Sudan University of Science and Technology

COLLEGE OF GRADUATE STUDIES

Enhanced Detection of Malicious Nodes in Ad-hoc on Demand Distance Vector Protocol using Cross Layer Design

كشف محسن للعقد الخبيثة في بروتوكول متجه المسافة المخصص عند الطلب باستخدام تصميم الطبقات المتقاطعة

A Research Submitted in Partial fulfillment for the E Requirements of the Degree of M.Sc in Electronics Engineering (computer & networks)

Prepared By:

Weaam Ahmed Mohamedali Hassan

Supervised By:

Dr. FathElrahmanIsmaelKhalifa

Dec 2018

الاستهلال

﴿ وَمِنَ النَّاسِ وَالدَّوَابِّ وَالْأَنْعَامِ مُخْتَلِفٌ أَلْوَانُهُ كَذَلِكَ إِنَّمَا يَخْشَى اللَّهَ مِنْ عِبَادِهِ الْعُلَمَاءُ إِنَّ اللَّهَ عَزِيزٌ غَفُورٌ ﴾

صدق الله العظيم

سورة فاطر (28)

DEDICATION

With love and respect

Dedicated to my mother

Dedicated to my father

Dedicated to my siblings

Whom I cherish their friendship

Dedicated to my beloved husband

Dedicated to my special people

… Who mean so much to me

….Dedicated to all my teachers

…… In whom I believe so much

ACKNOWLEDGEMENTS

I would like to acknowledge and express my gratitude to- after Allah the Almighty – my beloved ones For the incorporeal and financial support they have been giving me . And for all those whomever helped me on this research ,especially my supervisor Dr/Fath-Elrhman Ismail Khalifa , who was the foundation stone for this research.

The thanks also to all those who ever gave me any piece of information or data about this research no matter how important it was , and to whomever gave me few minutes of their time and efforts from teachers to college.

Finally, I am pleasured to give the thanks and credits to Sudan University of Science and Technology-Collage of Engineering-School of Electronics Engineering ,where I have studied, and I ask Allah that it keeps on serving the education, science and country.

ABSTRACT

A Mobile Ad-Hoc Network (MANET) is a popular type of wireless network that is formed by a collection of mobile nodes. Each node in such network has the capability to communicate with its neighbors and non-neighbors through a wireless medium designed to accommodate the properties of a self-organized environment without protection against any inside or outside network attacks. In addition to, it does not have any central authority to ensure that any node in the network it is not malicious, which introduces security flaws to the networks. we propose security policy to detect malicious nodes over the Ad hoc On Demand Distance Vector (AODV) MANET routing protocol. To improve security in AODV routing protocol- which adds extra features to it and making path formation more secure- we are Using Cross-layer design shares knowledge about the state and conditions of one layer to the other layers. In this work, the link and routing layer are considered. In the security policy. The algorithm that is used in AODV protocol benefits from the in-formations feedback-coming from link to network layer- clarifying the number of requests sent from the nodes is shown to indicate whether the node is malicious or not. The improvement of the system performance considers the achieved result of this research using the mat-lab simulator. It evaluates the AODV security performance metrics in term of end-to-end delay which has average of values equal 7.9140, the overall improvement increasing in the bit rate and Packet delivery ratio**, and** Throughput with average of values are 6.2595, 0, 0016 and 0, 9313 respectively.

المستخلص

إن شبكة المانيت هي نوع شائع من الشبكات اللاسلكية التي يتم تشكيلها من خلال مجموعة من العقد المتنقلة. كل عقدة في هذه الشبكة لديها القدرة على التواصل مع جيرانها وغير الجيران من خلال وسيلة لاسلكية مصممة لاستيعاب خصائص بيئة ذاتية التنظيم دون حماية ضد أي هجمات داخلية أو خارجية. وليس لديها أي سلطة مركزية للتأكد من أي عقدة في الشبكة على أنها عقدة خبيثة مما يؤدي ذلك إلى عيوب أمنية في الشبكة. نحن نقترح سياسة أمنية للكشف عن العقد الخبيثة عبر بروتوكول متجه المسافة المخصص عند الطلب. لتحسين الأمان في بروتوكول التوجيه بإضافة ميزات إضافية إليه وجعل تكوين المسار أكثر أمانا، نستخدم تصميم الطبقات عبر مشاركة المعلومات حول حالة وظروف طبقة واحدة إلى الطبقات الأخرى. في هذا العمل يتم اعتبار طبقة الارتباط وطبقة التوجيه. في سياسة الأمن ، تستفيد الخوارزمية الأمنية المستخدمة في بروتوكول)متجه المسافة المخصص عند الطلب) من المعلومات الراجعة أو الواردة من طبقة الارتباط إلى طبقة التوجيه– توضح عدد الطلبات المرسلة من العقد لتوضيح ما إذا كانت العقدة ضارة أم لا. يعتبر تحسين أداء النظام النتيجة المحققة لهذا البحث باستخدام برنامج المحاكاة(ماتلاب)، يقوم بتقييم مقاييس أداء أمن متجه المسافة المخصص عند الطلب من حيث التأخير من طرف إلى طرف والذي انخفض بمتوسط قيم 7,9140، وزيادة التحسين العام في معدل البت ونسبة حزم البيانات والإنتاجية بمتوسط قيم 6,2595، 0,0016، 0,9313 على التوالي .

