many applications, a lot have to be done to ensure security in these networks to be used in practical applications.

This thesis aims mainly at providing Enhanced RID-AODV protocol that is capable to avoiding multiple malicious nodes that are acting as black hole nodes in mobile ad hoc networks (MANETs). The proposed protocol provides an enhancement to a preceding existing protocol, which is also a combination of two other protocols. The problem in the previous protocols, which we tried to solve in our protocol, is imposing more overhead and increasing end-to-end delay.

Enhanced RID-AODV protocol is distinguished from its preceding ones because it is light weighted and simulation results show an increase in throughput and packet delivery ratio, while the average end-to-end delay and overhead ratio have been decreased. Due to the fact that the proposed protocol is based on creating dynamic blacklist in each node aiming at preventing using the neighbouring malicious nodes as intermediate nodes. So, the nodes will choose the optimized path from the source to the destination.

Many cases and scenarios were simulated to check the performance of the proposed protocol and compare it with the preceding ones. The simulation results show the improvement in performance metrics in all cases.

6.2 Future Work:

Enhanced RID-AODV protocol may provide a general solution for many network layer attacks that target the routing process. So, it is recommended to check this protocol on other network layer attacks.

In this version of Enhanced RID-AODV protocol, each node in the MANET creates its own blacklist and when a node adds another node's address to its blacklist, that node will be blacklisted for a pre-specified period of time. This aims at giving a chance for a falsely blacklisted node to be removed from the blacklist. However, if there is a real malicious node, it will continue to be blacklisted then delisted then blacklisted and so on. Another suggested work is to make a reputation measure for each node by creating a counter of how many times a node has been blacklisted. This reputation measure may be used to decide how long to blacklist a malicious node. Therefore, the blocking period of a node will be a variable that is directly proportional to how many times that node has been blacklisted in its history. However, this idea should be simulated to test its performance because it may have other drawbacks.

References

[1] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC: 2501, IETF. [Online]. Available: http://tools.ietf.org/html/rfc2501

[2] A. Bakshi, A.K.Sharma and A. Mishra, "Significance of Mobile AD-HOC Networks (MANETS)", International Journal of Innovative Technology and Exploring Engineering (IJITEE). Volume-2, Issue-4, March 2013. ISSN: 2278-3075

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.

[4] A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, 2013.

[5] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs". 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[6] H. Aldabbas, T. Alwada'n, H. Janicke and A. Al-Bayatti, "Data Confidentiality in Mobile Ad hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 1, February 2012, DOI : 10.5121/ijwmn.2012.4117

[7] L. Raja, Capt. Dr. S. Santhosh Baboo, "An Overview of MANET: Applications, Attacks and Challenges", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 408-417, ISSN 2320–088X

[8] Aarti and Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, ISSN: 2277 128X

[9] J. Hoebeke, I. Moerman, B. Dhoedt and P. Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", The Journal of the Communications Network, vol. 3, no. 3, 2004, pp. 60-66

[10] N. Zanoon, N. Albdour, H. S. A. Hamatta1, and R. Al-Tarawneh, "SECURITY CHALLENGES AS A FACTOR AFFECTING THE SECURITY OF MANET: ATTACKS, AND SECURITY SOLUTIONS", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015, DOI : 10.5121/ijnsa.2015.7301

[11] S. U. Agalawe and N. R. Chopde, "SECURITY ISSUES: THE BIG CHALLENGE IN MANET", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014, pg. 417-424, ISSN 2320–088X

[12] P. Visalakshi and S. Anjugam, "Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey", International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005.

[13] B. Lu, "Handbook of Research on Wireless Security," in Security in Mobile Ad Hoc Networks, Inormation Science Reference, (West Chester University, USA) 2008, Sec. 3, Ch. 26

[14] G. Aashima and P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review," International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012, ISSN: 2249 – 8958

[15] H. Yang, H. Y. Luo, F. Ye, S. W. Lu and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions" (2004). IEEE Wireless Communications. vol. 11 (1), pp. 38-47.

[16] R. Sheikh, M. S. Chandee and D. K. Mishra, "Security Issues in MANET: A Review," 2010 Seventh International Conference On Wireless And Optical Communications Networks (WOCN), Sept. 2010, pp. 1-4, DOI: 10.1109/WOCN.2010.5587317

[17] A. Dorri, S. R. Kamel and E. kheyrkhah, "SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015, DOI:10.5121/ijcses.2015.6102

[18] A. A. Morey and J. W. Bakal, "Review of a Secure Approach to Prevent Packet Dropping and Message Tampering Attacks on AODV-based MANETs", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (3) , 2015, 2373-2376

[19] L. Tamilselvan and V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008

[20] S. Kurosawa, H. Nakayama, N. Kat, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, pp. 338-346, Nov. 2007

[21] K. El Defrawy and G. Tsudik, "PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs)", Proc. IEEE Int'l Conf. Network Protocols (ICNP '08), pp. 258-267, Oct. 2008.

[22] A. Kanthe, D. Simunic , R. Prasad, "Effects of Malicious Attacks in Mobile Ad-hoc Networks", 2012 IEEE International Conference on Computational Intelligence and Computing Research, ISBN:978-1-4673-2481-6,18-20, December 2012, Coimbatore, India.

[23] I. Aad, P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, Vol. 16, No. 4, 2008, pp. 791- 802.

[24] D. Mishra, K. Y. Jain and S. Agarwal, "Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)", Proceeding from ACT'09: IEEE Advances in Computing, Control and Telecommunication Technologies, Trivandrum, 28-29 December 2009, pp. 621-623.

[25] E. Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", Proc. IEEE Conference on Local Computer Networks, 2007.

[26] S. Buchegger and J.Y.L. Boudec "A Robust Reputation System for Mobile Ad-hoc Networks", Technical Report, IC/2003/50, EPFL/IC/LCA, Lausanne, Switzerland, July 2003.

[27] H. Deng, W. Li and D.P. Agrawal, "Routing security in wireless Ad Hoc networks", Cincinnati University of Cincinnati, OH, USA; IEEE Communications Magazine, ISSN: 0163-6804, Vol.40, Oct. 2002, pp.70- 75

[28] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," 2002 International Conference on Parallel Processing Workshops, pp. 73-78 Vancouver, Canada, Aug, 2002. DOI: 10.1109/ICPPW.2002.1039714

[29] P.A.R Kumar, S.Selvakumar, "Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms", IEEE International Advance Computing Conference (IACC 2009), pp. 1275-1280, March, 2009

[30] D. Wadbude, V. Richariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, 2012, pp. 274-279

[31] L. Himral, V. Vig and N. Chand, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[32] M. Shakshuki, N. Kang and Sheltami,"EAACK- A Secure Intrusion-DetectionSystem for MANETs", IEEE Transactions on Industrial Electronics, vol. 60, no. 3, March 2013.

[33] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[34] O. Shree, F. J. Ogwu, "A Proposal for Mitigating Multiple Black-Hole Attack in Wireless Mesh Networks", Wireless Sensor Network, vol. 5, no. 4, pp- 76-83, 2013.

[35] C. Kim, E. Talipov, and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks", The International Conference on Emerging Directions in Embedded and Ubiquitous Computing (EUC'06), Seoul, 1-4 August 2006, pp. 522-531. Springer, 2006.

[36] S. K. Sarkar, T.G. Basavaraju and C. Puttamadappa, "Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications", 2nd Edition, Boca Raton: CRC Press, FL, USA, 2013

[37] A. Hinds, M. Ngulube, S. Zhu, and H. Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, Feb. 2013, DOI: 10.7763/IJIET.2013.V3.223

[38] S. Habib, S. Saleem and K. M. Saqib, "Review on MANET Routing Protocols and Challenges", 2013 IEEE Student Conference on Research and Development (SCOReD), 16 -17 December 2013, Putrajaya, Malaysia

[39] Priyanshu and A. K. Maurya, "SURVEY: COMPARISON ESTIMATION OF VARIOUS ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORK", International Journal of Distributed and Parallel Systems (IJDPS) Vol.5, No.1/2/3, May 2014, DOI : 10.5121/ijdps.2014.5309

[40] X. Hong, K. Xu, and M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks", IEEE Networks, Vol. 16, Issue 4, pp. 11-21, Jul/Aug 2002

[41] A. K. Gupta, H. Sadawarti, and A. K. Verma, "Review of Various Routing Protocols for MANETs", International Journal of Information and Electronics Engineering, Vol. 1, No. 3, Nov. 2011

[42] M. N. Abdulleh, S. Yussof and H. S. Jassim, "Comparative Study of Proactive, Reactive and Geographical MANET Routing Protocols", Communications and Network, Vol. 7, pp. 125-137, doi:10.4236/cn.2015.72012

[43] T. Javed and S. Zafar, "Delay Analysis of Manet Routing Protocols", World Applied Sciences Journal, vol. 19, No. 5, pp. 615-620, 2012 DOI: 10.5829/idosi.wasj.2012.19.05.1529

[44] L. Raja, Capt. Dr. S. Santhosh Baboo, "Comparative study of reactive routing protocol (AODV, DSR, ABR and TORA) in MANET", International Journal Of

Engineering And Computer Science, ISSN:2319-7242, Vol. 2, No. 3, pp. 707-718, Mar. 2013

[45] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing", Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, LA, Feb. 1999, pp. 90-100

[46] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC: 3561, IETF. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[47] P. Nand and Dr. S.C. Sharma, "Routing Load Analysis of Broadcast based Reactive Routing Protocols AODV, DSR and DYMO for MANET", International journal of grid and distributed computing vol. 4, No. 1, pp. 81-92, Mar 2011

[48] K. Vanaja and Dr. R. Umarani, "An Enriched Reactive Routing Protocol - AODV for Mobile Adhoc Networks", International Journal of Computer Communication and Information System (IJCCIS), Vol. 2, No. 1, July–Dec 2010, ISSN: 0976–1349

[49] M. N. Alslaim, H. A. Alaqel and S. S. Zaghloul, "A Comparative Study of MANET Routing Protocols", IEEE 2014 Third International Conference on e-Technologies and Networks for Development (ICeND), Apr-May 2014, pp. 178-182, DOI: 10.1109/ICeND.2014.6991375

[50] C. Perkins, S. Ratliff, J. Dowdell, L. Steenbrink and V. Mercieca, "Dynamic MANET On-demand (AODVv2) Routing draft-ietf-manet-aodvv2-07" Internet Engineering Task Force, Mar. 2015. [Online]. Available: https://tools.ietf.org/html/draft-ietf-manet-aodvv2-07

[51] Anuj K. Gupta, Harsh Sadawarti and Anil K. Verma, "IMPLEMENTATION OF DYMO ROUTING PROTOCOL ", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol.1, No.2, May 2013, page(s):49-57.

