Sudan University of Science and Technology
School of Electronics Engineering
Department of Computer and Networking

Performance Evaluation of Secure Routing Protocol in Mobile Ad Hoc Network

تقييم الاداء لبروتوكول التوجبه الامن فى شبكة اد هوك نقالة

A research

Submitted to the school of Electronic Engineering,

In partial fulfillment of the requirements for the Degree of Master

In

Computer Engineering and Networking

Prepared by:

Soha Elkhidir Yousif

Supervised by:

Dr. Ahmed Abdalla

March 2018

ABSTRACT

A mobile ad-hoc network (MANET) is a collection of mobile devices that used wireless communications capability without any central network authority or infrastructure. Due to its dynamic behavior and lack of central authority security becomes the challenging task for this network. Nodes can get compromised from various types of threats such as black hole and wormhole attacks. Black hole attack is a type of routing attack where a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. It can be used as a denial-of-service attack where it can drop the packets. This work focuses on evaluating the security of one of the popular routing protocol for MANETs, namely the Ad hoc On Demand Distance Vector (AODV) routing protocol to avoid black hole attacks. The proposed Intrusion Detection System AODV (IDSAODV) and AODV Uppsala University (AODV-UU) are considered as modification of the AODV protocol and they used to detect and avoid black hole attacks. A comparative evaluation performance is done for the protocols; AODV, IDSAODV, AODV-UU with Network Simulator NS-2.32. The Simulation has been carried with and without black hole attacks on different parameters, namely; routing overheads, packet delivery ratio and average delay for each of the three versions of the AODV protocol. Results proved that AODV-UU has all the advantages of IDSAODV and AODV when black hole is used or not. It has higher throughput, lower delay and lower routing overhead. However, quality of service decreases severely when number of node increases.

مستخلص البحث

الشبكات اللاسلكيه العشوائيه المتنقله هي مجموعه من الاجهزه المحموله التى تستخدم الاتصال اللاسلكي بدون استخدام اي سلطه مركزيه للشبكه او بنيه تحتيه . نظرًا لسلوكها الديناميكي ونقصها في أمن السلطة المركزية ، تصبح المهمة الصعبة لهذه الشبكة. يمكن اختراق العقد من أنواع مختلفة من التهديدات مثل الثقب الأسود والهجمات الدودية. هجوم الثقب الأسود هو نوع من هجوم التوجيه حيث تعلن عقدة خبيثة نفسها بأنها تحتوي على أقصر مسار للعقدة التي تريد أعترض حزمها. ويمكن استخدامه بمثابة هجوم الحرمان من الخدمة حيث يمكن إسقاط الحزم. يرتكز هذا العمل على تقييم أمن أحد بروتوكولات التوجيه الشائعة لـ MANET ، أي بروتوكول التوجيه المخصص عند الطلب (AODV) لتجنب هجمات الثقب الأسود. يعتبر بروتوكول نظام الكشف عن التطفل (IDSAODV) و بروتوكول جامعة Uppsala (AODV-UU) المقترحان بمثابة تعديل لبروتوكول AODV ويستخدمان لكشف وتجنب هجمات الثقب الأسود. يتم إجراء تقييم مقارن للبروتوكولات IDSAODV، AODV-UU مع AODV باستخدام محاكي الشبكة (NS-2.32). وقد أجريت محاكاة بهجمات ثقوب سوداء وبدونها على معايير مختلفة ، وهي: توجيه النفقات العامة ، ونسبة تسليم الحزم ومتوسط التأخير لكل من الإصدارات الثلاثة من بروتوكول AODV. أثبتت النتائج أن AODV-UU لديه كل مزايا IDSAODV و AODV عند استخدام الثقب الأسود أو عدم إستخدامه, وان لديها أعلى إنتاجية ، تأخير أقل وانخفاض توجيه النفقات العامة. ومع ذلك ، تنقص جودة الخدمة بشدة عند زيادة عدد العقد.

ACKNOWLEDGEMENTS

I express my gratitude towards the Almighty God for His blessings upon me. I would like to express my deep sense of respect and gratitude towards my supervisor Dr. Ahmed Abdalla, who has been the guiding force behind this work. Without his unconditional support it wouldn't have been possible. As my supervisor, he has constantly encouraged me to remain focused on achieving my goal. I want to thank him for giving me the opportunity to work under him. His invaluable advice and assistance helped me to complete this thesis. I consider it my good fortune to have got an opportunity to work with such a wonderful person. I am really thankful to all my friends. My sincere thanks to everyone who has provided me with kind words, a welcome ear, new ideas, useful criticism, or their invaluable time, I am truly indebted. Last, but not the least, I would like to dedicate this thesis to my family, for their love, patience, and understanding.

Soha Elkhidir.

DEDICATION

To my parents

The reasons of what I become today

Thank you for your great support and continuous love

And all of my friends without whom none of my success would be possible

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

ABR	Associativity-Based Routing
ACO	Ant Colony Optimization
AODV	Ad-hoc on Distance Vector
A-SAODV	Adaptive secure Ad-hoc On Distance Vector
CBR	Constant Bit Rate
CGSR	Cluster Gateway Switch Routing Protocol
DOS	Denial of Service
DRPI	Dynamic Route Pheromone Bound Value Information Table
DSDV	Destination Sequenced Distance Vector
DSN	Destination Sequence Number
DSR	Dynamic Source Routing
FIFO	First in First out
HSN	highest Sequence Number
IASAODV	Intrusion Avoidance System Ad-hoc On Distance Vector
IDSAODV	Intrusion Detection System Ad-hoc On Distance Vector
IIDSAODV	Improved Intrusion Avoidance System Ad-hoc On Distance Vector
MANT	Mobile Ad-Hoc Networks
NAM	Network Animator
NS2	Network Simulator 2
OLSR	Optimized Link State Routing
OTCL	Object oriented Tool Command Language
PDR	Packet Delivery Ratio
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
SLSP	Secured Link State Protocol
SRRD_REP	Secure Reliable Route Discovery Replay
SRRD_REQ	Secure Reliable Route Discovery Request
SSN	Source Sequence Number
TCL	Tool Command Language
TCP	Transmission Control Protocol
TORA	Temporally Ordered Routing Algorithm
TTL	Time to Live
UDP	User Datagram Protocol
VM	Virtual Machine
ZRP	Zone Routing Protocol

CHAPTER ONE

Introduction

1.1 Overview

Mobile ad hoc network (MANET) is a network of mobile nodes that requires no infrastructure or centralized management in order to communicate. The nodes can join or leave the network any time thus have a dynamic approach of network topology. Each mobile node acts not only as a host but also as a router to establish a route. When a source node intends to transfer the data packets to a destination node, then the packets are transferred through intermediate nodes. Hence, quick deployment of the nodes to establish a route is an important issue in MANET. The most widely used routing protocol in MANETs is the ad hoc on-demand distance vector (AODV) routing protocol. AODV is a reactive routing protocol used to find a route between a source and a destination and allows mobile nodes to obtain new routes for new destinations.

There are three messages which are defined by AODV. These messages are Route Errors (RERRs), Route Request (RREQs) and Route Replies (RREPs). For discovering and maintaining routes in the network these three messages are used, by using UDP packets from source to destination. A node uses its IP address as the source address in the IP header of a message when it requests for a route and broadcasts RREQ Message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted. A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node. Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects

a link crack in an active route, route error (RERR) message is generated by the node in order to notify other nodes that the link is down.

In black hole attack the victim node sends the request for shortest path that leads its data towards destination. The malicious node (the attacker) listens to this request and advertises itself as shortest path to the victim node.

1.2 Problem statement

Black hole is one of the most powerful attacks. It can cause a complete failure of the compromised MANET by dropping all the traffic and breaking communications between nodes when a malicious node is placed between two or several nodes. The vulnerability of the route discovery packets in AODV is exploited by the attacker with a simple modification in the routing protocol, in order to control all the traffic between nodes.

1.3 Proposed solution

The research investigates using of IDS AODV and AODV-UU protocols to prevent black hole attacks and carries out a simulation-based comparison and analysis for MANET performance in terms of average delay, number of dropped packets and packet delivery ratio. This analysis is done to check the effect of those protocols to reduce black hole attacks.