TABLE OF CONTENT

LIST OF FIGURE

LIST OF TABLES

LIST OF abbreviations

AODV	AD Hoc On Demand Distance Vector Routing Protocol
CTS	Clear To Send
DDOS	Distributed Denial Of Service
DSR	Dynamic Source Routing
DSDV)	Destination Sequenced Distance Vector
(EN –SIM AODV	Encrypt Security Improved AODV
IP SEC	Internet Routing Protocol
MANET	Mobile Ad Hoc Network
MPR	Multiple Point Relays
OLSR	Optimized Link State Routing
OSI	Open System Interconnection
PDA	Packet Drop Attack
RTS	Request To Send
RREQ	Route Request
RREP	Route Replay
SE AODV	Security AODV
SRP	Secure Routing Protocol
TC	Topology Control
TCP	Transmission Control Protocol
TAODV	Trusted AODV
TID	Tropical Intrusion Detection
ZRP	Zone Routing Protocol

LIST OF SYMBOLS

Nd	Node Delay Time ms	
Td	Transmission Delay Time in ms	
Rd	Receiving Delay Time in ms	
Pd	Processing Delay time in ms	
Pdr	Packet delivery ratio	

CHAPTER ONE

Introduction

CHAPTER ONE

INTRODUCTION

1.1Preface:

A Mobile Ad-Hoc Network (MANET) is a popular type of wireless network that is formed by a collection of mobile nodes. Each node in such network has the capability to communicate with its neighbors and non-neighbors through a wireless medium without using any existing network infrastructure. Due to the lack of infrastructure, all nodes in Ad-Hoc network are designed to act as an end system and a router for other nodes[1].There are infrastructure-less networks where all the nodes act as host as well as routes to deliver data. By the nature and the architecture, the performance is affected by channel conditions, network connectivity, mobility and resource limitations, to improve different performance metrics of MANET, various cross-layering approaches are utilized where different OSI layer information is exchanged between different layers of the protocol stack, and end-to-end performance is optimized by adapting to this information at each protocol layer. And their associated routing protocols. MANET has the lot of challenges so that network needs some standardized way (routing protocol) to make a communication between two mobile nodes with more security and less time.

AODV is a popular distance vector proactive routing algorithm. create and maintain routes only if these are needed, on demand. They usually use distance-vector routing algorithms that keep only information about next hops to adjacent neighbors and costs for paths to all known destinations. Resent days Mobile Ad Hoc Network (MANET) mostly uses reactive on-demand routing protocols where routes are launch only when the node needed. Most of the protocols which one is belongs to this category are not including proper security facilities [2].Security is the major concern

problem in MANET as to provide infrastructure less wireless network and where any node without any authentication comes in the network and leaves network there is no central authority that can govern the authentication of nodes, which can make sure that the nodes in the network are not malicious. To achieve efficient, secure and reliable routing path for MANETs, we propose a routing mechanism that uses cross layer strategies[3]. The cross-layer strategy involves incorporating feedback and information from layers below the network layer to make decisions at the network layer[4].

1.2Problem Statement

MANETs use wireless media for transmission where scattered over a large area, some nodes or network components may be unmonitored or hard to monitor, and exposed to the physical attacks and do not have any central authority to detection and to be ensure that any node in the network is not a malicious, which introduces security flaws to the networks.

1.3 Proposed Solution

The solution of the above mentioned problem is to modify AODV routing protocol based on CROSS LAYER DESIGN by exchange information between layers and apply different detection scheme to increase level of security and reliability in MANET.

1.4 Research aims and objectives

The aim of this research is to improve security of AODV routing protocol based CROSS LAYER DESIGN simulate the operation of AODV.

The detailed objectives of this research are include:

- To improve traffic throughput.
- To enhance bit rate.
- To reduce end to end delay.
- To increase packet delivery ratio.

1.5 Methodology

There is a sequence of facts and event that was concerned to accomplish this researcher. Having knowledge of security of the AODV routing protocol with in-formations gathered from different layers (CROSS LAYER DESIGN) and how its work is the major step to achieve the objectives of this research and enhance security policy in the Manet network, then a mathematical coordination of the system algorithms and the system parameters get covered. The operation of the AODV routing protocol will be enhanced with cross layer design by using malicious detection mechanism and helping information feedback from Mac to network layer. The enhanced algorithm is simulated by mat-lab code, and for the improvement of the system performance a simulation of the objectives research parameters performance improvements is applied as results (decrease the end to end delay, increase the bit rate, **Packet delivery ratio**, and Throughput) and finally the thesis is documented.

1.6 Thesis outlines

This thesis is organized as follows : Chapter one consist of preface, problem statement, proposed solution, research aims and objective, and thesis outlines, Chapter Two consist of literature review it contain :related works of cross layer design , AD hoc networks, AODV routing protocol and different methods to implementand enhance security in each other .Chapter Three consists of research methodology, which is the security algorithms of AODV based cross layer design parameters and their mathematical representations. Chapter Four include the simulation and result contain of :Simulation of AODV algorithm using Mat-lab program , and security parameters such as, resource limitations, traffic throughput, overhead, end to end delay. Chapter Five summarizes the results obtained in this thesis.

CAPTER TWO

Literature Review

CHPTER TWO

Literature Review

2.1 Background of Wireless Network

The wireless communication landscape has been changing dramatically, driven by the rapid advances in wireless technologies and the greater selection of new wireless services and applications. The emerging third-generation cellular networks have greatly improved data transmission speed, which enables a variety of higher-speed mobile data services.