[52] Narendran Sivakumar and Satish Kumar Jaiswal, "Comparison of DYMO protocol with respect to various quantitative performance metrics", ircse 2009

[53] Sukant K. Bisoyi and Sarita Sahu, "Performance analysis of Dynamic MANET On-demand (DYMO) Routing protocol.", IJCCT Vol.1, International Conference (ACCTA-2010), August 2010.

[54] D. Johnson, Y. Hu and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC: 4728, IETF. [Online]. Available: http://www.ietf.org/rfc/rfc4728.txt

[55] G.S. Aujla and S.S. Kang, "Comprehensive Evaluation of AODV, DSR, GRP, OLSR and TORA Routing Protocols with varying number of nodes and traffic applications over MANETs", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 9, Issue 3, pp. 54-61, Mar/Apr 2013

[56] D.S. Som and D. Singh, "Performance Analysis and Simulation of AODV, DSR and TORA Routing Protocols in MANETs", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Vol. 1, Issue 3, Aug. 2012

[57] A. Aggarwal, S. Gandhi and N. Chaubey, "PERFORMANCE ANALYSIS OF AODV, DSDV AND DSR IN MANETS", International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, Nov. 2011, DOI: 10.5121/ijdps.2011.2615

[58] S. Sen, J.A. Clark and J.E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, Auerbach Publications 2010, pp. 127–145, DOI: 10.1201/EBK1439819197-9

[59] S.B. Sharma and N. Chauhan, "Security issues and their solutions in MANET", IEEE International Conference on Futuristic Trends on Computational Analysis and

Knowledge Management (ABLAZE), pp.289-294, 25-27 Feb. 2015, doi: 10.1109/ABLAZE.2015.7155013

[60] E. Cayirci and C. Rong, "Security in Wireless Ad Hoc and Sensor Networks", John Wiley and Sons Ltd, 2009, ISBN 978-0-470-02748-6

[61] A. Saeed, A. Razaa and H. Abbas, "A Survey on Network Layer Attacks and AODV Defence in Mobile Ad hoc Networks", 2014 IEEE Eighth International Conference on Software Security and Reliability-Companion (SERE-C), Jun/Jul, 2014, pp. 185-191, DOI: 10.1109/SERE-C.2014.37

[62] S. Behzad and S. Jamali, "A Survey over Black hole Attack Detection in Mobile Ad hoc Network", International Journal of Computer Science and Network Security (IJCSNS), Vol.15 No.3, March 2015

[63] E. Cayirci and R. Ghergherehchi, "MODELING CYBER ATTACKS AND THEIR EFFECTS ON DECISION PROCESS", IEEE conference Proceedings of the 2011 Winter Simulation Conference, pp. 2632-2641, Dec. 2011, DOI: 10.1109/WSC.2011.6147970

[64] C.K. Vanamala, P. Singhania and M.S. Kumar, "A SURVEY OF DIFFERENT LETHAL ATTACKS ON MANETs", International Journal of Advancements in Research & Technology, Vol. 3, Issue 3, Mar. 2014, ISSN 2278-7763

[65] G.J. Moses, P.S. Varma, N. Supriya and G. NagaSatish, "Security Aspects and Challenges in Mobile Adhoc Networks", International Journal of Computer Network and Information Security 2012, vol. 6, pp. 26-32, DOI: 10.5815/ijcnis.2012.06.04

[66] A. Abdelaziz, N. Mehdi and G. Salim, "Analysis of Security Attacks In AODV", 2014 IEEE International Conference on Multimedia Computing and Systems (ICMCS), Morocco, Apr. 2014, pp. 752-756, DOI: 10.1109/ICMCS.2014.6911193

[67] A. Abdelaziz, M. Nafaa and G. Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks" 15th IEEE International Conference on Computer Modelling and Simulation 2013 (UKSim), Apr. 2013, pp. 693-698, DOI: 10.1109/UKSim.2013.48

[68] Y. khamayseh, A. Bader, W. Mardini and M. BaniYasein, "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 1, April 2011

[69] H. Noori, "Realistic Urban Traffic Simulation as Vehicular Ad-Hoc Network (VANET) via Veins Framework", 12th Conference of Open Innovations Framework Prgramm. FRUCT, Nov.2012.

[70] T. Issariyakul and E. Hossain, "Introduction to Network Simulator NS2" Springer, 2009, DOI: 10.1007/978-0-387-71760-9

[71] The Network Simulator ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns

[72] N. Hegde and S. Manvi, "Simulation of Wireless Sensor Network Security Model Using NS2", International Journal of Latest Trends in Engineering and Technology (IJLTET). Vol. 4 May 2014

[73] C. Manikandan, R.Parameshwaran, K.Hariharan, N.Kalaimani and K.P. Sridhar, "Combined Security and Integrity Agent Integration into NS-2 for Wired, Wireless and Sensor Networks" Australian Journal of Basic and Applied Sciences, 7(7): 376-382, 2013 ISSN 1991-8178

Appendix A:

Acronyms and Abbreviations

MANET	Mobile Ad Hoc Network
DSDV	Destination-Sequenced Distance-Vector Routing
OLSR	Optimized Link State Routing Protocol
AODV	Ad Hoc On-Demand Distance Vector
DSR	Dynamic Source Routing
DYMO	Dynamic MANET On-demand
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
R-RREQ	Reverse Route Request
PDR	Packet Delivery Ratio
PAN	Personal Area Networking
WLAN	Wireless Local Area Network
NS	Network Simulator
NAM	Network Animator
CREQ	Route Confirmation Request
IDSAODV	Intrusion Detection System AODV
MPR	Multi Point Relays
IETF	Internet Engineering Task Force
MAC	Medium Access Control
IP	Internet Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol

Appendix B:

Published Papers

B-1: First Paper:

Detection and Mitigation Mechanism for Multiple Black Hole Attacks in Mobile Ad Hoc Networks

Accepted and orally presented in the 4th Palestinian International Conference on Computer and Information Technology (PICCIT 2015), held on October 7-8, 2015 in Palestine Polytechnic University, Hebron, Palestine.

An extended version of this paper (titled: **Efficient Mechanism for Mitigating Multiple Black Hole Attacks in MANETs**) has been published in the Journal of Theoretical and Applied Information Technology (JATIT), Vol.83. No.1, pp. 156-164, January 2016.

Appendix B:

Published Papers

B-1: First Paper:

Detection and Mitigation Mechanism for Multiple Black Hole Attacks in Mobile Ad Hoc Networks

Accepted and orally presented in the 4th Palestinian International Conference on Computer and Information Technology (PICCIT 2015), held on October 7-8, 2015 in Palestine Polytechnic University, Hebron, Palestine.

An extended version of this paper (titled: **Efficient Mechanism for Mitigating Multiple Black Hole Attacks in MANETs**) has been published in the Journal of Theoretical and Applied Information Technology (JATIT), Vol.83. No.1, pp. 156-164, January 2016.

Journal of Theoretical and Applied Information Technology
10th January 2016. Vol.83. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT MECHANISM FOR MITIGATING MULTIPLE BLACK HOLE ATTACKS IN MANETS

ABDUL-RAHMAN SALEM, DR. RUSHDI HAMAMREH
Computer Engineering Department
Al-Quds University, Jerusalem, Palestine
E-mail: asalem@outlook.com, rhamamreh@eng.alquds.edu

ABSTRACT

Mobile ad hoc networks (MANETs) have emerged as a major next generation wireless networking technology. Due to their inherent capabilities of instant communication, they are used for wide range of applications such as emergency operations and disaster recovery. On the other hand, many challenges are facing MANETs including security, routing, transmission range and dynamically changing topology with high nodes mobility. Security is considered as the main obstacle for the widespread adoption of MANET applications. Black hole attack is a type of DoS attack that can disrupt the services of the network layer. It has the worst malicious impact on network performance as the number of malicious nodes increases. Several mechanisms and protocols have been proposed to detect and mitigate its effects using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay. This paper proposes an enhanced and modified mechanism called "Enhanced RID-AODV", based on a preceding mechanism: RID-AODV. The proposed enhancement is based on creating *dynamic blacklists* for each node in the network. Each node, according to criteria depends on the number of mismatches of hash values of received packets as compared with some threshold values, can decide to add or remove other nodes to or from its blacklist. Enhanced RID-AODV was implemented in ns-2 simulator and compared with three previous solutions for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay.