1.4 Research Objective

The aim of this thesis is to evaluate the performance of IDS AODV and AODV-UU protocols to prevent the black hole attacks in AODV

routing protocol and to study their abilities to limit the influence of the black hole attacks.

1.5 Methodology

In this thesis Network Simulator 2 is chosen as a simulation environment it simulates wired and wireless network, it is providing substantial support to simulate bunch of protocols like TCP, UDP, HTTP, DSR and AODV, to implement the black hole AODV attacks and the prevention mechanism IDSAODV, AODV-UU are modifying from the existing AODV routing protocol in ns-2 by patching and installing them in ns2-32. Scenarios are generated by CBR traffics with varying numbers of black hole nodes with number of mobile node. The output of the NS-2 simulation, trace file, is studied to measure the performance by using routing overhead, packet delivery ratio and average delay at the end of the simulation as performance metrics. The trace file is analyzed using the AWK script. The NS2 simulator gives two files as output; NAM (Network Animator) generates NAM file, which is used for graphical visualization and other file called trace file is used for calculating the results.

I.6 Thesis Outline

The thesis includes five chapters, chapter one provides introduction of it, the problem statement and objectives while chapter two covers background study of AODV routing protocols and highlights of its black hole attack and literature review. In chapter three the methodology section, where the framework of the simulator, routing metric and simulation environment are defined while chapter four presents the

implementation and performance evaluation results. And chapter five includes the conclusion and future work.

CHAPTER TWO

Background and Related Works

2.1 Background

MANET is a set of mobile nodes that perform basic networking functions like packet forwarding, routing, and service discovery without the need of an established infrastructure [11]. All the nodes of an ad hoc network depend on each another in forwarding a packet from source to its destination, due to the limited transmission range of each mobile node's wireless transmissions. The features of MANET:

- Continuously self-configuring
- Infrastructure-less network
- Connected without wires

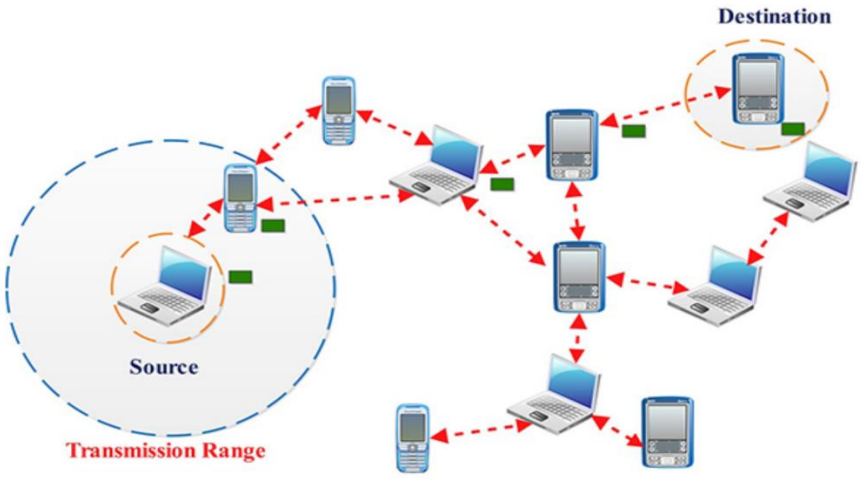


Figure 2.1 Mobile Ad hoc Network

2.1.1 OVERVIEW OF ROUTING PROTOCOLS

Routing protocols for ad hoc wireless networks can be classified into three types based on the underlying routing information update mechanism employed. An ad hoc routing protocol could be reactive (on demand), proactive (table driven) or hybrid

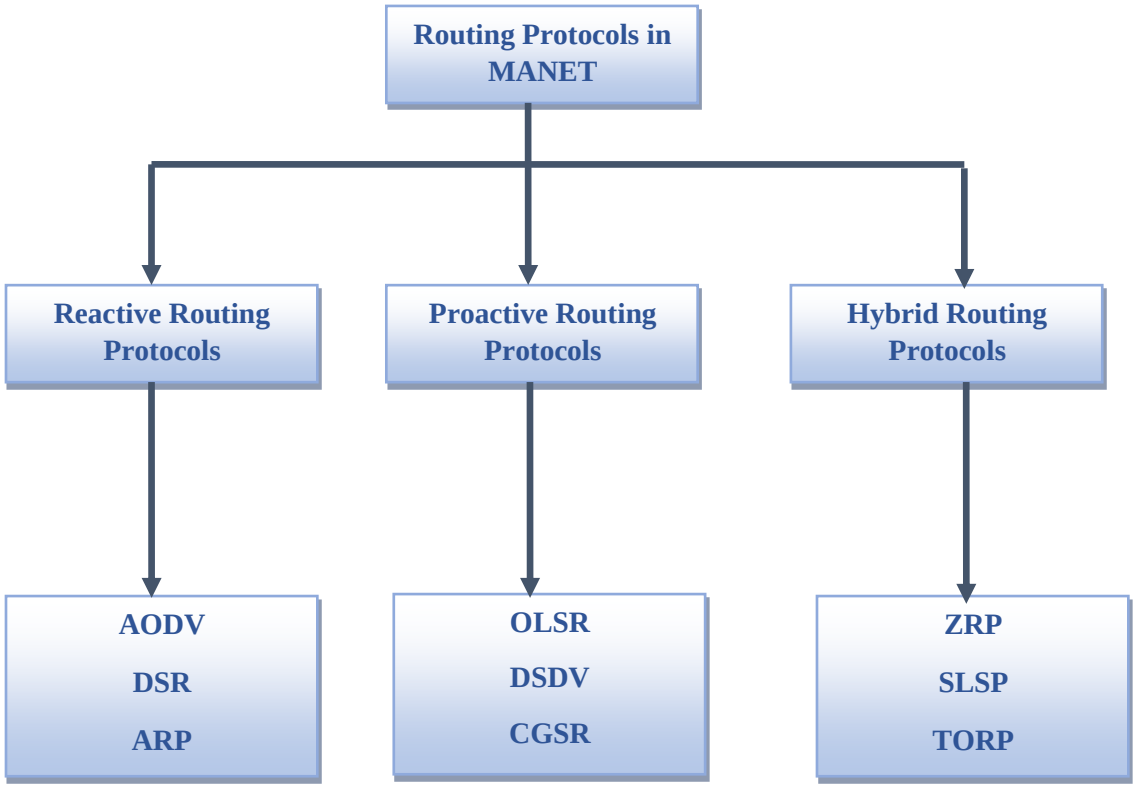


Figure 2.2 Routing protocols in MANET

2.1.2 Ad-Hoc On-Demand Distance Vector (AODV)

AODV routing protocol is a reactive routing protocol for the MANET that maintains routes only between nodes that need to communicate each other the routing messages do not contain information about the whole route path, but only about the source and the destination information. Therefore, the routing messages do not have an increasing size. It uses the Source Sequence Number (SSN) or the Destination sequence number (DSN) to specify how fresh a route is, which is used to grant loop freedom [11]. The following subsections give a brief description of how routes are built and maintained in MANETs. Neighbor connectivity is established with periodic Hello Messages [12]. Routes are found by flooding of route request (RREQ) messages as can be seen in Figure 2.3. As each node receives and retransmits the RREQ it records the previous hop in its routing table. In AODV, when a source node A wants to send a data packet to a destination node F and does not have a route to F, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. A timer call RREP_WAIT_TIME is started when the RREQ is sent. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors.

This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP), as can be seen in Figure 2.3, to the source node through the reverse path where the RREQ arrived. The destination node will ignore the same RREQ that arrives later. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node. Once the source receives the first

RREP message, it starts the data transmission along the path traced by the RREP packet.