Meanwhile, new standards for short-range radio such as Bluetooth, 802.11, Hiperlan, and infrared transmission are helping to create a wide range of new applications for enterprise and home networking, enabling wireless broadband multimedia and data communication in the office and home. Before delving into these technologies and applications, we first examine some of the main characteristics of wireless communication as related to specification and classification of these networks, and then review the key capabilities exhibited by the various types of wireless networks **[5].**

2.1.1Wireless Communication Characteristics

In general, wireless networking refers to the use of infrared or radio frequency signals to share information and resources between devices.

Many types of wireless devices are available today; for example, mobile terminals, pocket size PCs, hand-held PCs, laptops, cellular phone, PDAs, wireless sensors, and satellite receivers, among others. Due to the differences found in the physical layer of these systems, wireless devices and networks show distinct characteristics from their wire line counterparts, specifically

Higher interference results in lower reliability, Infrared signals suffer interference from sunlight and heat sources, and can be shielded/absorbed by various objects and materials. Radio signals usually are less prone to

being blocked; however, they can be interfered with by other electrical devices.

The broadcast nature of transmission means all devices are potentially interfering with each other, Self-interference due to multipath, Low bandwidth availability and much lower transmission rates, typically much slower-speed compared to wire line networks, causing degraded quality of service, including higher jitter, delays, and longer connection setup times, Highly variable network conditions, Higher data loss rates due to interference, User movement causes frequent disconnection , Channel changes as users move around, Received power diminishes with distance, Limited computing and energy resources: limited computing power, memory, and disk size due to limited battery capacity, as well as limitation on device size, weight, and cost, Limited service coverage. Due to device, distance, and network condition limitations, service implementation for wireless devices and networks faces many constraints and is more challenging compared to wired networks and elements.

2.1.2 Types of Wireless Networks

Many types of wireless networks exist, and can be categorized in various ways set out in the following subsections depending on the criteria chosen for their classification. by Network Formation and Architecture, Wireless networks can be divided into two broad categories based on how the network is constructed and the underlining network architecture:

a- Infrastructure-based network:

A network with pre-constructed infrastructure that is made of fixed and wired network nodes and gateways, with, typically, network services delivered via these preconfigured infrastructures. For example, cellular networks hare infrastructure-based networks built from PSTN backbone switches, MSCs, base stations, and mobile hosts. Each node has its specific responsibility in the network, and connection establishment follows a strict

signaling sequence among the nodes [6]. WLANs typically also fall into this category.

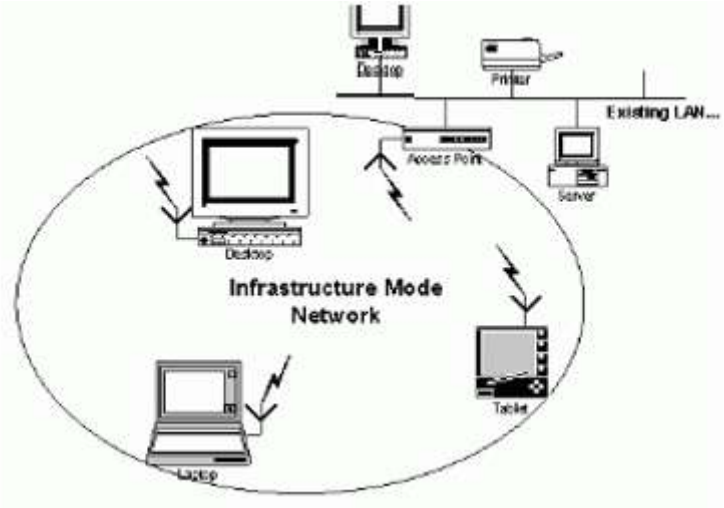

Figure 2.1: Infrastructure Network

b- Infrastructure-less (ad hoc) network:

In this case a network is formed dynamically through the cooperation of an arbitrary set of independent nodes. There is no prearrangement regarding the specific role each node should assume. Instead, each node makes its decision independently, based on the network situation, without using a preexisting network infrastructure. For example, two PCs equipped with wireless adapter cards can set up an independent network whenever they are within range of one another. In mobile ad hoc networks, nodes are expected to behaves routers and take part in discovery and maintenance of routes to other nodes[7].

A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves in a random fashion, thus the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger

Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations etc. Each of the nodes i.e. the mobile routers has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure2.1 shows a simple example of a mobile ad-hoc network with three nodes Node A, Node B, and Node C. Assuming, Node A and Node C are not within range of each other to exchange information; however the Node B can be used to forward data packets between Node A and Node C as Node B is within the range of both Node A and Node C. The Node B will act as a router and these three nodes together form a mobile ad-hoc network having the path named as A-B-C.

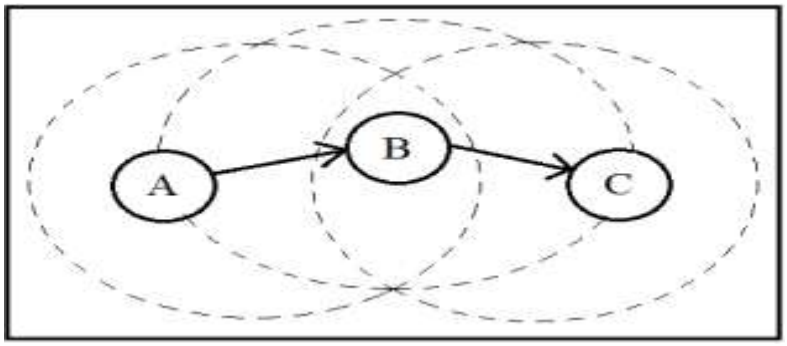

Figure 2.2: Example of a Mobile Ad-Hoc Network

2.1.3 Characteristics of Mobile Ad hoc Network

Characteristics of Mobile Ad hoc Network are as follows:-

Distributed nature: The control of the network is distributed among the nodes, there is no centralize concept between nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

Multi hop routing: When any node tries to send information to other nodes, the destination node is not in the source node's communication range, the packet should be forwarded via one or more intermediate nodes. Behave as an Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router. Dynamic topology: Nodes can move arbitrarily with different speeds; thus, the network topology may change randomly at unpredictable time. The nodes in the MANET dynamically establish routing among themselves. Light-weight terminals: The nodes at MANET are mobile in nature having less CPU capability, power storage and small memory. Shared Physical Medium: With the appropriate equipment and adequate resources the wireless communication medium is accessible to any entity. Accordingly, access to the channel cannot be restricted [8].