Keywords: *Enhanced RID-AODV, MANET Security, Network Layer Attack, Multiple Black Hole Attacks.*

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a self-configuring network formed by co-operating and independent nodes that connect and communicate with each other wirelessly without pre-existing infrastructure. If two mobile nodes are within each other transmission range, then they can communicate with each other directly; otherwise, the nodes in between have to forward the packet for them. So, mobile nodes are not only functioning as hosts but they are also functioning as routers [1].

Because MANETs are infrastructure-less networks with no centralized administration, they can be self deployed in short time. The easy deployment of nodes, self-organizing nature and freedom of mobility make MANETs suitable for a broad range of applications. They can be useful in disaster recovery and emergency operations where there is not enough time or resources to install and configure an infrastructure. They are also used in other applications; for example, in military services, maritime communications, vehicle networks, casual meetings, campus networks, robot networks… etc [2].

On the other hand, MANETs are vulnerable to various attacks at all layers. So, much research has been conducted on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality: intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. The network layer, especially the routing protocol, is vulnerable because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, the lack of clearly defined physical network boundary and the transient nature of services in the network. Standard information security measures such as encryption and authentication do not provide complete protection; thus, intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs [3].

Attacks in MANET can be divided, according to the criteria that whether they disrupt the operation of a routing protocol or not, into two classes: passive attacks and active attacks. In *passive attacks*, the attacker attempts to discover valuable information but does not disrupt the operation of the routing protocol. *Active attacks*;

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

however, involve actions like modification and deletion of exchanging data to absorb packets destined to other nodes to the attacker for analyzing or disabling the network. Some typical kinds of active attacks that can be performed against MANETs are: black hole attack, gray hole attack, flooding attack, selfish attack, rushing attack, spoofing, wormhole attack, sleep deprivation and impersonation [4].

Black hole attack is a type of active attack that exploits the route reply message (RREP) feature of the ad hoc on-demand distance vector (AODV) routing protocol. This attack involves some modification of the data stream or the creation of a false stream. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. A RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any other RREP messages from other neighboring nodes or even from the actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them [5].

So, the black hole attack is a DoS attack that disrupts the services of routing layer by exploiting the route discovery process of AODV. According to many research studies that focus on studying the effects of malicious attacks on network performance, the simulation results show that the black hole attack is more dangerous than other attacks in the network layer [6].

Several mechanisms and protocols have been proposed to detect and mitigate its effect using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay.

In this paper, we propose a modified and enhanced protocol, called "Enhanced RID-AODV", based on a preceding mechanism: RID-AODV. It aims to detect and mitigate the effects of multiple black hole attacks in MANETs by increasing the throughput and packet delivery ratio (PDR) and by decreasing the end-to-end delay as compared to its predecessors. The proposed idea in this paper is creating a *dynamic blacklist* in each node, then prevent sending or forwarding to blacklisted nodes in both directions for a pre-specified period of time. The criteria to add a node in the blacklist is reaching a threshold in the number of mismatched hashing value from that node. The threshold is a function of mobility (*variable threshold*) to cancel the effect of normal link failure which is most likely caused by nodes mobility. The proposed solution, "Enhanced RID-AODV", was implemented in ns-2 simulator and compared with three previous solutions (namely RID-AODV, RAODV and IDSAODV) for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay.

The rest of this paper is organized as follows: section II provides some details about the black hole attack, section III provides the related work in detection and mitigation of black hole attack. The proposed solution is introduced in section IV, the simulation and network environment are described in section V, in section VI, the analysis and the results are discussed. Finally, the conclusion is presented in section VII.

2. CLASSIFICATION OF SECURITY ATTACKS IN MANETS

Security attacks can be categorized, according to the criteria that whether they disrupt the operation of a routing protocol or not, into two broad classes: passive and active attacks. Passive attacks, where adversaries do not make any emissions, are mainly against data confidentiality. In active attacks, malicious acts are carried out not only against data confidentiality but also data integrity. Active attacks can also aim for unauthorized access and usage of the resources or the disturbance of an opponent's communications. An active attacker makes an emission or action that can be detected [7][8].

The active attacks are generally launched by compromised nodes or malicious nodes. They are classified into four groups:

- *Dropping Attacks:* Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point, most of routing protocol has no mechanism to detect whether data packets have been forwarded or not.

- *Modification Attacks:* Black hole and Sinkhole attacks are example of modification and dropping attacks. These attacks modify packets and disrupt the

Journal of Theoretical and Applied Information Technology
10th January 2016. Vol.83. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

overall communication between network nodes. In such attacks, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node then captures important routing information and uses it for further actions such as dropping or selective forwarding attacks.

- *Fabrication Attacks:* In fabrication attack, the attacker send fake message to the neighboring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages.

- *Timing Attacks:* In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.

Malicious node may illegally modify the routing information of the received messages before forwarding them, it can alter one or several fields in the message, depends on the goals that it may want to achieve. The modification may include the route request (RREQ), route reply (RREP) and/or route error (RERR) as shown in table 1 below [9].

Table 1: Possible malicious modifications of routing protocols fields messages

Fields	Messages	Modifications
Type	All	Change the message type
Flags	All	Reverse the setting
Hop count	RREQ, RREP	Decrease it to update other nodes reverse route tables, or increase it to suppress its update
RREQ ID	RREQ	Increase it to make the faked RREQ message acceptable, or decrease it to make the RREQ message unacceptable
Dest_IP	RREQ, RREP	Replace it with another IP address
Dest_SEQ	RREQ, RREP	Increase it to update other nodes forward route tables, or decrease it to suppress its update
Orig_IP	RREQ, RREP	Replace it with another IP address
Orig_Seq	RREQ	Increase it to update other nodes reverse route tables, or decrease it to suppress its update
Prefix size	RREP	Increase/Decrease the size of the subnet prefix
Lifetime	RREP	Decrease/increase it to shorten/extend the lifetime of the route entry updated by this RREP message
Dest count	RERR	Modify it according to the number of unreachable destinations included in the RERR message
Un_Dest_IP	RERR	Replace it with another IP address
Un_Dest_SEQ	RERR	Increase it to update other nodes routing table, or decrease it to suppress this entry

3. BLACK HOLE ATTACK IN MANETS

Routing protocols in Mobile Ad Hoc Networks by their nature are distributed routing protocols with the assumption that all nodes in the network will cooperate truly and participate honestly. However, the existence of malicious nodes makes this assumption not true. Such nodes may drop the packets, if they are not the destination, without forwarding them or may disrupt the routing discovery and maintenance processes resulting in abnormal network operation that affects the performance of the network and may cause denial of service [10].

A black hole attack is a kind of denial of service (DoS) where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them (drop all packets) without forwarding them to the destination [11].

In reactive routing protocols such as AODV, the destination sequence number (*dest_seq*) is used to describe the freshness of the route. A higher value of *dest_seq* means a fresher route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new *dest_seq* number larger than the current *dest_seq* number. In this way the intruder becomes part of the route to that destination [12]. Figure 1 illustrates the black hole attack where nodes S and D are the source and destination respectively and node B is the black hole.

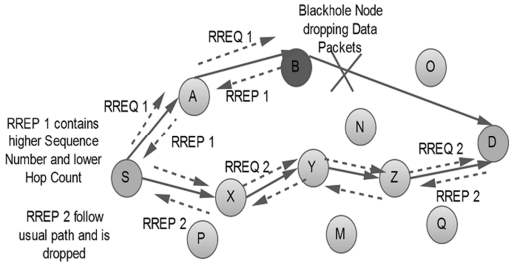

Figure 1: Black Hole Attack Illustration

A black hole has two properties: First, the node exploits the ad hoc routing protocol to advertise itself as having a valid route to a destination, even though the route is spurious with the intention of intercepting packets. Second, the node consumes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the intercepted packets. In an ad hoc network that uses the AODV protocol, a black hole node absorbs the network traffic and drops all packets [11].

4. RELATED WORK

Some research studies in the literature have focused on studying the effect of malicious nodes on network performance only without providing any solutions. However, several mechanisms and protocols using different strategies have been proposed to protect MANETs against black hole attacks. In [6] the authors studied the effect of malicious attacks in mobile ad hoc networks including black hole attack, packet drop attack and gray hole attack on AODV protocol under different performance metrics: throughput, packet drop rate and end-to-end delay. It was found that the black hole attack is more dangerous than other attacks conducted in this paper.

Paper [13] provides a quantitative study of the performance impact of black hole attacks in ad hoc networks using DSR as the routing protocol. The authors used the following performance metrics to evaluate the impact of black hole attack on network performance: System Fairness, Number of hops for received packets, Total system throughput and Probability of interception. The simulation results of the impact of black hole node on system fairness showed that with no black hole node, the system has high fairness index.

In [14], authors analyzed the effects of black hole attack in mobile ad hoc network using AODV and DSR routing protocols. For the simulation, throughput was considered as the main measure. Though the simulation results showed a higher data packet loss when using DSR as compared to AODV, the dropped packet rate was still high for both protocols. DSR data loss was around 55 - 60 percent whereas that of AODV was around 45 - 50 percent. AODV protocol provides better performance than the DSR in the presence of black holes with minimal additional delay and overhead.

A black hole detection scheme for tactical MANETs using topology graph is proposed in[15]. This mechanism is called TOGBAD. It detects the attack using a topology graph, looking at the number of neighbors a node claims to have and the actual number of neighbors according to the graph. TOGBAD was developed for the OLSR proactive routing protocol, where topology information can be obtained.

Authors of [16] proposed an approach that uses improved security mechanisms to be introduced in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. The performance of these two protocols (SAODV and ARAN) was tested in simulation and their communication costs were measured using the ns-2 simulator, which is suitable for the present purpose. The evaluation metrics used in this study were overhead and end-to-end delay. The results show good performance.