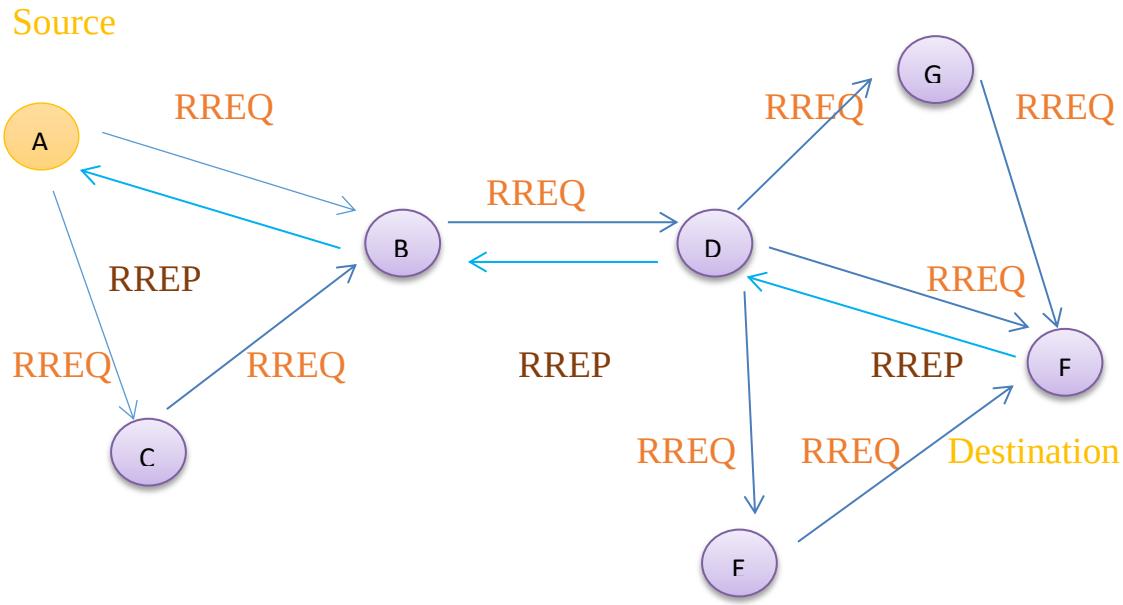


Figure 2.3 AODV Route Discovery

2.1.2.1 Black Hole Attack in AODV

A black hole attack is one of the active DOS attacks possible in MANETs [13] .In this attack, a malicious node may advertise a fresh path to a destination during routing process. In case when black hole node present in network when source node broadcast RREQ packets for route to destination, the black hole node fake reply with RREP packets. After getting all replies from all possible paths when source node do hope count then it will found that the black hole node is having shortest path and it will selects this path to send data. But the black hole did not forward packets it will receive packets and drop them.

2.1.2.2 Intrusion Detection System (IDS) AODV

To prevent black hole attack, IDSAODV is applying to prevent or reduce the effects of network performance. Inside IDSAODV, there are RREP caching mechanism to reduce the effects of the attack by ignoring the first RREP packet. Figure 2.4 shows RREP caching mechanism in IDSAODV. First, the node will wait for the first arrived RREP packet. If the first RREP packet arrived, IDSAODV will ignore it and wait for the next RREP packet [14]. The node will establish routing patch through the node that sends the next RREP packet. This RREP caching mechanism assumes that the first RREP packet comes from the black hole node [15] which contains false RREP. In the black hole, the malicious node will send false RREP that contains the highest sequence number and hop count was set to one that will manipulate the other nodes to establish routing patch to it. With IDSAODV, the first RREP packet is ignored and it will reduce chances to establish the routing path to the malicious node.

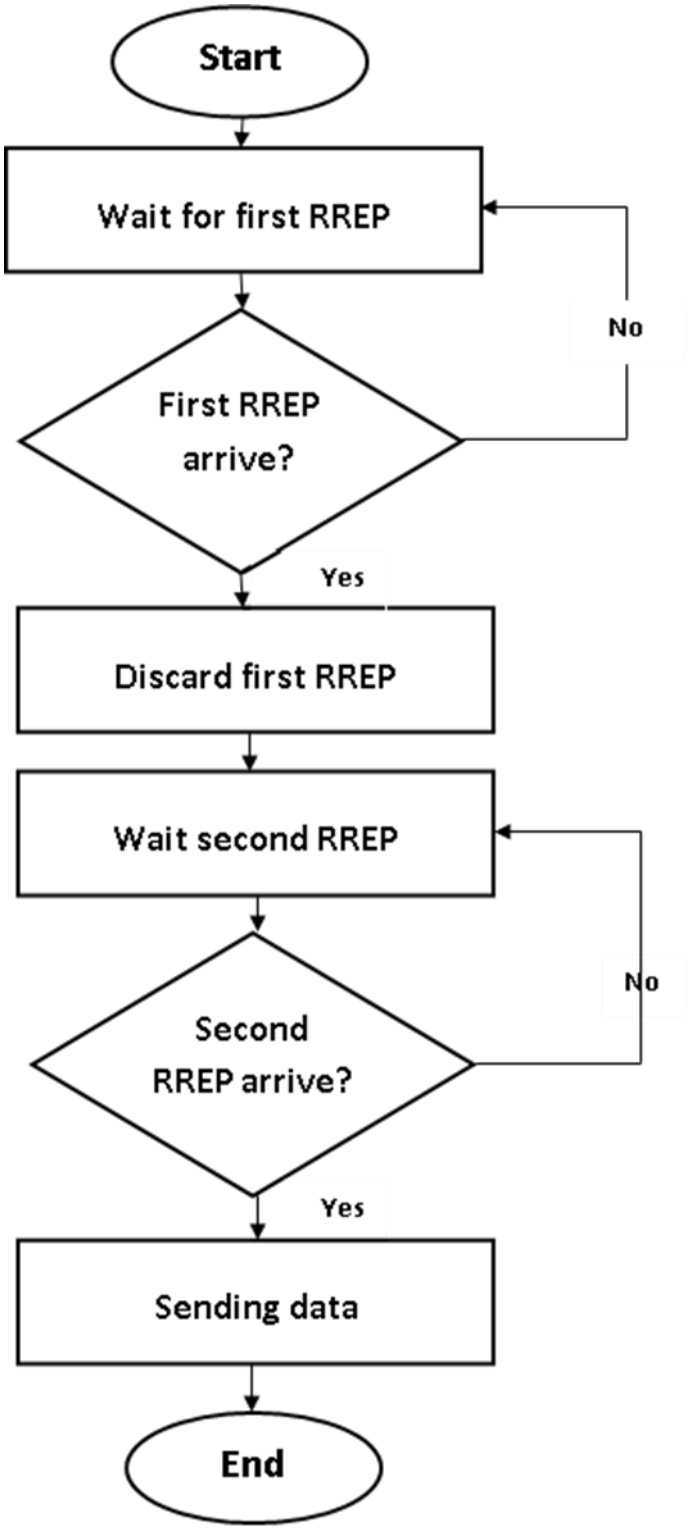


Figure 2.4 RREP cashing mechanism in IDSAODV

2.1.2.3 Ad-Hoc On-Demand Distance Vector (AODV-UU)

AODV-UU implements the AODV protocol, and it is compliant with IETF RFC 3561. AODV-UU was developed by the Uppsala University it uses kernel modules to utilize the Netfilter. In addition, AODV-UU (Uppsala University) includes Internet gatewaying support as well as multiple interface support [18]. The suffix UU is added for the word Uppsala University. AODV-UU was initially written in C for running with Linux. It is popular among the academician and researchers. A linux kernel framework for mangling packets for each network protocol certain hooks are defined, these hooks correspond to well-defined places the protocol stack and allow custom packet mangling code to be inserted in form of kernel modules. In particularly, packets arriving on the NF_IP_PRE_ROUTING or NF_IP_LOCAL_OUT hook are queued in user-space to allow AODV-UU to process them, while packet arriving on the NF_IP_POST_ROUTING i.e., packets should be sent out by the system, are re-routed to ensure usage of the last routing information available from the kernel routing, which can be changed as an effect of AODV-UU operation, e.g., route discoveries [19].

When a packet traverses the protocol stack, it is caught by the netfilter hooks (NF_IP_PRE_ROUTING, NF_IP_LOCAL_OUT, NF_IP_POST_ROUTING) that have been set up by the AODV-UU kernel module, kaodv-mod. The aodv_hook() function of the kaodv-mod module identifies the packet type and either tell the netfilter to accept the packet, i.e., to let it through and allow the system to process it on its own, or to queue it for further processing by AODV-UU in user-space.