2.1.4 Benefits of MANET

Highly suitable network in such circumstances where fixed infrastructure is too much costly, un trustworthy, not trusted and due to unavailability of such a network. Quickly installation with least possible user intervention. Detailed planning and installation of base stations is not required. Ad hoc networks can be attached to the WWW or Internet, thereby incorporating many different devices and making possible for other users to use available services. Capacity, range and energy arguments promote their use in tandem with existing cellular infrastructures as they can extend coverage and interconnectivity. MANET also fitted to use the future 4G architecture and their services, aims to provide ubiquitous computer environments that support users in completing their tasks, accessing information and communicating anywhere , anytime and from any device [9].

2.1.5 Classification of routing protocols in MANET:

In MANET there are different types of routing protocols for routing the packets. Each routing has own rule to packet transfer method from source to destination.

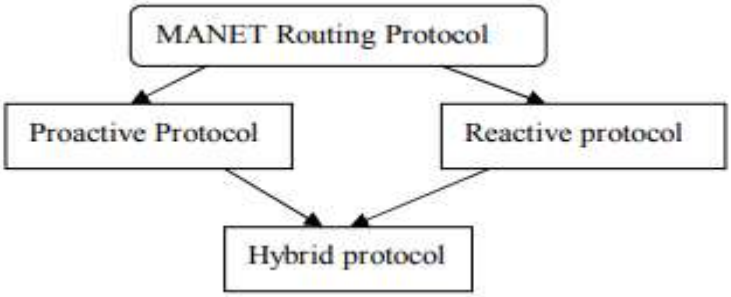

Figure 2.3 MANET Routing Protocols

a. Proactive Protocol

In this routing protocol network have unique routing table for send the data packets and want to establish connection to other nodes in the network. This protocol one type of demand-based operation which utilize network order to energy and bandwidth more efficiently. Pattern on a demand basis rather than maintaining routing between all nodes at all time. This is the flip-side of demand-based operation. In cases where the additional latency which demand-based operations may be unacceptable, if there are adequate bandwidth and energy resources, proactive operations may be desirable in these situations [6, 7, 8]. There are different type of proactive protocol like, Destination-Sequenced Distance-Vector (DSDV), Fisheye State Routing (FSR), Source Tree Adaptive Routing (STAR), Optimized Link-State Routing (OLSR), Cluster head gateway switch routing (CGSR), Wireless routing protocol (WRP), Global state routing (GSR)[10].

Optimized Link State Routing (OLSR)

It is a proactive routing protocol where the routes are always available when needed. OLSR is an optimized version of a pure link state protocol. The topological changes cause the flooding of the topological information to all available hosts in the network. To reduce the possible overhead in the network protocol multipoint relays (MPR) are used. Reducing the time interval for the control messages transmission brings more reactivity to the topological changes, OLSR uses two kinds of the control messages namely hello and topology control. Hello messages are used for finding the information about the link status and the host's neighbors. Topology control messages are used for broadcasting information about its own advertised neighbors, which includes at least the MPR selector list [11].

Destination Sequenced Distance Vector (DSDV)

DSDV is one of the most widely known proactive or table-driven routing protocols for MANETs [12].

The routing algorithm of DSDV is depended on the numeral of hops to arrive at the destination node. To transmit the data packets among the nodes in the network, DSDV protocol utilizing routing tables which are stored in every node. DSDV protocol has three major characteristics which are: decreasing the high routing overhead, solve the "count to infinity" problem and avert the loops. Each mobile node contains a table of routing information which includes all the routes to the destinations and information [13]. Figure 3 shows the advantages and disadvantages of DSDV protocol [14].

b. Hybrid protocol

It is a one special type protocol that separates the network into several zones, which makes a hierarchical protocol as the protocol ZHLS (zone-based hierarchical link state). this protocol which effectively combines the

best features of proactive and reactive routing protocol Hybrid routing protocol is based on GPS (Global positioning system), which allows each node to identify its physical position before mapping an area with table to identify it to which it belongs. Reactive protocols obtain the necessary route when it is required, by using route discovery process. In proactive protocols, nodes periodically exchange information to maintain up-to-date routing information. Hybrid routing protocols combine basic properties of both approaches [15].

There are different types of Hybrid protocol like, Zone routing protocol (ZRP), Zone-based hierarchical link state routing protocol.