In [17] a proposed method was introduced to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is a large difference between the sequence number of source node or intermediate node that has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, then it is surely from the malicious node, immediately remove that entry from the RR-Table. The proposed method cannot find multiple black hole nodes.

In [18] the authors proposed and implemented a new intrusion detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to modern approaches, EAACK demonstrates privileged malicious behavior detection rates in definite situations while it does not greatly affect the network performances. The demonstrated results show positive performances.

A lightweight routing protocol IDSAODV was proposed in [19] as a solution for black hole attack problem in MANETs. The authors of [19] manually analyzed the output file obtained from simulation and found out very soon after the first RREP from the destination node a second RREP arrived at the source node. Through simulation, they found out that the first RREP was from the black hole node and the second RREP was from the intended destination. At this point, for future simulations, they assumed that the first RREP would always be from black hole node and modified the AODV protocol to ignore the first RREP and send using second RREP route. A RREP caching mechanism to count the second

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RREP message was added to aodv.cc file in ns-2 simulator.

The simulation results of [19] demonstrate that IDSAODV improved the PDR in a MANET with a single black hole node; thus, proving the successful implementation of the route caching mechanism.

Many of the proposed solutions that make the route establishment process longer while the nodes are moving are facing from the link failure problem. In [5], the authors addressed this issue by getting advantage of the reverse AODV (RAODV) routing protocol proposed in [20]. RAODV discovers route using reverse route discovery procedure where the destination node sends reverse-route request (R-RREQ) messages to its neighbors to find a valid route to the source node after receiving RREQ from source node. Their simulation results of RAODV show that it does improve the performance of AODV in metrics such as packet delivery ratio (PDR), end-to-end delay, and energy consumption [20].

Although RAODV has not been designed to prevent black hole attacks and it was developed with the aim of solving path failure problem, authors of [5] proposed to use it in mitigating the effects of black hole attacks in ad hoc networks. So, they proposed RID-AODV by combining RAODV (proposed in [20]) and IDSAODV (proposed in [19]) to withstand multiple black hole attacks in client-based WMNs.

5. THE PROPOSED SOLUTION

The proposed protocol, "Enhanced RID-AODV", is a modification and enhancement of the RID-AODV protocol proposed in [5]. That protocol is based on RAODV [20] and IDSAODV [19] as mentioned in the previous section. Our solution is to get advantage of the nature of the reverse route discovery procedure in RAODV. The detection of the malicious nodes and mitigation their effects can be achieved by creating and maintaining *dynamic blacklist* in each node according to some criteria. Then each non malicious node will prevent sending or forwarding to the neighboring nodes that exist in its own blacklist either in the forward or reverse path In other words, each node will not use blacklisted nodes as intermediate nodes. Dynamic blacklist means that each node adds and removes nodes to or from its blacklist automatically according to specific criteria as will be explained in this section.

In addition, we can get another advantage of the nature of the reverse route discovery procedure in RAODV to create full path (bidirectional) integrity check implemented in hop-by-hop basis to detect any modifications on the traversing packets and to detect the causing nodes.

The criteria for each node to add another node's address in its blacklist is the repetitive mismatch in the hash value of the receiving frames (layer 2 frame) from the same neighboring node. So, each node keeps a counter for each other node that receives a frame from the neighboring nodes. If there is a mismatch between the received hash value and the calculated value, the corresponding counter for the sending (or forwarding) node will be incremented. When the counter reaches some threshold value $malPcktThreshold$, then the corresponding neighboring node will be blacklisted.

If node n_i has p neighboring nodes (p is $\subseteq$ of all nodes) and n_i is receiving from q nodes ($q\ is\ \subseteq\ of\ p$), then $n_i$will keep only q counters for this purpose. For example, for the network in figure 2, the node 9 will maintain less than or equal to 5 counters.

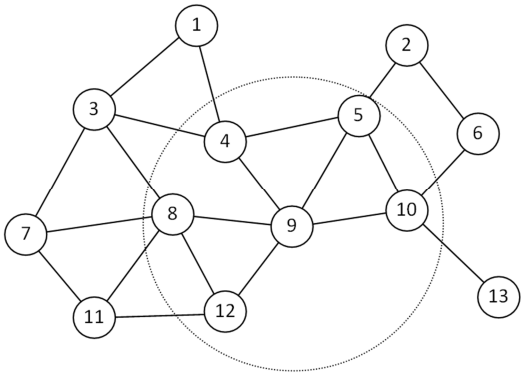

Figure 2: Each node maintains a small number of counters

To distinguish between hash value mismatch that may occur as a result of normal link failure, which is from the nature of MANETs due to mobility of nodes that communicate wirelessly, or from the existence of malicious nodes, the threshold value $malPcktThreshold$ should be considered as a function of mobility (*variable threshold*). If the node is moving with relatively high speed the mismatch of hash values is most likely due to normal link failure, and so the threshold should be high. On the other hand, if there are many hash value mismatches while the node is moving slowly, there is most likely a malicious node. So, the value of $malPcktThreshold$ is directly proportional to the

Journal of Theoretical and Applied Information Technology
10th January 2016. Vol.83. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

node speed and it was implemented by using equation (1):

$$malPcktThreshold = NodeSpeed + C \quad (1)$$

Where C is the threshold value when the node speed is zero.

The malicious node may not act as a black hole all the time, it may become benign for some period of time, then it may (or may not) resume its malicious activities. So, when a node adds another node's address to its blacklist, the blacklisted node will not stay in its blacklist forever. However, it will be blacklisted for a previously specified period of time. So, when a node is added to another node's blacklist, not only the address of the blacklist is added but also the expiry time for that node to be released from that blacklist. The blacklisted node expiry time is computed using equation (2):

$$blkListedNodeExpTime = CURRENT\_TIME + blocking\ Period \quad (2)$$

Each time the node wants to send (or forward) a packet to a neighboring node, it will check if it is blacklisted, and if so it will also check the expiry time for that node. If it's expired, it will be removed from the blacklist of that node and its corresponding counter and expiry timer will be reset. Because of that it is dynamic blacklist.

Now when a node wants to send (or forward) a packet, in either the forward path or reverse path, it will check the routing table to decide what is the next hop. Then it will check if the next hop is blacklisted or not, if it's blacklisted, it will check the blacklist expiry time. If the next hop node is still blacklisted, then the node will remove that node from its neighbor list and run the handle link failure procedure. Then the node will try to send (or forward) the packet by using another path. Figure 3 and figure 4 are pseudo codes for the proposed solution. Figure 3 describes how the node decides to add or remove other nodes to or from its blacklist, and figure 4 how the node behaves when sending or forwarding a packet.

Pseudo code for the proposed solution: How the node decides to add or remove other nodes in its blacklist:

1. Generate new hash value ($NewHash$).
2. Compare the generated hash value New_Hash with the received hash value with the packet $HashVal$.
3. if($NewHash \neq HashVal$)
   then, $incr\ malNodeCouter(PrevHopAddr)$
4. Check the speed of the node ($NodeSpeed$).
5. Compute the threshold that will be used to consider a node as blacklisted
   $malPcktThreshold = NodeSpeed + C$
6. *//To add a node to a blacklist*
   if(isBlacklisted(NextHop) == FALSE && $malNodeCouter(NextHop) > malPcktThreshold$)
   then,
   a. $addBlackList(NextHop)$.
   b. $blkListedNodeExpTime(NextHop) = CURRENT\_TIME + Blocking\ Period$
7. *//To remove a node from a blacklist*
   else if(isBlaklisted(NextHop) == TRUE && $CURRENT\_TIME > BlkListedNodeExpTime(NextHop)$)
   then,
   a. $removeBlackList(NextHop)$.
   b. $malNodeCouter(NextHop) = 0$
   c. $blkListedNodeExpTime(NextHop) = 0$

   //For other cases: keep the blacklist as it is

Figure 3: Pseudo code for the proposed solution: How the node decides to add or remove other nodes in its blacklist

Pseudo code for the proposed solution: How the node behaves when sending or forwarding a packet:

1. if(isBlacklisted(NextHop) == TRUE)
   then,
   a. *// Delete blacklisted node from neighbors list*
      $nb\_delete(NextHop)$
   b. *//Consider link with blacklisted node as link failure*
      $handle\_link\_failure(NextHop)$

Figure 4: Pseudo code for the proposed solution: how the node behaves when sending or forwarding a packet

6. SIMULATION AND NETWORK ENVIRONMENT

The simulation was carried out using ns-2 simulator under Ubuntu Linux operating system. Ns-2 is a discrete-event simulator that is written in C++, which is object oriented language. During the simulation the packet header (aodv_packet.h file) of the AODV route request and route reply (changed to route reverse request) are modified to hold the hash value ($Hash\_Val$) with packet. In addition to that, the files aodv.h and aodv.cc were modified to implement the proposed solution together with previous protocols. Simulation was

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

done by referring to many resources including but not limited to [21][22][23].

The simulation area is a square field of 1000m x 1000m with fixed sender and receiver nodes that communicate using intermediate mobile nodes, which are moving randomly during simulation time (these random movements were generated using '*setdest*' tool) and are sending random traffic pattern among each other (created using '*cbrgen.tcl*' command). The sender and receiver were placed in points (200,200) and (800,800) respectively. The parameter considered in this simulation is given in table 2 below.