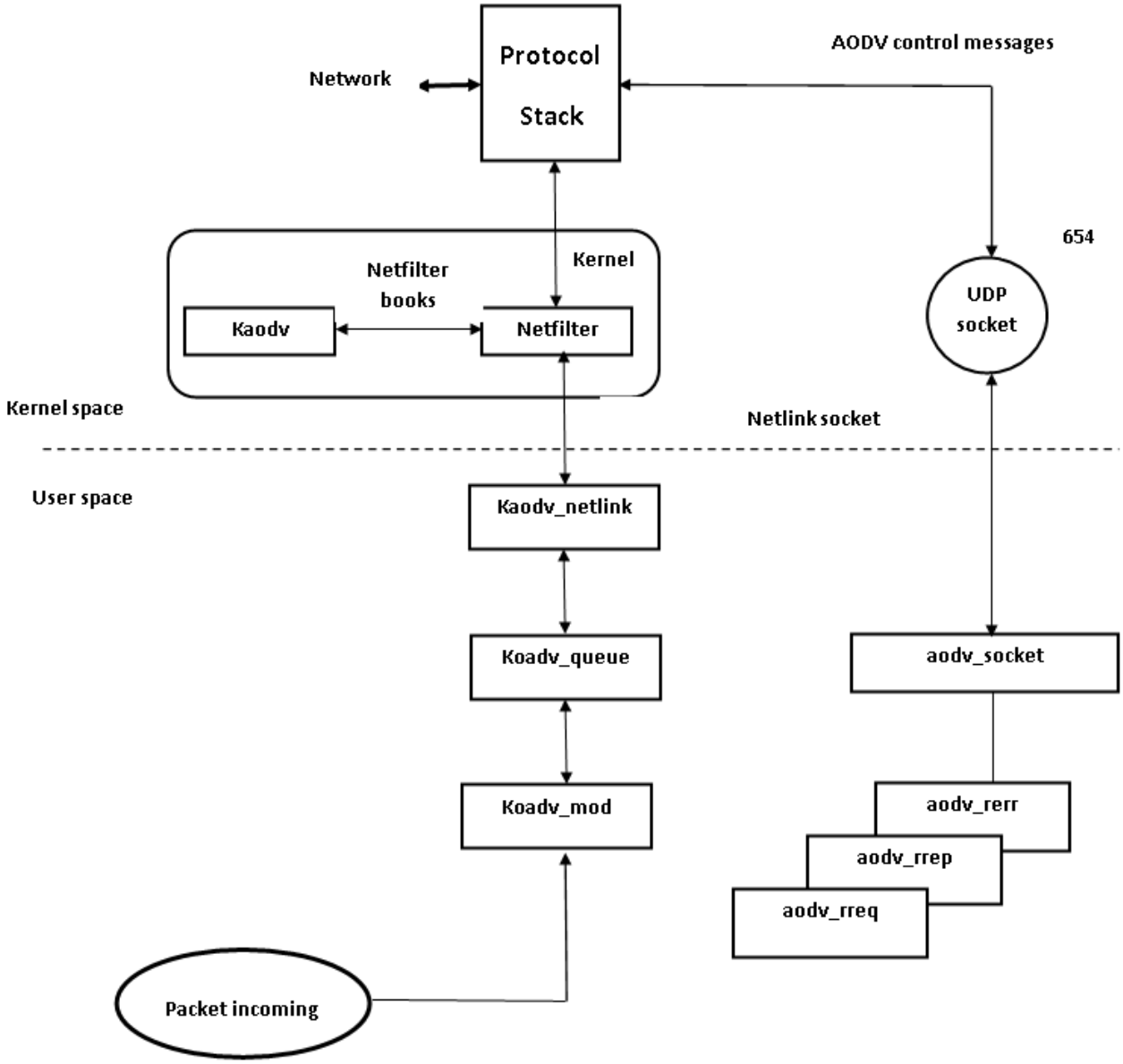


Figure 2.5 packet handling of AODV-UU from [19]

If AODV control message is a RREQ message the rreq_route_discovery() function and rt_table_find() function in aodv_rreq.c file will check the route entry in the routing table. Then the kaodv_update_route_timeout() function in the kaodv_mod.c file updates the routes and the rreq_process() function in the aodv_rreq.c file will check if the current node is destination node. If yes, the rrep_create() function and rrep_send() function in the aodv_rrep.c file will send the

RREP. If not, the RREP is only sent if a fresh enough route existed by the rrep_send() function in the aodv_rreq.c file. If a fresh enough route is not existed, the RREQ is forwarded to the neighbors by the rreq_forward() function in the aodv_rreq.c file.

If AODV control message is a RREP message is a RREP the rt_table_find() function and the rt_table_insert() function in the aodv_rrep.c file will create the forwarding route and update the precursor list by the precursor_add() function in the aodv_rrep.c file. Then the rrep_process() function in aodv_rrep.c file will check the RREP message for current node or not. If yes, the rrep_send() function in the aodv_rrep.c file will send the queued message. Otherwise, the rrep_forward() function in the aodv_rrep.c file will forward the RREP to the neighbors.

2.2 Related Works

Security is the primary concern in wired or wireless networks. A lot of work has been done in the field of detecting misbehavior in MANETs. A number of security mechanisms has been developed and proposed to reduce the effect of black hole attacks in MANT.

In [1] Enhanced Modified AODV by adding two types of control packets and threshold value: Secure Reliable Route Discovery Request (SRRD_REQ) and Secure Reliable Route Discovery Reply (SRRD_REP). SRRD_REQ messages are also known as control packets sent by the source node along with SRRD-ID as destination sequence number of destination node over the MANET on regular intervals and SRRD_REP message in response of SRRD_REQ by the destination to the source node after matching SRRD_ID. SRRD_REP can only be generated by the destination node as assumption which means there is no role of other nodes.

In [2] proposed an Ant Colony Optimization algorithm to find the best route from source node to destination node. This algorithm can be implemented to solve the Traveling Salesman Problem in the Ad hoc Network. This algorithm gives the best solution for the shortest path problem in Ad hoc networks.

In [3] Proposed method that checking whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not.

In [4] Proposed SCAODV is Root nodes are created first. Root nodes are used for detection of malicious nodes. From source node RREQ is generated. At that time one timer is used for measuring current time.

In [5] the solution assumes that nodes are already authenticated and hence participate in communication. The approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and it is eliminated. The source node transmits the RREQ to all its neighbors.

In [6] the ACO inspired ad hoc routing protocols are considered in this work and put to partial comparison. Some of them are proactive, reactive or hybrid. And it can be evaluated that some of them may outperform the standard ad hoc routing protocols like AODV, DSDV, and DSR.

In [7] the multiple paths technique are established between source node and destination node using idea of Max Min Ant System and the isolation of malicious nodes are based on the DRPI table's (dynamic route pheromone bound value information table) values of THROUGH and FROM which promiscuously updated as the ant agents travels from

source to destination and vice versa. As seek road in the Ant colony algorithm, our improved secure mechanism introduce two kinds of ant as F-ANT and B-ANT. The function of F-ANT and B-ANT is same as the RREQ and RREP in AODV.

In [8] modify the AODV Protocol and propose a detection technique called Intrusion Avoidance System (IASAODV), which helps to detect and avoid the Black Hole nodes.

In [9] analyzed the effect of black hole attack in the performance of AODV protocol. The simulation results show that when the black hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol. So, the detection and prevention of black hole attack in the network exists as a challenging task.

In [10] Proposed Intrusion detection is based in collection and analysis of system and network audit data. Upon detection, intrusion should be reported to security management. It continuously monitors activities like packet traffic. Each mobile node runs IDS independently to observe behavior of neighboring nodes, looking signs of intrusion locally, making decision to prevent the system from attack or it can also request for data and actions from neighboring nodes if needed.

In [11] Proposed Intrusion Avoidance System (IASAODV) can be considered as modification of the AODV protocol and can be used to detect and avoid the black hole attack. The proposed algorithm is divided into major stages: The first stage is based on the routing messages of both RREQ and RREP messages that are exchanged in the route discovery. The second stage is based on the DSN of the RREP message, the number of RREP message(s) calculated in the first stage and the arrival time of RREP at the source.