Zone Routing Protocol (ZRP)

Proactive routing uses excess bandwidth to maintain routing information, while reactive routing involves long route request delays. Reactive routing also inefficiently floods the entire network for route determination. The zone routing protocol (ZRP) aims to address the problems by combining the best properties of both the proactive and reactive approaches. In ad-hoc network, it can be assumed that the largest part of the traffic is directed to nearby nodes. Therefore, ZRP reduces the proactive scope to a zone centered on each node. In a limited zone, the maintenance of routing information is easier. Further, the amount of routing information never used is minimized. In ZRP each node is assumed to maintain routing information only for those nodes that are within its routing zone. Because the updates are only propagated locally, the amount of update traffic required to maintain a routing zone does not depend on the total number of network nodes. A node learns its zone through a proactive scheme Intra zone Routing Protocol (IARP). For nodes outside the routing zone, Inter zone Routing Protocol (IERP) is responsible for reactively discovering routes to destinations located beyond a node's routing zone. The IERP is distinguished from standard flooding-based query/response protocols by

exploiting the structure of the routing zone. The routing zones increase the probability that a node can respond positively to a route query. This is beneficial for traffic that is destined for geographically close nodes [16].

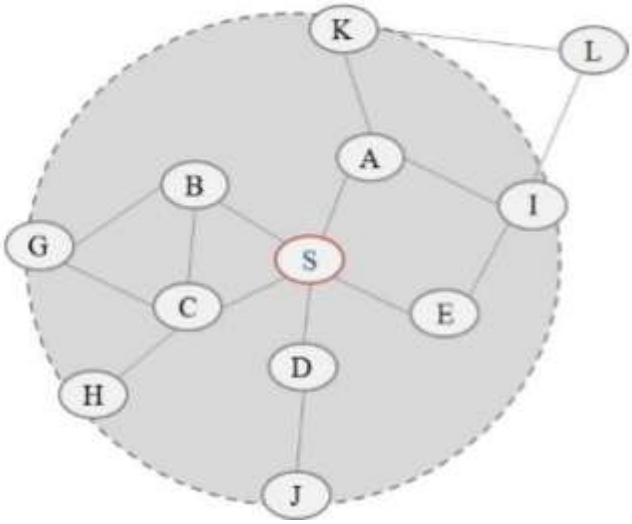

Figure 2.4: Zone Routing Protocol

c. Reactive (on-demand) protocol

These protocols enable dynamic, self-starting, multi-hop routing between mobile nodes wishing to establish and maintain an Ad-hoc network. This protocol does not require nodes to maintain routes to destination that are not in active communication and obtain routes quickly for new destination by route discovery procedure. Reactive protocols are being more efficient at signaling and power consumption, suffers longer delay while route discovery. Proactive and reactive protocols have been improving to be more scalable, secure and to support higher quality of service. Some of the reactive protocols are: Cluster Based Routing Protocols (CBRP), Ad-hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Temporary Ordered Routing Algorithm (TORA)[17].

Table 2.1: Reactive protocol

Destination addr	Next-hop addr	Destination sequence	Hop count	Life time

Ad-Hoc on Demand Distance Vector Protocol (AODV)

The Ad-hoc On-Demand Distance Vector protocol is a very simple, efficient and effective routing protocol for mobile Ad-hoc networks which do not have fixed topology. Every node in the network acts as a specialized router and the routes are obtained as needed, which makes the network self-starting. As the protocol does not require periodic global advertisements, the demand on the available bandwidth is less. A monotonically increased sequence number counter is maintained by each node in order to supersede any stale cached routes. The route discovery process consists of a route-request message (RREQ) which is broadcasted [18]. If a node has a valid route to the destination, it replies to the route-request with a route-reply (RREP) message. The destination node uses the so called reverse route entry in its routing table, which contains the no. of hops to source node, address of the source node, and the address of the node from which it receives the message i.e. the next hop's address. Coping up with dynamic topology and broken links: When the nodes in the network move from their places and the topology is changed or the links in the active path are broken, the intermediate node that discovers this link breakage propagates an RERR packet. And the source node re-initializes the path discovery if it still desires the route. This ensures quick response to broken links [19].

Whenever an AODV router receives a request to send a message, it checks its routing table to see if a route exists. Each routing table entry consists of the following fields: Destination address, Next hop address, Destination sequence number, Hop count. Four types of messages used by the nodes in

the AODV 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[20].

2.1.6 Cross layer design

The design of efficient routing protocols is a critical issue for MANET having no fixed topology. Therefore, the source-initiated on demand routing protocol, which establishes the route between the source and the destination only when the source demands that, becomes the most popular routing protocol in the MANET. The layered concept (for example OSI) was primarily created for wired networks and naturally follows their architectural design. Designing wireless networks with strict layering principle did not fulfill the expectation raised in wire-line network design. The ad hoc mobile networks oppose strict layered protocol design because of their dynamic nature, infrastructure-less architecture, limited resources, mobility of nodes and time varying unstable links and topology[21].To improve different performance metrics, various cross-layering approaches are utilized where different OSI layer information are exchanged. AODV is a popular distance vector proactive routing algorithm. Investigate a modified version of AODV routing protocol, based on route discovery by utilizing cross layer information [22].

The concept of cross-layer design is based on architecture where the layers can exchange information in order to improve the overall network performances [23]. The basic purpose of cross layer design is to use multilayer parameters from OSI stack to increase the efficiency and performance of multi-hop wireless networks. Cross layer design approach can be used to improve the overall performance of multi-hop wireless networks such as wireless sensor networks (WSN), mobile ad hoc networks (MANET), and wireless mesh networks (WMN). The concept of

cross-layer design is based on architecture where the layers can exchange information in order to improve the overall network performance. It provides the inter layer communication between non-adjacent layers. Also helps in determining the behavior of other layers by retrieving and receiving the data from them. Hence there is a sharing of parameters, status and information among all the layers without any effect on the layer structures of the network. There are basically three issues being considered in cross layer design: Security, Quality of Service and Mobility. These three issues can also be viewed as the three major goals of cross layer design. To achieve this goal, sharing of data among the layers and exchanging of data among the nodes is required in cross layer design.