TABLE2: PARAMETERS USED IN NS-2 SIMULATION

Parameter	Value
Simulator	ns-2
Routing protocol	AODV, IDSAODV, R-AODV, RID-AODV, Enhanced RID-AODV
Simulation time	100 sec
Simulation area	1000m x 1000m
Number of nodes	40
Number of malicious nodes	0,1,2,3,4,5,6,7
Sender node	Fixed at point (200,200)
Receiver node	Fixed at point (800,800)
Intermediate nodes	Moving randomly
Maximum speed of mobile nodes	20 m/s
Data Rate	50 Kb/s
Pause time	0 sec
Transport type	UDP, CBR
Data packet size	Default
MAC Protocol	IEEE 802.11

In this research, the proposed solution together with four preceding protocols were implemented and simulated with the same environment parameters to be able to make a comparison among them. That include: the genuine AODV protocol with simulation of black hole malicious nodes, the IDSAODV protocol proposed in [19], RAODV proposed in [20], RID-AODV that was proposed on [5] and our proposed solution in this paper which is Enhanced RID-AODV. For each protocol many scenarios were generated to simulate the existence of different number of malicious nodes in order to study the effect of multiple malicious nodes on network performance and the effectiveness of each solution to compare among these solutions; we made as many combinations of nodes to act as malicious nodes and then we computed the average of the results.

Performance Metrics:

In this simulation, the following three performance metrics were considered and computed as the average of many cases in all scenarios of multiple malicious nodes for all the protocols in the study. Three separate scripts were generated to compute these performance metrics using *awk* command.

- **Throughput:** The amount of data transferred over the period of time expressed in kilobits per second (kbps). Throughput has been calculated using equation (3):

$$Throughput = \frac{\sum Size\ of\ Received\ Data\ Packets}{Simulation\ Time} \quad (3)$$

- **Packet Delivery Ratio (PDR):** The percentage ratio of the total number of data packets received by the destination node to the number of data packets sent by the source node as in equation (4).

$$PDR = \frac{\sum Number\ of\ Received\ Data\ Packets}{\sum Number\ of\ Sent\ Data\ Packets} * 100\% \quad (4)$$

- **Average End-to-End Delay:** The average delay between the sending of the data packet by the source node and its receipt at the destination node. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer… etc. The average end-to-end delay was computed using equation (5).

$$Avg\_E2E\_Delay = \frac{\sum_i (Receive\ Time\ of\ P_i - Sent\ Time\ of\ P_i)}{Number\ of\ Received\ Packet} \quad (5)$$

7. RESULTS AND ANALYSIS

Simulation results show that only one black hole in the network - without any solution - is able to decrease the PDR to almost 10% of its value without black hole. And only a small number of black holes in the network are able to reduce the throughput and the packet delivery ratio to almost zero resulting in denial of service (DoS) for the legitimate nodes, as illustrated in figure 5 and figure 6 respectively.

These two figures also show the results of applying four solutions: IDSAODV, R-AODV,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RID-AODV and the proposed Enhanced RID-AODV on increasing the throughput and the packet delivery ratio. It's obvious that the proposed protocol "Enhanced RID-AODV" has the highest throughput and the packet delivery ratio. That happens because of the effect of applying the dynamic blacklists with variable threshold resulting in reducing the packet loss due to malicious nodes.

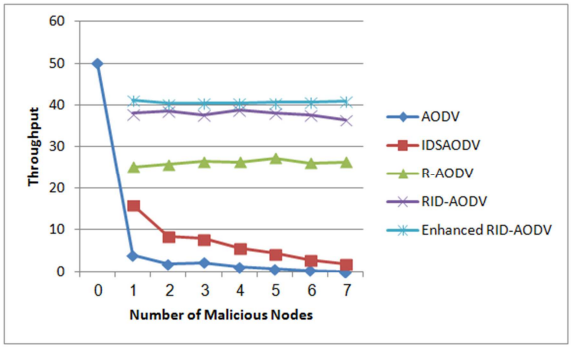

Figure 5: Effect of number of malicious nodes on Throughput for different protocols in mitigating multiple black hole attacks

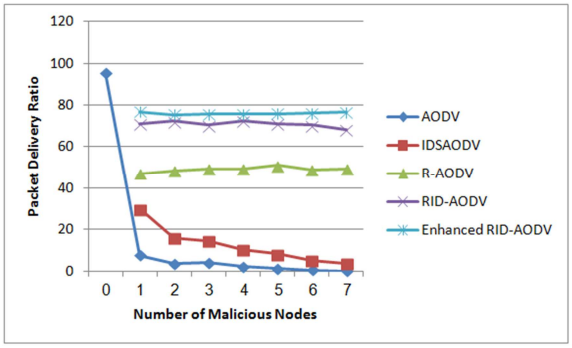

Figure 6: Effect of number of malicious nodes on Packet Delivery Ratio for different protocols in mitigating multiple black hole attacks

Another major improvement as a result of applying the proposed protocol is decreasing the average end-to-end delay; that because of the effect of the dynamic blacklists in forwarding packets to only the non malicious intermediate nodes to create right paths and to avoid the malicious nodes in both the forward and reverse paths. This is clear in figure 7 below.

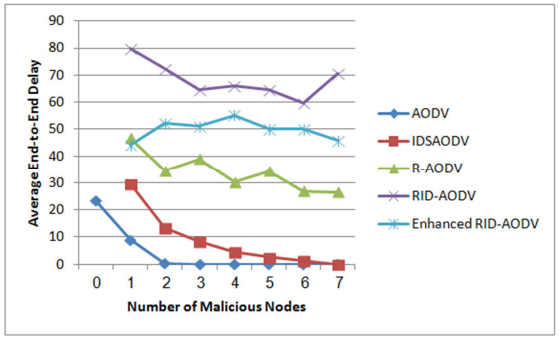

Figure 7: Effect of number of malicious nodes on Average End-to-End Delay for different protocols in mitigating multiple black hole attacks

8. CONCLUSION

In this paper a new mechanism, called "Enhanced RID-AODV", was proposed to detect and mitigate the effects of multiple black hole attacks in MANETs. It is an enhanced and modified version of a previously proposed mechanism called RID-AODV. RID-AODV is a combination of reverse routing and route caching technique. The proposed idea in this paper is creating a dynamic blacklist in each node, then prevent sending or forwarding to blacklisted nodes in both directions for a pre-specified period of time. The criteria to add a node in the blacklist is reaching a threshold in the number of mismatched hashing value from that node. The threshold is a function of mobility (variable threshold) to cancel the effect of normal link failure which is most likely caused by nodes mobility. According to the simulation results, Enhanced RID-AODV provides higher throughput and higher packet delivery ratio than its preceding version. Also, the dynamic blacklists provide positive effects in decreasing the end-to-end delay.

REFERENCES

[1] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC: 2501, IETF. [Online]. Available: http://tools.ietf.org/html/rfc2501

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, 2013.

[4] S. Behzad and S. Jamali, "A Survey over Black hole Attack Detection in Mobile Ad hoc Network", International Journal of Computer Science and Network Security (IJCSNS), Vol.15 No.3, March 2015

[5] O. Shree, F. J. Ogwu, "A Proposal for Mitigating Multiple Black-Hole Attack in Wireless Mesh Networks", Wireless Sensor Network, vol. 5, no. 4, pp- 76-83, 2013.

[6] A. Kanthe, D. Simunic , R. Prasad, "Effects of Malicious Attacks in Mobile Ad-hoc Networks", 2012 IEEE International Conference on Computational Intelligence and Computing Research, ISBN:978-1-4673-2481-6,18-20, December 2012, Coimbatore, India.

[7] E. Cayirci and C. Rong, "security in wireless ad hoc and sensor networks". John Wile and Sons, 2009

[8] A. Saeed, A. Raza and H. Abbas, "A Survey on Network Layer Attacks and AODV Defense in Mobile Ad Hoc Networks", IEEE Eighth International Conference on Software Security and Reliability, SERE 2014, USA 2014

[9] A. K. Abdelaziz, N. Mehdi and G. Salim, "Analysis of security attacks in AODV", International Conference on Multimedia Computing and Systems(ICMCS), (2014)

[10] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs". 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[11] L. Tamilselvan and V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008

[12] S. kurosawa and A. Jamalipour, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Nov 2007.

[13] I. Aad, P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, Vol. 16, No. 4, 2008, pp. 791- 802.

[14] D. Mishra, K. Y. Jain and S. Agarwal, "Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)", Proceeding from ACT'09: IEEE Advances in Computing, Control and Telecommunication Technologies, Trivandrum, 28-29 December 2009, pp. 621-623.

[15] E. Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", Proc. IEEE Conference on Local Computer Networks, 2007.

[16] D. Wadbude, V. Richariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, 2012, pp. 274-279

[17] L. Himral, V. Vig and N. Chand, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[18] M. Shakshuki, N. Kang and Sheltami,"EAACK- A Secure Intrusion-DetectionSystem for MANETs", IEEE Transactions on Industrial Electronics, vol. 60, no. 3, March 2013.

[19] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[20] C. Kim, E. Talipov, and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks", The International Conference on Emerging Directions in Embedded and Ubiquitous Computing (EUC'06), Seoul, 1-4 August 2006, pp. 522-531. Springer, 2006.

[21] The Network Simulator ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns

[22] N. Hegde and S. Manvi, "Simulation of Wireless Sensor Network Security Model Using NS2", International Journal of Latest Trends in Engineering and Technology (IJLTET). Vol. 4 May 2014

[23] C. Manikandan, R.Parameshwaran, K.Hariharan, N.Kalaimani and K.P. Sridhar, "Combined Security and Integrity Agent Integration into NS-2 for Wired, Wireless and Sensor Networks" Australian Journal of Basic and Applied Sciences, 7(7): 376-382, 2013 ISSN 1991-8178

Appendix B:

Published Papers

B-2: Second Paper:

Protocol to Avoid Multiple Black Hole Attacks in MANETs

Accepted and orally presented in the 2015 International Conference on Information and Computer Technology (ICICT 2015), held on November 12-13, 2015 in Dubai – United Arab Emirates. This conference is organized by International Association of Computer Science and Information Technology (IACSIT).