In [12] Ant Colony Optimization (ACO) is used to modify the Ad-hoc On Demand Distance Vector (AODV) routing protocol. The ant place of at each node calculates its pheromone value by using the forwarding ratio at node.

In [13] proposed technique introduced a novel method against malicious attack in MANETs. This algorithm is proficient in providing an optimal path because operations to be performed in each node are very simple, thus it is robust and fault tolerant.

In [14] proposed a new protocol by enhancing the existing protocol IDSAODV. The solution is named as "Improved IDSAODV (IIDSAODV)". IIDSAODV uses the sequence number attribute of AODV protocol to overcome this problem.

In [15] introduced a prevention of black hole attack through IDS. The IDSAODV Protocol will discard the first RREP packet from Black Hole node and choose second coming RREP packet from destination. The IDSAODV Protocol will also find another path to destination.

In [16] the comparisons of three routing protocol have been measured between AODV, Secure AODV and Adaptive Secure AODV to study the performance of each routing protocols in a free-attack simulation environment.

In [17] introduced the main features of different simulator and consider their advantages and disadvantages.

In [18] the proposed aim to implement Ad-hoc on demand Distant Vector – particularly University of Indonesia AODV (AODV-UI) routing protocol on low-end inexpensive generic wireless routers as a proof of concept. AODV-UI is an improved version of AODV routing protocol that implements gateway interconnection and reverse route capability.

In [19] the 202 papers presented in special sessions and workshops cover a wide range of topics in computational sciences technologies to computational sciences technologies to specific areas of computational sciences such as computer graphics and virtual reality.

CHAPTER THREE

The Methodology

3.1 Introduction

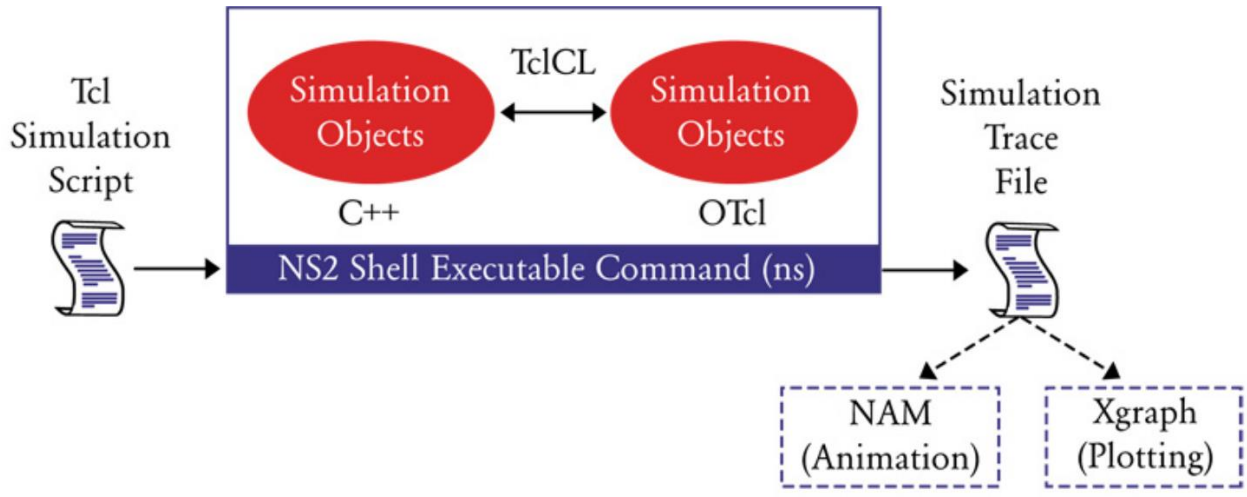
This section gives the overview of tools, performance metrics which are chosen for evaluating the performance of the techniques.

3.2 Simulation Environment

As surveyed in [17], there are many network simulators with different features and NS-2 is one of the most popular open source network simulators. Network Simulator (Version 2), widely known as NS2, is simply an event-driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community.

NS2 is a discrete-event simulator, where actions are associated with events rather than time. An event in a discrete-event simulator consists of execution time, a set of actions, and a reference to the next event. These events connect to each other and form a chain of events on the simulation timeline. Unlike a time-driven simulator, in an event-driven simulator, time between a pair of events does not need to be constant. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e.,a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). NS2 uses OTcl to create and

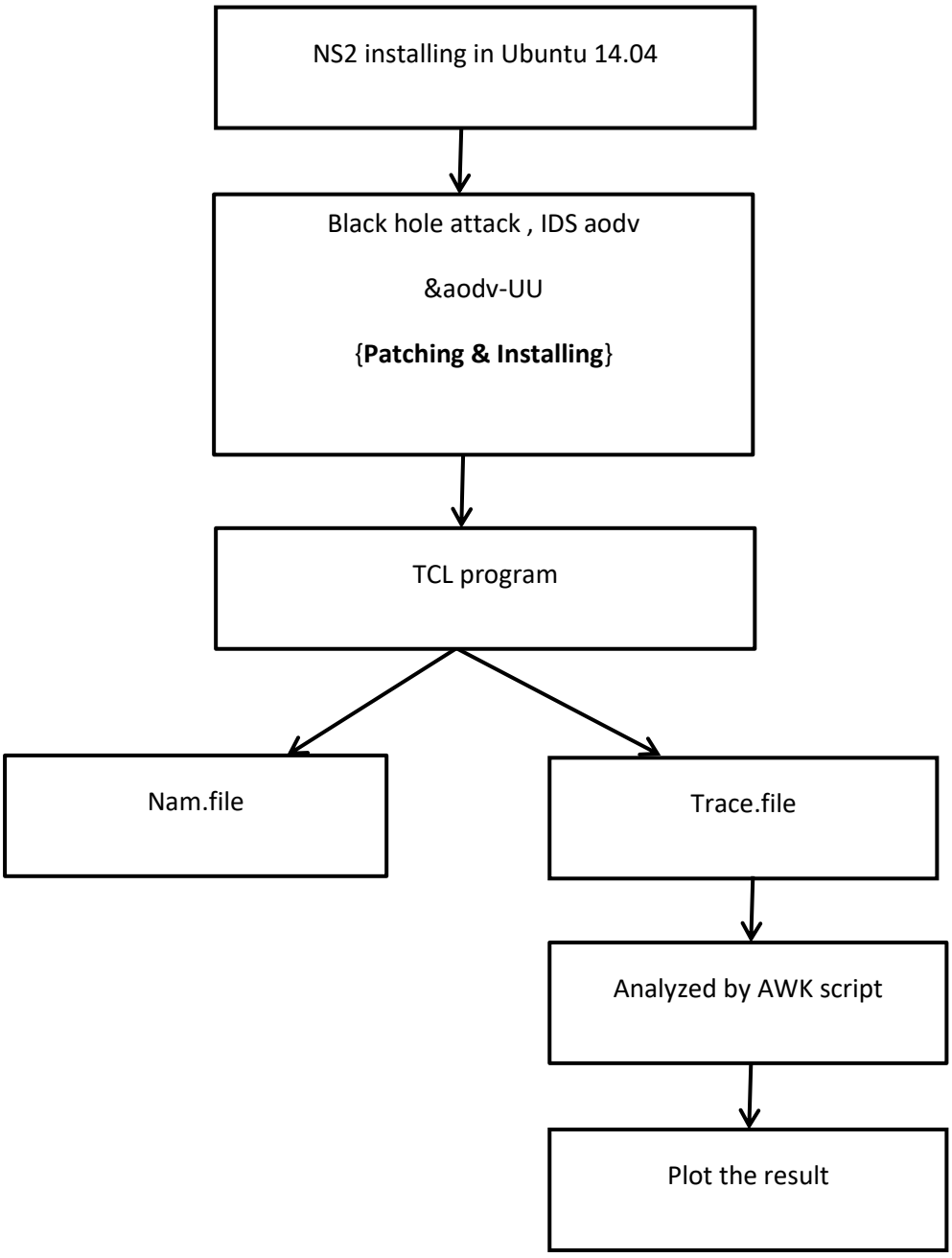
configure a network, and uses C++ to run simulation. All C++ codes need to be compiled and linked to create an executable file. Since the body of NS2 is fairly large, the compilation time is not negligible. OTcl, on the other hand, is an interpreter, not a compiler. Any change in an OTcl file does not need compilation. Nevertheless, since OTcl does not convert all the codes into machine language, each line needs more execution time. In summary, C++ is fast to run but slow to change. OTcl, on the other hand, is slow to run but fast to change. It is therefore suitable to run a small simulation over several repetitions (each may have different parameters). NS2 is constructed by combining the advantages of these two languages. NS2 provides users with an executable command ns which takes on input argument, the name of a Tcl simulation scripting file. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and XGraph are used. To analyze a particular behavior of the network, users can extract a relevant subset of text-based data and transform it to a more conceivable presentation.