Classification of cross layer design:

According to the sharing of data inside one node can be classified into two categories:

a- Managerial method : that allows a vertical plane to act as a public library having all the required information that can be shared among the nodes and the other is.

b- non-manager method : in which one layer directly communicates with the other layer.

Another classification based upon the sharing of information among the nodes in a network:

a- centralized method :in which a central node is used to control the information sharing in cross layer.

b- distributed method :in this, the information is organized and shared without the use of a central node[24].

Goals Of Cross Layer Design

The goals of cross -layer designs are represented as a coordination model that accounts for the functions that the design may support. Figure 2.5 shows the coordination model, which shows the three major goals- QoS,

security and mobility. Normally, the aim of the cross- layer design is to achieve at the minimum, one of the three goals [25].

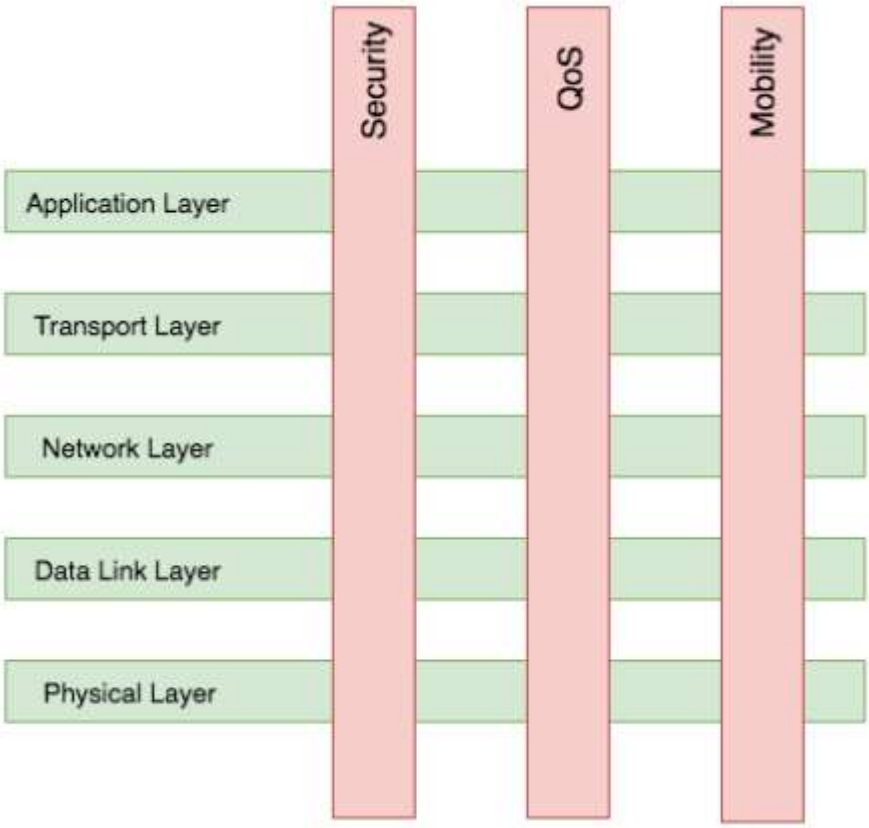

Fig 2.5Goals of Cross Layer Designs

a. Quality of Service (QoS)

The main aim of QoS coordination plane is to provide high quality of service in the wireless communication across five layers. In the wireless networks to get improved quality, upper layers must be aware of the information and characteristics of the two lower layers (physical layer and data link layer)[26] this direct sharing of information among the upper three layers and lower two layers is not possible in the traditional waterfall like concept of wireless network model. Hence, the QoS coordination plane helps in achieving the improved QoS communication in cross layer design.

b. Mobility

This coordination plane helps in guarantying an uninterrupted communication in wireless networks. Nodes in wireless sensor network can be stable or mobile in nature [27] for the mobile nodes, the events like channel switch or route change must be discovered and solved to get uninterrupted communication throughout the session.

c. Security

The security coordination plane implements the protocols that are concerned with the security issues among the five layers of TCP/IP protocols. Various security methods like Wi-Fi protected access must be deployed to perform secured communication across the cross layered design. It might be deployed at application layer like end to end security, at network layer and/or data link layer and physical layer to help perform secure communication in cross layer design [28].

Cross layer Implementation At TCP/IP

Mostly applications are dependent on TCP for communication. In TCP/IP protocol there are five layers. Each layer cooperates with the layer above it and layer below it. Because of Transmission Control Protocol (TCP) of transport layer and Internet Protocol (IP) of Network layer, TCP/IP model is most desirable for quick and efficient communication; TCP/IP model consists of five layers the functions of each layer.

i. Physical Layer

This layer focuses on physical devices and transmission media. It provides multiple antenna gains and improves integrity and throughput of data transmissions. This is the layer responsible for coding and modulation implementations. Also, it adjusts the transmitting power and controls the effects of mobility and propagation effects.

ii. Data Link Layer

It is the media access layer, helps in error recovery, manages retransmissions and queuing of packets. It is further divided into two sub layers: Medium Access Control (MAC) sub-layer and Logical Link Control (LLC) sub-layer.

iii. Network Layer

The main responsibilities of this layer are to discover the neighbors, routing and allocate resource functions. The main part is routing in which it guides the packet in the network from source to destination [29] there are multiple routing protocols designed to satisfy the requirements of Wireless networks. These protocols can predetermine the performance on the bases of packet loss ratio, end to end delay and network throughput.

iv. Transport Layer

The main function of this layer is to control congestion, do error recovery, flow control, packet sequencing (reordering) and end-to-end connection setup. It also helps the application layer in mapping and allocating the flow to routes which are found at network layer.

v. Application Layer

This layer acts as an interface between the end user and the TCP/IP model. It considers the requirements of the end users and divides the services into multiple categories like real time services or non-real time services, multimedia services etc.