This paper also was accepted to be published in the Journal of Advances in Computer Networks (JACN).

Protocol to Avoid Multiple Black Hole Attacks in MANETs

Rushdi A. Hamamreh and Abdul-Rahman Salem

***Abstract*—Mobile Ad Hoc Networks (MANETs) form a promising approach for applications that need fast installation with no infrastructure especially in disaster recovery and emergency operations. However, many challenges are facing MANETs including security, routing, transmission range and dynamically changing topology with high nodes mobility. Security is considered as the main obstacle for the widespread adoption of MANET applications. Black hole attack is a type of DoS attack that can disrupt the services of the network layer. It has the worst malicious impact on network performance as the number of malicious nodes increases. Several mechanisms and protocols have been proposed to detect and mitigate its effects using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay. This paper proposes an enhanced and modified mechanism called "Enhanced RID-AODV", based on a preceding mechanism: RID-AODV. The proposed enhancement is based on creating *dynamic blacklists* for each node in the network. Each node, according to criteria depends on the number of mismatches of hash values of received packets as compared with some threshold values, can decide to add or remove other nodes to or from its blacklist. The threshold is a function of mobility (*variable threshold*) to cancel the effect of normal link failure. Enhanced RID-AODV was implemented in ns-2 simulator and compared with three previous solutions for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay and overhead ratio.**

***Index Terms*—Enhanced RID-AODV, MANET security, multiple black hole attacks, network layer attack.**

I. Introduction

Mobile Ad Hoc Network (MANET) is a self-configuring network formed by co-operating and independent nodes that connect and communicate with each other wirelessly without pre-existing infrastructure. If two mobile nodes are within each other transmission range, then they can communicate with each other directly; otherwise, the nodes in between have to forward the packet for them. So, mobile nodes are not only functioning as hosts but they are also function as routers [1].

Because MANETs are infrastructure-less networks with no centralized administration, they can be self deployed in short time. The easy deployment of nodes, self-organizing nature and freedom of mobility make MANETs suitable for a broad range of applications. They can be useful in disaster recovery and emergency operations where there is not enough time or resources to install and configure an infrastructure. They are also used in other applications; for example, in military services, maritime communications, vehicle networks, casual meetings, campus networks, robot networks… etc [2].

On the other hand, MANETs are vulnerable to various attacks at all layers. So, much research has been conducted on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality: intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. The network layer, especially the routing protocol, is vulnerable because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, the lack of clearly defined physical network boundary and the transient nature of services in the network. Standard information security measures such as encryption and authentication do not provide complete protection; thus intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs [3].

Attacks in MANET can be divided, according to the criteria that whether they disrupt the operation of a routing protocol or not, into two classes: passive attacks and active attacks. In passive attacks, the attacker attempts to discover valuable information but does not disrupt the operation of the routing protocol. Active attacks; however, involve actions like modification and deletion of exchanging data to absorb packets destined to other nodes to the attacker for analyzing or disabling the network. Some typical kinds of active attacks that can be performed against MANETs are: black hole attack, gray hole attack, flooding attack, selfish attack, rushing attack, spoofing, wormhole attack, sleep deprivation and impersonation [4].

Black hole attack is a type of active attack that exploits the route reply message (RREP) feature of the ad hoc on-demand distance vector (AODV) routing protocol. This attack involves some modification of the data stream or the creation of a false stream. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. A RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any other RREP messages from other neighboring nodes or even from the actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them [5].

So, the black hole attack is a DoS attack that disrupts the services of routing layer by exploiting the route discovery

process of AODV. According to many research studies that focus on studying the effects of malicious attacks on network performance, the simulation results show that the black hole attack is more dangerous than other attacks in the network layer [6].

Several mechanisms and protocols have been proposed to detect and mitigate its effect using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay.

In this paper, we propose a modified and enhanced protocol that aims to detect and mitigate the effects of multiple black hole attacks in MANETs. The proposed solution, "Enhanced RID-AODV", was implemented in ns-2 simulator and compared with three previous solutions for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay and overhead ratio.

The rest of this paper is organized as follows: section II provides some details about the black hole attack, section III provides the related work in detection and mitigation of black hole attack. The proposed solution is introduced in section IV, the simulation and network environment is described in section V, in section VI, the analysis and the results are discussed. Finally, the conclusion is presented in section VII.

II. BLACK HOLE ATTACK IN MANETS

Routing protocols in Mobile Ad Hoc Networks by their nature are distributed routing protocols with the assumption that all nodes in the network will cooperate truly and participate honestly. However, the existence of malicious nodes makes this assumption not true. Such nodes may drop the packets, if they are not the destination, without forwarding them or may disrupt the routing discovery and maintenance processes resulting in abnormal network operation that affects the performance of the network and may cause denial of service [7].

A black hole attack is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them (drop all packets) without forwarding them to the destination [8].

In reactive routing protocols such as AODV, the destination sequence number (*dest_seq*) is used to describe the freshness of the route. A higher value of *dest_seq* means a fresher route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new *dest_seq* number larger than the current *dest_seq* number. In this way the intruder becomes part of the route to that destination [9]. Fig. 1 illustrates the black hole attack where nodes S and D are the source and destination respectively and node B is the black hole.

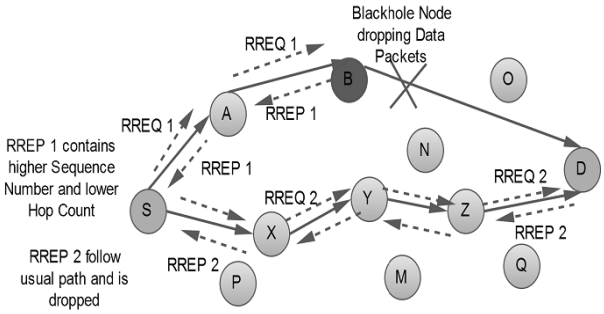

Fig. 1. Black Hole Attack Illustration

A black hole has two properties: First, the node exploits the ad hoc routing protocol to advertise itself as having a valid route to a destination, even though the route is spurious with the intention of intercepting packets. Second, the node consumes the intercepted packets. In an ad hoc network that uses the AODV protocol, a black hole node absorbs the network traffic and drops all packets [8].

III. RELATED WORK

Some research studies in the literature have focused on studying the effect of malicious nodes on network performance only without providing any solutions. However, several mechanisms and protocols using different strategies have been proposed to protect MANETs against black hole attacks. In [6] the authors studied the effect of malicious attacks in mobile ad hoc networks including black hole attack, packet drop attack and gray hole attack on AODV protocol under different performance metrics: throughput, packet drop rate and end-to-end delay. It was found that the black hole attack is more dangerous than other attacks conducted in this paper.

Paper [10] provides a quantitative study of the performance impact of black hole attacks in ad hoc networks using DSR as the routing protocol. The authors used the following performance metrics to evaluate the impact of black hole attack on network performance: System Fairness, Number of hops for received packets, Total system throughput and Probability of interception. The simulation results of the impact of black hole node on system fairness showed that with no black hole node, the system has high fairness index.

In [11] authors analyzed the effects of black hole attack in mobile ad hoc network using AODV and DSR routing protocols. For the simulation, throughput was considered as the main measure. Though the simulation results showed a higher data packet loss when using DSR compared to AODV, the dropped packet rate was still high for both protocols. DSR data loss was around 55 - 60 percent whereas that of AODV was around 45 - 50 percent. AODV protocol provides better performance than the DSR in the presence of black holes with minimal additional delay and overhead.

A black hole detection scheme for tactical MANETs using topology graph is proposed in [12]. This mechanism is called TOGBAD. It detects the attack using a topology graph, looking at the number of neighbors a node claims to have and the actual number of neighbors according to the graph. TOGBAD was developed for the OLSR proactive routing protocol, where topology information can be obtained.

Authors of [13] proposed an approach that uses improved security mechanisms to be introduced in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. The performance of these two protocols (SAODV and ARAN) was tested in simulation and their communication costs were measured using the NS-2 simulator, which is suitable for the present purpose. The evaluation metrics used in this study were overhead and end-to-end delay. The results show good performance.

In [14] a proposed method was introduced to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is a large difference between the sequence number of source node or intermediate node that has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, then it is surely from the malicious node, immediately remove that entry from the RR-Table. The proposed method cannot find multiple black hole nodes.

In [15] the authors proposed and implemented a new intrusion detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to modern approaches, EAACK demonstrates privileged malicious behavior detection rates in definite situations while it does not greatly affect the network performances. The demonstrated results show positive performances.

A lightweight routing protocol IDSAODV was proposed in [16] as a solution for black hole attack problem in MANETs. The authors of [16] manually analyzed the output file obtained from simulation and found out very soon after the first RREP from the destination node a second RREP arrived at the source node. Through simulation, they found out that the first RREP was from the black hole node and the second RREP was from the intended destination. At this point, for future simulations, they assumed that the first RREP would always be from black hole node and modified the AODV protocol to ignore the first RREP and send using second RREP route. A RREP caching mechanism to count the second RREP message was added to aodv.cc file in NS-2.

The simulation results of [16] demonstrate that IDSAODV improved the PDR in a MANET with a single black hole node; thus, proving the successful implementation of the route caching mechanism.

Many of the proposed solutions that make the route establishment process longer while the nodes are moving are facing from the link failure problem. In [5], the authors addressed this issue by getting advantage of the reverse AODV (RAODV) routing protocol proposed in [17]. RAODV discovers route using reverse route discovery procedure where the destination node sends reverse-route request (R-RREQ) messages to its neighbors to find a valid route to the source node after receiving RREQ from source node. Their simulation results of RAODV show that it does improve the performance of AODV in metrics such as packet delivery ratio (PDR), end-to-end delay, and energy consumption [17].