Basic architecture of NS

Figure 3-1 Basic architecture of NS

3.3 Step of method



3.4 Performance Metrics

In the evaluation of routing protocols different performance metrics are used. They show different characteristics of the whole network performance.

3.4.1 Routing Overheads

The number of routing packets transmitted for every data packet sent. Each hop of the routing packet is treated as a packet. Normalized routing load are used as the ratio of routing packets to the data packets. As for the calculation, Normalized Routing Load = routing packets sent / packet received.

3.4.2 Packet Delivery Ratio

It can be measured as the ratio of the received packets by the destination nodes to the packets sent by the source node.

3.4.3 Average Delay

The delay experienced by packet from the time it was sent by a source till the time it reached the destination.

3.5 Evaluation Technique

To deploy the effect of black hole attack, a protocol "BLACKHOLEAODV" is implemented in ns-2. Node which adopts this protocol behaves like a black hole node. To reduce the effect of black hole attack, IDSAODV and AODV-UU are implemented. AODV is used as the basic routing protocol and all the data packets are CBR packets of size 512 bytes. To evaluate the routing overheads, packet delivery ratio and average delay; simulation is done with various number of mobile nodes and connections are number of source-destination pairs Network, simulator ns-2 (version 2.32) is used for the simulation. The AWK-scripts

are used to calculate the results and these results are plotted using graph. It should be noted that all the analysis and comparison is performed using a varying number of mobile nodes. And tested this scenario with AODV protocol in the first. Second, tested those protocols with various numbers of black hole attack by simulation models network of 10,20,30,40, and 50 mobile nodes. Network traffic and scenario are configured according to Table 3-1.

Table 3-1 Simulation Parameters

Parameters	Values
Simulation Time	500s
No. Of Nodes	10,20,30,40,50
Traffic Model	CBR
Protocol	AODV,ISDAODV,AODV-UU
Packet Size	512
Area	750 * 750
No. of attacker nodes	1,2,3,4,5

CHAPTER FOUR

Experimental Results and Observations

4.1 Introduction

The following tables 4-1 show the observations of the AODV, IDSAODV and AODV-UU protocols with various numbers of nodes to study the performance of each routing protocols in simulation environment using different performance metrics. The results are provided through graphs plotted as Performance metrics vs. numbers of node. In tables 4-2 Show the observations of those protocols also with various number of black hole attacks.

4.2 CBR Traffic

Table 4-1 Observations for Varying Number of Node

	Routing Over Heads			Packet Delivery Ratio (%)			Average Deley (msec)		
No OF Node	AODV	IDSAODV	AODV-UU	AODV	IDSAODV	AODV-UU	AODV	IDSAODV	AODV-UU
10	0.02	0.02	0	99.16	99.16	100	82.03	82.03	29.14
20	0.08	0.03	0.03	99.7	99.89	99.96	97.76	94.86	84.23
30	0.52	0.85	0.61	98.01	96.28	97.73	130.55	166.53	106.71
40	1.4	1.23	0.77	95.49	96.02	97.32	174.67	177.06	121.18
50	2.7	2.17	2.09	90.75	91.48	93.5	308.74	273.07	208.84

4.3 CBR Traffic with Black Hole

Table 4-2 Observations for Varying Number of Nodes within number of attack begin from (1) attack when the node (10) and increases by one in each set of node.

	Routing Over heads			Packet Delivery Ratio (%)			Average Deley (msec)		
No.of Node	AODV	IDSAODV	AODV-UU	AODV	IDSAODV	AODV-UU	AODV	IDSAODV	AODV-UU
10	0.01	0.01	0.01	0.16	0.16	100	1013.97	1013.97	20.13
20	0.34	0.26	0.05	0.8	11.73	99.87	134.91	168.49	71.08
30	0.1	0.28	0.25	7.64	16.38	99.17	60.87	64.44	86.98
40	0.26	0.45	0.46	0.7	6.22	98.66	1156.79	198.4	105.94
50	0.4	0.75	1.98	13	4.72	93.64	244.98	180.46	173.62

4.2.1 Routing Overheads

Figure 4-1 Represent the total amount of Routing Overheads collected during the simulations against the number of Nodes for the considered protocols obtained by table 4-1.

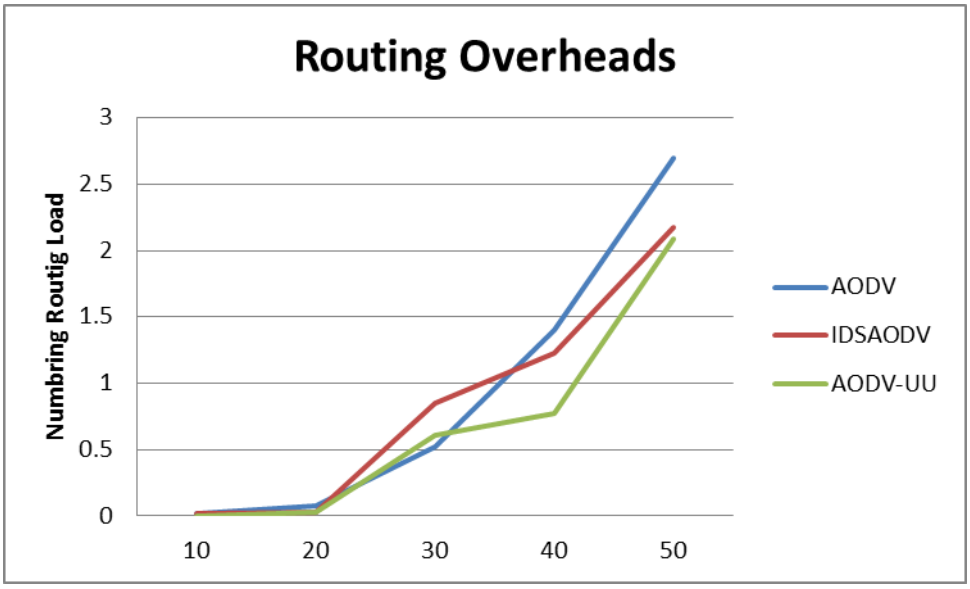


Figure 4-1 Routing Overheads vs. Number of Nods

The results from figure 4-1, show that the routing overhead decreased when the number of nodes decreased, because AODV performance is reduce when number of nodes equal (50) or more, AODV-UU is outperform the other two routing protocols AODV perform better than IDSAODV but when moving to larger number of node (starting from 40 nodes), IDSAODV gives better outputs towards the end compared with AODV.

4.3.1 Routing Overheads with Black hole

Figure 4-4 Represent the total amount of Routing Overheads collected during the simulations against the number of black hole attacks and Nodes for the considered protocols obtained by table 4-2.