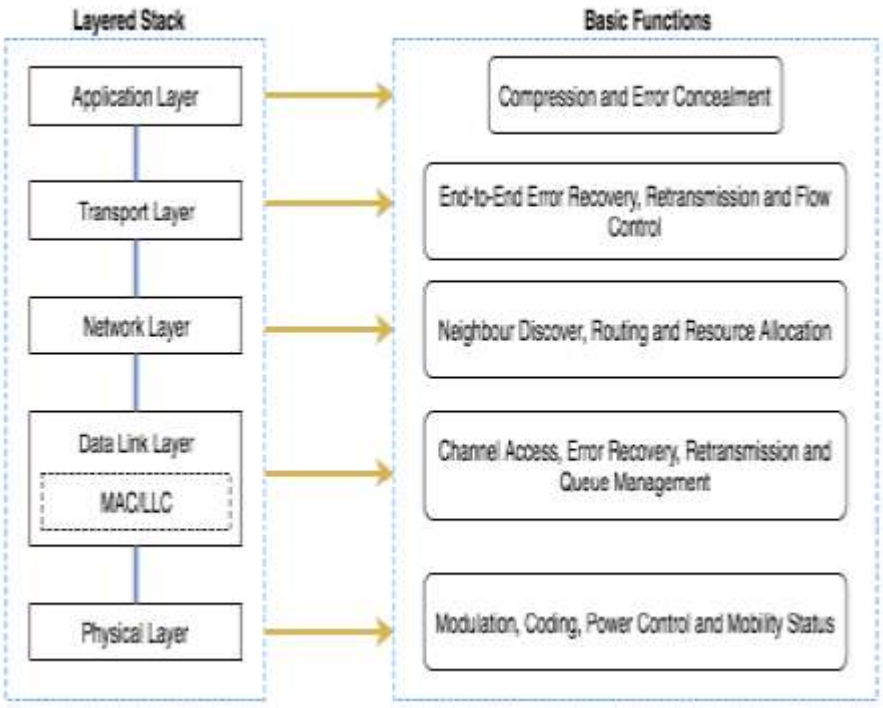

Fig2.6 Layered Stack and main functions of each layer[30][31]

Multi-hop wireless networks are more vulnerable to different security risks due to inherent attack prone features such as shared MAC, multi-hop decentralized architecture, wireless medium etc. The attackers can exploit these features to bring serious disorders and routing disruption. Furthermore, multi-hop wireless networks are exposed to multi-layer threats. A security mechanism for one layer cannot protect the other layer. Hence cross layer security mechanisms are indeed necessary to protect these multi-hop wireless networks from passive, active and denial of service attacks.

In [32], cross layer architecture is proposed with different parameters at different layers. More optimized algorithms can be design by allowing MAC layers to provide information to Network layer regarding: In MAC layer, some information can be analyzed such as contention, fairness, scheduling, and Network layer facilitate in optimal path selection based on information received from and MAC layer [33].

2.1.7 Security in MANET Routing:

Multi-hop wireless networks are more vulnerable to different security risks due to inherent attack prone features such as shared MAC, multi-hop decentralized architecture, wireless medium etc. The attackers can exploit these features to bring serious disorders and routing disruption. Furthermore, multi-hop wireless networks are exposed to multi-layer threats. A security mechanism for one layer cannot protect the other layer. Hence cross layer security mechanisms are indeed necessary to protect these multi-hop wireless networks from passive, active and denial of service attacks.

Cross layer architecture is proposed with different parameters at different layers. More optimized algorithms can be design by allowing MAC layers to provide information to Network layer regarding: In MAC layer, some information can be analyzed such as contention, fairness, scheduling, Network layer facilitate in optimal path selection based on information received from and MAC layer [34].Security in MANET is a major problem as to provide secure communication between the nodes in the infrastructure less wireless network. As ad hoc network is self-configuring, open radio communication link between node to node, frequent changeable physical topology, and modified assets. Following qualities describes secure network:

1. **Confidentiality**

To keep the information secret from the unknown users. It maintains the information safe and secure from the attacks.

2. **Integrity of Message**

To keep the accuracy and consistency of the data during its transit from one node to another node. So, that the data is not restricted by the node.

3. Availability of Nodes

As in MANET for communication the nodes are required to be available all the time so that the information can be relayed over such path.

4. Authorization

It specifies the permissions of the entity to take part in the communication over network [35].

2.2 Related Works

The authors of [36] proposed the TID mechanism over the AODV MANET routing protocol. The TID mechanism performs its intrusion detection mechanism locally in the previous node of the attacker node in contrast with the RID mechanism, which performs its intrusion detection mechanism by means of the source node. As a piece of future work, we will perform more enhanced intrusion detection mechanism that could perfectly detect a group attack if applied on the MANET. Subsequently, the new enhanced security mechanism will be evaluated using the same performance metrics and simulation parameters.