Although RAODV has not been designed to prevent black hole attacks and it was developed with the aim of solving path failure problem, authors of [5] proposed to use it in mitigating the effects of black hole attacks in ad hoc networks. So, they proposed RID-AODV by combining RAODV and IDSAODV (proposed in [16]) to withstand multiple black hole attacks in client-based WMNs.

IV. THE PROPOSED SOLUTION

The proposed solution, "Enhanced RID-AODV", is a modification and enhancement of the RID-AODV protocol proposed in [5]. That protocol is based on RAODV [17] and IDSAODV [16] as mentioned in the previous section. Our solution is to get advantage of the nature of the reverse route discovery procedure in RAODV. The detection of the malicious nodes and mitigation their effects can be achieved by creating and maintaining *dynamic blacklist* in each node according to some criteria. Then each non malicious node will prevent sending or forwarding to the neighboring nodes that exist in its own blacklist either in the forward or reverse path (In other words, each node will not use blacklisted nodes as intermediate nodes). Dynamic blacklist means that each node adds and removes nodes to or from its blacklist automatically according to specific criteria as will be explained in this section.

In addition, we can get another advantage of the nature of the reverse route discovery procedure in RAODV to create full path (bidirectional) integrity check implemented in hop-by-hop basis to detect any modifications on the traversing packets and to detect the causing nodes.

The criteria for each node to add another node's address in its blacklist is the repetitive mismatch in the hash value of the receiving frames (layer 2 frame) from the same neighboring node. So, each node keeps a counter for each other node that receives a frame from the neighboring nodes. If there is a mismatch between the received hash value and the calculated value, the corresponding counter for the sending (or forwarding) node will be incremented. When the counter reaches some threshold value $malPcktThreshold$, then the corresponding neighboring node will be blacklisted.

If node n_i has p neighboring nodes (p is $\subseteq$ of all nodes) and n_i is receiving from q nodes ($q\ is\ \subseteq\ of\ p$), then $n_i$will keep only q counters for this purpose.

To distinguish between hash value mismatch that may occur as a result of normal link failure, which is from the nature of MANETs due to mobility of nodes that communicate wirelessly, or from the existence of malicious nodes, the threshold value $malPcktThreshold$ should be considered as a function of mobility (*variable threshold*). If the node is moving with relatively high speed the mismatch of hash values is most likely due to normal link failure, and so the threshold should be high. On the other hand, if there are many hash value mismatches while the node is moving slowly, there is most likely a malicious node. So, the value of $malPcktThreshold$ is directly proportional to the node speed and it was implemented by using equation (1):

$$malPcktThreshold = NodeSpeed + C \quad (1)$$

Where C is some constant value.

When a node adds another node address to its blacklist, the blacklisted node will not stay in its blacklist forever. However, it will be blacklisted for a previously specified period of time. So, when a node is added to another node's blacklist, not only the address of the blacklist is added but also the expiry time for that node to be released from that blacklist. The blacklisted node expiry time is computed using equation (2):

$$blkListedExpTime = CURRENT\_TIME + blockingPeriod \quad (2)$$

Each time the node wants to send (or forward) a packet to a neighboring node, it will check if it is blacklisted, and if so it will also check the expiry time for that node. If it's expired, it will be removed from the blacklist of that node and its corresponding counter and expiry timer will be reset. Because of that it is dynamic blacklist.

Now, when a node wants to send (or forward) a packet, in either the forward path or reverse path, it will check the routing table to decide what is the next hop. Then it will check if the next hop is blacklisted or not, if it's blacklisted, it will check the black list expiry time. If the next hop node is still blacklisted, then the node will remove that node from its neighbor list and run the handle link failure procedure. Then the node will try to send (or forward) the packet by using another path.

Pseudo code for the proposed solution – how the node decides to add or remove other nodes in its blacklist:

1. Generate new hash value ($NewHash$).
2. Compare the generated hash value New_Hash with the received hash value with the packet $HashVal$.
3. if($NewHash \neq HashVal$)
   then, $incr\ malNodeCouter(PrevHopAddr)$
4. Check the speed of the node ($NodeSpeed$).
5. Compute the threshold that will be used to consider a node as blacklisted
   $malPcktThreshold = NodeSpeed + C$
6. *//To add a node to a blacklist*
   if(isBlacklisted(NextHop) == FALSE && $malNodeCouter(NextHop) > malPcktThreshold$)
   then,
   a. $addBlackList(NextHop)$.
   b. $blkListedNodeExpTime(NextHop) = CURRENT\_TIME + Blocking\ Period$
7. *//To remove a node from a blacklist*
   else if(isBlaklisted(NextHop) == TRUE && $CURRENT\_TIME > BlkListedNodeExpTime(NextHop)$)
   then,
   a. $removeBlackList(NextHop)$.
   b. $malNodeCouter(NextHop) = 0$
   c. $blkListedExpTime(NextHop) = 0$

   //For other cases: keep the blacklist as it is

Pseudo code for the proposed solution when sending or forwarding a packet (in both directions forward and reverse):

if(isBlacklisted(NextHop) == TRUE)
then,
a. *// Delete blacklisted node from neighbors list* $nb\_delete(NextHop)$
b. *//Consider link with blacklisted node as link failure* $handle\_link\_failure(NextHop)$

V. SIMULATION AND NETWORK ENVIRONMENT

The simulation was carried out using ns-2 simulator under Ubuntu Linux operating system. Ns-2 is a discrete-event simulator that is written in C++, which is object oriented language. During the simulation the packet header (aodv_packet.h file) of the AODV route request and route reply (changed to route reverse request) are modified to hold the hash value ($Hash\_Val$) with packet. In addition to that, the files aodv.h and aodv.cc were modified to implement the proposed solution together with previous protocols. Simulation was done by referring to many resources including but not limited to [18][19][20].

The simulation area is a square field of 1000m x 1000m with fixed sender and receiver nodes that communicate using intermediate mobile nodes, which are moving randomly during simulation time (these random movements were generated using '*setdest*' tool) and are sending random traffic pattern among each other (created using '*cbrgen.tcl*' command). The sender and receiver were placed in points (200,200) and (800,800) respectively. The parameter considered in this simulation is given in table 1 below.

TABLE1: PARAMETERS USED IN NS-2 SIMULATION

Parameter	Value
Simulator	ns-2
Routing protocol	AODV, IDSAODV, R-AODV, RID-AODV, Enhanced RID-AODV
Simulation time	100 sec
Simulation area	1000m x 1000m
Number of nodes	40
Number of malicious nodes	0,1,2,3,4,5,6,7
Sender node	Fixed at point (200,200)
Receiver node	Fixed at point (800,800)
Intermediate nodes	Moving randomly
Maximum speed of mobile nodes	20 m/s
Data Rate	50 Kb/s
Pause time	0 sec
Transport type	UDP, CBR
Data packet size	Default
MAC Protocol	IEEE 802.11

In this research, the proposed solution together with four preceding protocols were implemented and simulated with the same environment parameters to be able to make a comparison among them. That include: the genuine AODV protocol with simulation of black hole malicious nodes, the IDSAODV protocol proposed in [16], RAODV proposed in [17], RID-AODV that was proposed on [5] and our proposed solution in this paper which is Enhanced

RID-AODV. For each protocol many scenarios were generated to simulate the existence of different number of malicious nodes in order to study the effect of multiple malicious nodes on network performance and the effectiveness of each solution to compare among these solutions; we made as many combinations of nodes to act as malicious nodes and then we computed the average of the results.

Performance Metrics

In this simulation, the following four performance metrics were considered and computed as the average of many cases in all scenarios of multiple malicious nodes for all the protocols in the study. Four separate scripts were generated to compute these performance metrics using *awk* command.

- **Throughput:** The amount of data transferred over the period of time expressed in kilobits per second (kbps). Throughput has been calculated using formula (3):

$$Throughput = \frac{\sum \text{ReceiveDataPacketsSize}}{SimulationTime} \quad (3)$$

- **Packet Delivery Ratio (*PDR*):** The percentage ratio of the total number of data packets received by the destination node to the number of data packets sent by the source node as in equation (4).

$$PDR = \frac{\sum Numberof\ \text{ReceivedDataPackets}}{\sum NumberofSentDataPackets} \quad (4)$$

- **Average End-to-End Delay ($AvgDelay_{E-E}$):** The average delay between the sending of the data packet by the source node and its receipt at the destination node. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. The average end-to-end delay was computed using equation (5).

$$AvgDelay_{E-E} = \frac{\sum_i (\text{ReceiveTime of } P_i - SentTimeof\ P_i)}{Numberof\ \text{ReceivedPackets}} \quad (5)$$

- **Overhead Ratio (OH):** The ratio of the total number of control packets sent at the routing level and the total number of packets sent from the source node as in equation (6).

$$OH = 1 - \frac{NumberofSentDataPcktsAtRTR}{NumberofAllPcktsAtRTR} \quad (6)$$

VI. RESULTS AND ANALYSIS

Simulation results show that only one black hole in the network - without any solution - is able to decrease the PDR to almost 10% of its value without black hole. And only a small number of black holes in the network are able to reduce the throughput and the packet delivery ratio to almost zero resulting in denial of service (DoS) for the legitimate nodes, as illustrated in fig. 2 and 3 respectively.