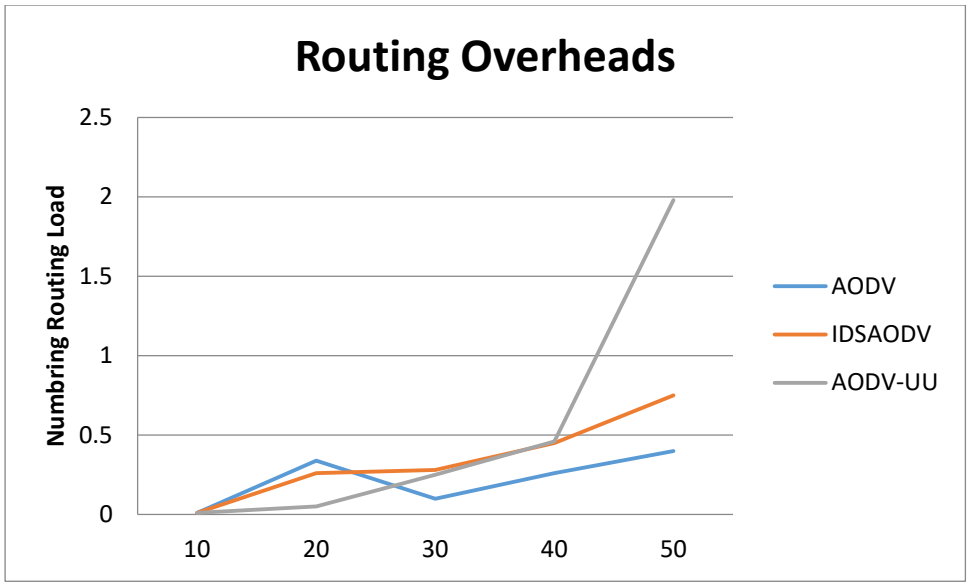


Figure 4-4 Routing Overheads vs. No of Nods & black holes

The result shows that AODV-UU had higher overheads when number of nodes (50) with black hole attacks (5) because AODV performance is reduce when the number of nodes equal (50) and AODV-UU performance not effect when black holes attacks is deployed. AODV had lower overheads compared with IDSAODV because they had lower throughput when black holes is deployed.

4.2.2 Packet Delivery Ratio

Based on the observations of table 4-1, the response of packet delivery ratio in % against varying number of Nodes is shown in Figure 4-2.

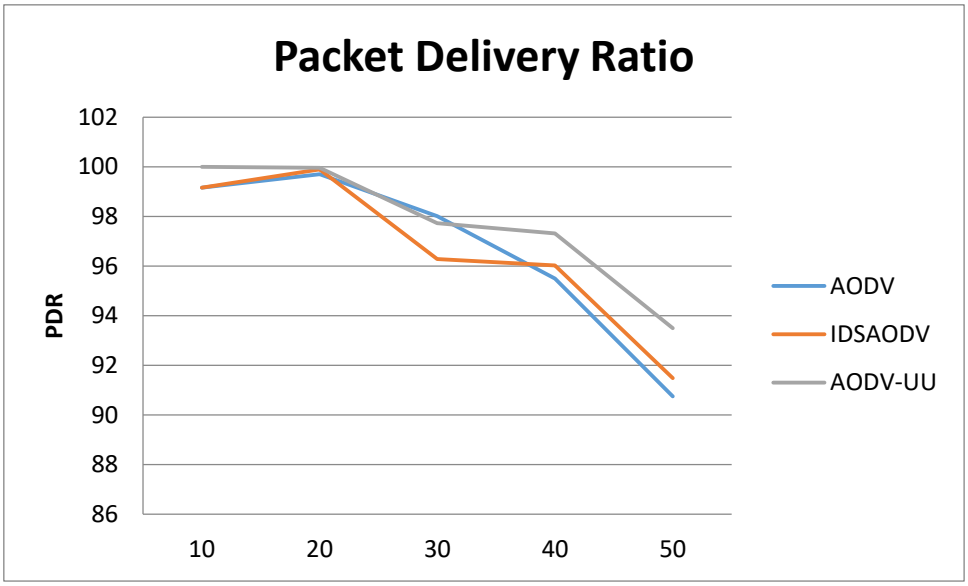


Figure 4-2 Packet Delivery Ratio vs. Number of Nods

From the figure 4-2, the result shows that AODV-UU outperform both AODV and IDSAODV in PDR percentage. It means that AODV-UU produced more throughputs compared to AODV and IDSAODV, AODV and IDSAODV they have similar perform in PDR percentage. IDSAODV had lower PDR when the number of nodes (30) compared to AODV-UU and AODV, AODV-UU established the communication between nodes before the request of the routing starting from the nodes because that had better performance from begging.

4.3.2 Packet Delivery Ratio with Black hole

Based on the observations of table 4-2, the response of packet delivery ratio in % against varying number of black holes and Nodes is shown in Figure 4-5.

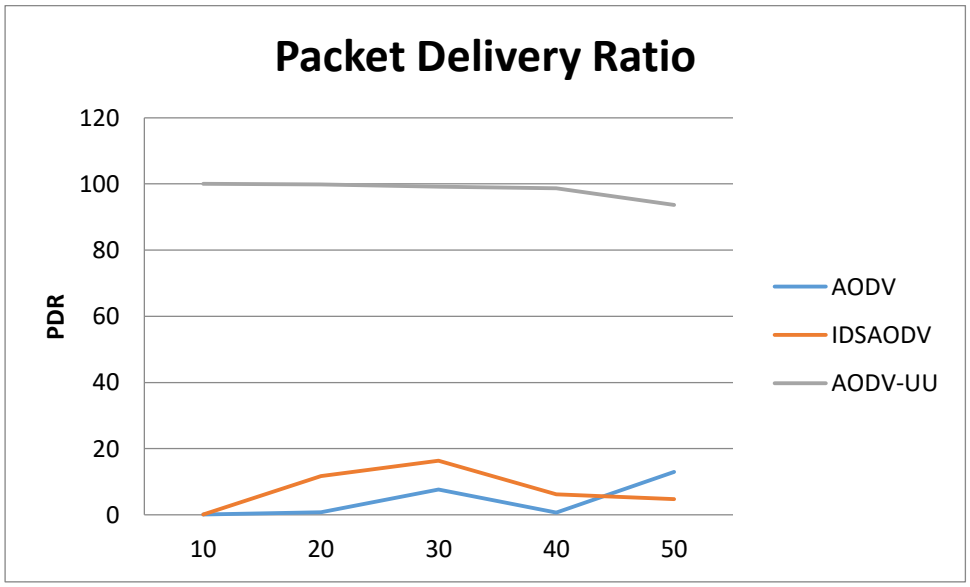


Figure 4-5 PDR vs. No of Nods & black holes

From the figure 4-5, the result shows that AODV-UU outperform both AODV and IDSAODV in PDR percentage. IDSAODV perform better than AODV. AODV-UU performance not effect when black hole attacks is deployed reverse to AODV and IDSAODV they had lower throughput.

4.2.3 Average Delay

Based on the observations of table 4-1, the response of Average Delay msec against varying number of Nodes is shown in Figure 4-3.

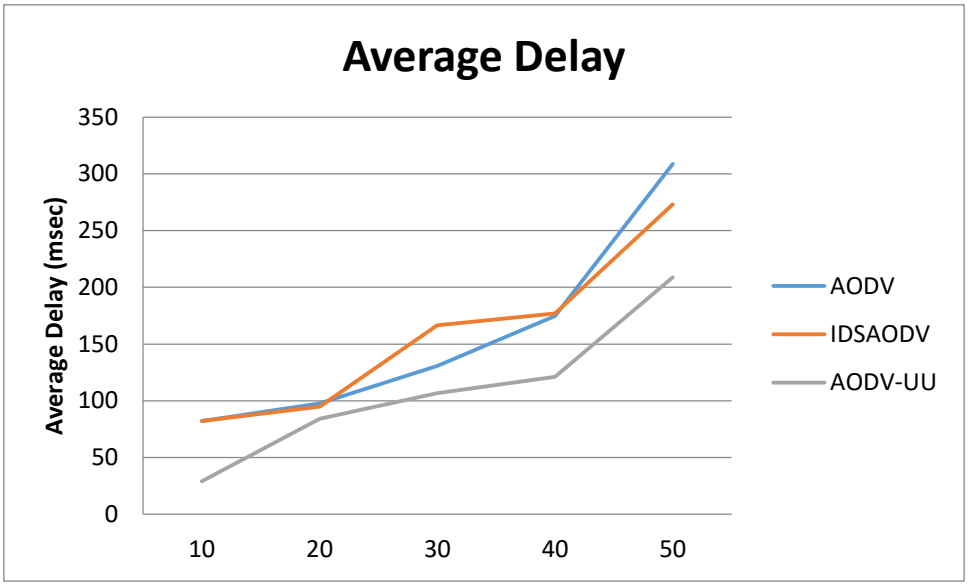


Figure 4-3 Average Delay vs. Number of Nodes

As the results shown in figure 4-2, higher delays produced in AODV and IDSAODV. And also we can see that AODV-UU had lower delay and giving much better performance compared to AODV & IDSAODV.

4.3.3 Average Delay with Black hole

Based on the observations of table 4-2, the response of Average Delay (msec) against varying number of black hole is shown in

Figure 4-6.

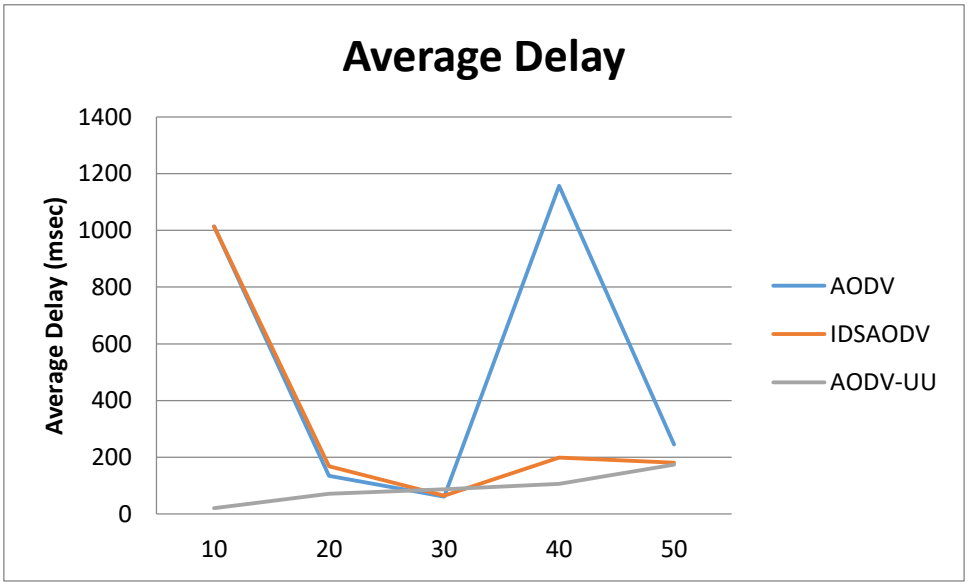


Figure 4-5, Average Delay vs. No of Nods & black holes

As the results shown in figure 4-5, there are some unstable results collected from AODV and IDSAODV compared AODV-UU because the black holes attacks drop most of the packets, When the no. of nods are (10, 40) with black holes (1, 4) the higher delays produced in AODV and IDSAODV when the no. of node is (10) with black hole (1), AODV-UU had lower delay and the performance of AODV-UU don't effect when black holes attacks is deployed.

CHAPTER FIVE

Conclusions

5.1 Conclusions

The simulation results show that when the black hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol. We introduced a black hole attacks in each scenario and compared the performance of the networks with and without a black hole. We also introduced a prevention of black hole attack through IDSAODV and AODV-UU. For this we implemented IDSAODV and AODV-UU protocols. The observation and results with black hole attacks shows that overhead decreases in the presence of AODV and IDSAODV because they had lower throughput and in AODV-UU did not change from overheads without black hole. While the performance of IDSAODV protocol using same network matrices it looks similar to AODV because the defense mechanism is weak. AODV-UU provides the best results for packet delivery ratio and average delay when implement number of black hole attacks and without implement the black hole attacks. And finally, the best routing protocol could be chosen, but still totally depends on the requirements of that routing environment or systems.

5.2 Recommendations for Future Work

As a future work, study the effect of other attacks can be occur on AODV such as wormhole and gray hole and implement AODV-UU routing protocol in different scenario within those type of attacks to evaluate AODV-UU performance under those threats in different Performance Metrics and can compere between AODV-UU and anther MANT routing protocol to study the level protection for all threats in each of them.

BIBLIOGRAPHY

[1] Anuj Ranaa, Vinay Ranab , Sandeep Guptac, EMAODV: TECHNIQUE TO PREVENT COLLABORATIVE ATTACKS IN MANETs, ScienceDirect, 2015.

[2] Somesh Maheshwari, Manish Bhardwaj, Secure Route Selection in Manet Using Ant Colony Optimization, Journal of Networks and Communications, Vol. 4, No. 3-1, pp. 54-56, 2015.

[3] Pooja Jaiswal, Dr. Rakesh Kumar, Prevention of Black Hole Attack in MANET, IRACST – International Journal of Computer Networks and Wireless Communications, Vol.2, No5, October 2012

[4] Shailja Sharma ,Umesh Kumar Singh, Kailash Chandra Phuleriya, SCAODV: A Protocol to Prevent Black Hole Attacks in Mobile Ad Hoc Networks, International Journal of Computer Science & Communication, Vol.6, issue 2, 2015.

[5] Nigahat, Dr. Dinesh Kumar, BLACK HOLE DETECTION AND PREVENTION USING AODV AND SHORTEST DISTANCE TECHNIQUE, NTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, Value: 3.00 , April, 2017.

[6] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, MANET Routing Protocols Based on Ant Colony Optimization, International Journal of Modeling and Optimization, Vol. 2, No. 1, February 2012.

[7] Sharndeep Kaur, Dr. Anuj Gupta, A Novel Technique to Detect and Prevent Black Hole Attack in MANET, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 6, June 2015.

[8] Tarek M. Mahmoud, Abdelmgeid A. Aly, and Omar Makram, Avoiding Black Hole attack of AODV routing protocol in MANET, Int. J. on Network Security, Vol.6, 2015.

[9] Ei Ei Khin, Thandar Phyu, IMPACTOFBLACKHOLEATTACKONAODVROUTING PROTOCOL, International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.

[10] Nisha, Simranjit Kaur, Sandeep Kumar Arora, Analysis of Black Hole Effect and Prevention through IDS in MANET, American Journal of Engineering Research (AJER), Volume-02, Issue-10, pp-214-220, 2013.

[11] Tarek M. Mahmoud, Abdelmgeid A. Aly, Omar Makram M, A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs, International Journal of Computer Applications, Volume 109 – No. 6, January 2015.

[12] C.V. Anchugam , K. Thangadurai, Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization – simulation Analysis, Indian Journal of Science and Technology, Vol 8(13), , July 2015.

[13] Sharndeep Kaur, Dr. Anuj Gupta, A Novel Technique to Detect and Prevent Black Hole Attack in MANET, International Journal of Innovative Research in Science, Engineering and Technology , Vol. 4, Issue 6, June 2015.

[14] Ankita Chaturvedi, Sanjiv Sharma, A New Technique for Preventing Black Hole Attack in Mobile Ad-hoc Networks, International Journal of Advances in Computer Science and Technology, Volume 3, No.10, October 2014.

[15] Nisha, Simranjit Kaur, Sandeep Kumar Arora, Analysis of Black Hole Effect and Prevention through IDS in MANET, Volume-02, Issue-10, pp-214-220, 2013.

[16] C. Sreedhar, Dr. S. Madhusudhana Verma, Dr. N. Kasiviswanath , Performance Analysis of Secure Routing Protocols in Mobile Ad-Hoc Networks, International Journal of Computer Science and technology, Vol. 3, Issue 1, Jan. - March 2012.

[17] Saba Siraj, et al, Network Simulation Tools Survey, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2012.

[18] Boma Anantasatya Adhi, Ruki Harwahyu, Abdusy Syarif, Harris Simaremare, Riri Fitri Sari, and Pascal Lorenz, AODV-UI Proof of Concept on MIPS-based Wireless Router, JOURNAL OF COMMUNICATIONS SOFTWARE AND SYSTEMS, VOL. 10, NO. 1, MARCH 2014.

[19] Beniamino Murgante, Sanjay Misra, Maurizio Carlini, Carmelo Torre, Hong-Quang Nguyen, David Taniar, Bernady O. Apduhan, Osvaldo Gervasi, Computational Science and Its Applications -- ICCSA 2013: 13th International Conference, ICCSA 2013, Ho Chi Minh City, Vietnam, June 24-27, 2013, Proceedings, Part 3.