These two figures also show the results of applying four solutions: IDSAODV, R-AODV, RID-AODV and the proposed Enhanced RID-AODV on increasing the throughput and the packet delivery ratio. It's obvious that the proposed protocol "Enhanced RID-AODV" has the highest throughput and the packet delivery ratio. That happens because of the effect of applying the dynamic blacklists with variable threshold resulting in reducing the packet loss due to malicious nodes.

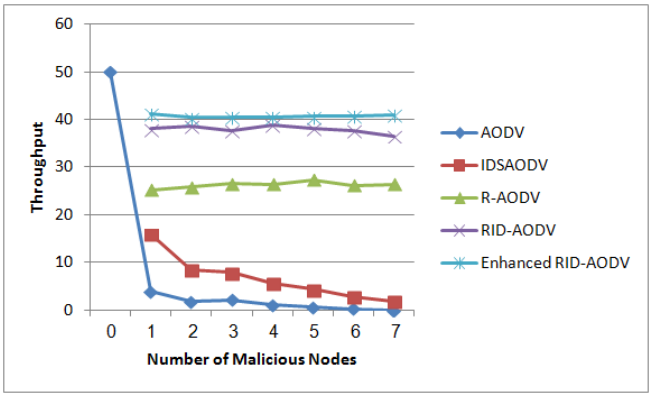

Fig. 2: Effect of number of malicious nodes on Throughput for different protocols in mitigating multiple black hole attacks

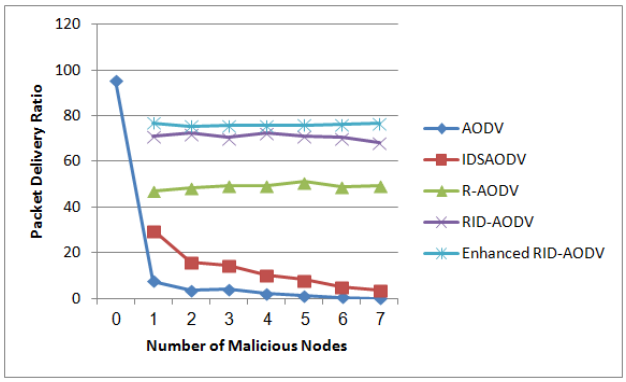

Fig. 3: Effect of number of malicious nodes on Packet Delivery Ratio for different protocols in mitigating multiple black hole attacks

Another major improvement as a result of applying the proposed protocol is decreasing the average end-to-end delay and the overhead; that because of the effect of the dynamic blacklists in forwarding packets to only the non malicious intermediate nodes to create right paths and to avoid the malicious nodes in both the forward and reverse paths. This is clear in fig. 4 and fig. 5.

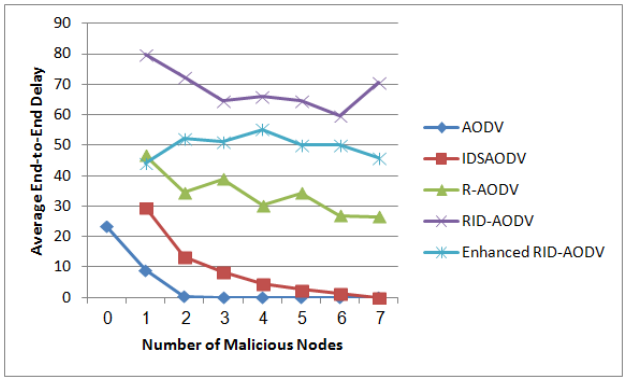

Fig. 4: Effect of number of malicious nodes on Average End-to-End Delay for different protocols in mitigating multiple black hole attacks

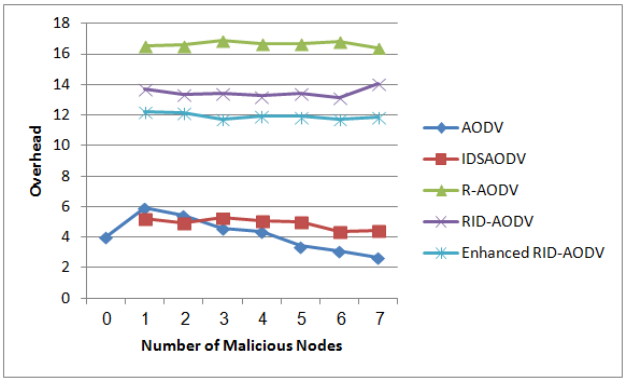

Fig. 5: Effect of number of malicious nodes on Overhead for different protocols in mitigating multiple black hole attacks.

VII. CONCLUSION

Several mechanisms and protocols have been proposed to detect and mitigate the effects of multiple black hole attack using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay. In this paper a new mechanism, called "Enhanced RID-AODV", was proposed to detect and mitigate the effects of multiple black hole attacks in MANETs aiming to increase the throughput and PDR while decreasing the the average end-to-end delay and overhead. It is an enhanced and modified version of a previously proposed mechanism called RID-AODV. RID-AODV is a combination of two other protocols: RAODV (reverse routing) and IDSAODV which is based on creating route caching technique.

The proposed idea in this paper is creating a dynamic blacklist in each node, then prevent sending or forwarding to blacklisted nodes in both directions for a pre-specified period of time. The criteria to add a node in the blacklist is reaching a threshold in the number of mismatched hashing value from that node. The threshold is a function of mobility (variable threshold) to cancel the effect of normal link failure which is most likely caused by nodes mobility.

According to the simulation results, Enhanced RID-AODV provides higher throughput and higher packet delivery ratio than its preceding version. Also, the dynamic blacklists provide positive effects in decreasing the overhead ratio and the end-to-end delay.

REFERENCES

[1] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC: 2501, IETF. [Online]. Available: http://tools.ietf.org/html/rfc2501

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.

[3] A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, 2013.

[4] S. Behzad and S. Jamali, "A Survey over Black hole Attack Detection in Mobile Ad hoc Network", International Journal of Computer Science and Network Security (IJCSNS), Vol.15 No.3, March 2015

[5] O. Shree, F. J. Ogwu, "A Proposal for Mitigating Multiple Black-Hole Attack in Wireless Mesh Networks", Wireless Sensor Network, vol. 5, no. 4, pp- 76-83, 2013.

[6] A. Kanthe, D. Simunic , R. Prasad, "Effects of Malicious Attacks in Mobile Ad-hoc Networks", 2012 IEEE International Conference on Computational Intelligence and Computing Research, ISBN:978-1-4673-2481-6,18-20, December 2012, Coimbatore, India.

[7] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs". 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[8] L. Tamilselvan and V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008

[9] S. kurosawa and A. Jamalipour, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Nov 2007.

[10] I. Aad, P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, Vol. 16, No. 4, 2008, pp. 791- 802.

[11] D. Mishra, K. Y. Jain and S. Agarwal, "Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)", Proceeding from ACT'09: IEEE Advances in Computing, Control and Telecommunication Technologies, Trivandrum, 28-29 December 2009, pp. 621-623.

[12] E. Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", Proc. IEEE Conference on Local Computer Networks, 2007.

[13] D. Wadbude, V. Richariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, 2012, pp. 274-279

[14] L. Himral, V. Vig and N. Chand, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[15] M. Shakshuki, N. Kang and Sheltami,"EAACK- A Secure Intrusion-DetectionSystem for MANETs", IEEE Transactions on Industrial Electronics, vol. 60, no. 3, March 2013.

[16] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[17] C. Kim, E. Talipov, and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks", The International Conference on Emerging Directions in Embedded and Ubiquitous Computing (EUC'06), Seoul, 1-4 August 2006, pp. 522-531. Springer, 2006.

[18] The Network Simulator ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns

[19] N. Hegde and S. Manvi, "Simulation of Wireless Sensor Network Security Model Using NS2", International Journal of Latest Trends in Engineering and Technology (IJLTET). Vol. 4 May 2014

[20] C. Manikandan, R.Parameshwaran, K.Hariharan, N.Kalaimani and K.P. Sridhar, "Combined Security and Integrity Agent Integration into NS-2 for Wired, Wireless and Sensor Networks" Australian Journal of Basic and Applied Sciences, 7(7): 376-382, 2013 ISSN 1991-8178

Dr. Rushdi Hamamreh is working as Associate Professor in the Computer Engineering Department at Al-Quds University in Jerusalem. This author is the head of the Computer Engineering Department at the university. He received the PhD degree from Saint Petersburg State Technical University, Russia, 2003. Dr. Hamamreh has many publications in the field of Computer and Mobile networks, Distributed systems, Multiagent systems, Information retrieval and Networks security. He has attended many Conferences, Seminars and Workshops. Member of the International and National Associations of research and teaching areas.

Abdul-Rahman Salem was born in Battir-Bethlehem in Palestine in the year 1977. He received his B.Sc. degree in electrical engineering with minor in Computer Science from Birzeit University in 2000; and currently, he is preparing for M.Sc. degree in electronics and computer engineering from Al-Quds University in Jerusalem. His main research interests are in the field of networking and security including wired and wireless networks. Currently, he is the acting director of the information security department at the Palestinian Central Bureau of Statistics (PCBS); in addition to his position as the head of network administration division in the same institution. He is also working as part time trainer for IT professional courses in local institutes.

Certificate

International Association of Computer Science and Information Technology

IACSIT
WWW.IACSIT.ORG

Certificate for Oral Presentation

This Certificate is Awarded to *Abdul-Rahman Salem(CT307)*

Paper Title:

Protocol to Avoid Multiple Black Hole Attacks in MANETs

For her/his attendance and delivery of an oral presentation in the 2015 International Conference on Information and Computer Technology(ICICT 2015) held in Dubai, UAE, November 11-13, 2015.

Conference Committee
ICICT 2015

JAIT
Journal of Advances in Information Technology

IAP
www.iap.org
International Academy Publishing