To keep the information secret from the unknown users. It maintains the information safe and secure from the attacks

The authors of [37] proposed a new secure routing protocol SE-AODV is proposed which adds extra features to same AODV routing protocol making path formation more secure. Malicious node in network tries to disrupt the path formation by various attacks and degrade the network performance. We followed evaluation of proposed algorithm performance by comparing it to SAODV and addressing the loopholes in SAODV and how proposed secure protocol overcomes it with Minimum overhead Maximum security.

The proposed scheme covered many attacks but for further giving more advance shape to this work an intrusion detection system for MANET can be designed which can focus on NODE_LIST field of control packet, a

trackback IP approach can be designed which can policy drive malicious node for further connection in network. As this approach can detect nodes increasing hop count, malicious node can be detected which don't want to come in path for other's connection, an intrusion system can isolate these nodes from network and increase of the network performance. As in MANET for communication the nodes are required to be available all the time so that the information can be relayed over such path.

Mahesh K. Marina and Samir R. Das in [38] contemplate, an on-demand, multipath distance vector protocol AOMDV that extends the single path AODV protocol to compute multiple paths. There are two main contributions of this work:

1. Use the notion of an advertised hop count to maintain multiple loop-free paths at each node.

2. Show how route discovery mechanism in the AODV protocol can be modified to obtain link-disjoint multiple paths from source and intermediate nodes to the destination. Currently working on augmenting the AOMDV protocol with a technique to uniquely identify each disjoins tpath on an end-to-end basis. This feature is very useful when it is necessary to route always along one specific path. For example, TCP retransmission timeout computation is sensitive to message reordering which can be avoided by always following the same end-to-end path as long as it is available. We will also look into other issues related to on demand multipath routing — for example, the availability of multiple paths in relationship with node density and load balancing with multiple paths.

The authors of [39] proposed , the performance analysis is carried out on Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) and Destination Sequenced Distance Vector (DSDV) protocols using NS2 simulator the interest in ad hoc networks has grown due to the availability of wireless communication

devices that work in the ISM bands. While designing an ad hoc network in particular we are concerned with the capabilities and limitations that the physical layer imposes on the network performance. Since in wireless networks the radio communication links are unreliable so it is desirable to come up with an integrated design comprising of physical, MAC and network layers. The main vision of MANET is to support robust and efficient operation in wireless networks by incorporating routing functionalities at each mobile node. For such designing aspects of ad hoc networks Routing-based approach, Information-theoretic approach, Dynamic control approach or Game-theoretic approach has been implemented.

In future, utilizing these performances we can design such a protocol that can be suitably provide data integrity as well as data delivery in highly random mobility network. Our focus is to analyze the energy metrics as the cost function for routing in these protocols for better QoS applications.

The authors of [40] show the routing security in wireless networks appears to be a nontrivial problem that cannot easily be solved. It is impossible to find a general idea that can work efficiently against all kinds of attacks, since every attack has its own distinct characteristics. In this article we study the routing security issues of MANET, analyze one type of attack, the black hole, that can easily be deployed against a MANET, and propose a feasible solution for it in the AODV protocol. One limitation of the proposed method is that it works based on an assumption that malicious nodes do not work as a group, although this may happen in a real situation. We are currently looking at this problem of team attacks.

The authors of [41] proposed the performance of Ad-hoc On Demand Vector (AODV) protocols modified by including the source route accumulation feature. As low transmission power of each ad-hoc node limits its communication range, the nodes must assist and trust each other

in forwarding packets from one node to another. However, this implied trust relationship can be threatened by malicious nodes that may modify or disrupt the orderly exchange of packets. Security demands that all packets be authenticated before being used. Based on this trust model, we design trusted routing protocols using trusted frame works and intrusion detection system (secure protocol) for MANET.

TAODV still has some imperfect points. For example, it cannot synchronize the trust level settings on different nodes when multiple paths cross with each other, in which case some node's access violation ratio is not 0. As a future work, we will focus on designing the synchronization control mechanism to solve this problem. A public key verification mechanism, such as certificate-based authentication, is needed for improvement of TAODV, in order to verify the binding between the node's identity and its public key.

CHAPTER THREE

Improving AODV Using Cross Layer Design

CHAPTER THREE

Improving AODV Using Cross Layer Design

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. AODV is a reactive protocol: the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node: a routing-entry not recently used is expired. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is uni-casted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors. Each routing table entry contains the following information [2] as destination, next hop, number of hops, destination sequence number, and active neighbors for this route.

3.1 AODV Routing protocol:

3.1.1 Control messages

a- Routing request

When a route is not available for the destination, a route request packet (RREQ) is flooded throughout the network. The RREQ contains the following fields [3]:

Table 3.1: Routing request

Source address	Request ID	Source Sequence No.	Destination Address	destination sequence No.	Hop count

-Routing reply b

If a node is the destination, or has a valid route to the destination, it uni-cast a route reply message (RREP) back to the source. This message has the following format

Table 3.2: Routing reply

Source Address	destination Address	destination Sequence No.	hop count	life-Time

The reason one can uni-cast RREP back is that every node forwarding a RREQ message caches a route back to the source node.

c- Route error

All nodes monitor their own neighbor-hood. When a node in active route gets lost, a route error message (RERR) is generated to notify the other nodes on both sides of the link of the loss of this link.

3.1.2 HELLO messages

Each node can get to know its neighbor-hood by using local broadcasts, so-called HELLO messages. Nodes neighbors are all the nodes that it can directly communicate with. Al-though AODV is a reactive protocol it uses these periodic HELLO messages to inform the neighbors that the link is still alive. The HELLO messages will never be forwarded because they are broadcasted with TTL = 1 When a node receives a HELLO message it refreshes the corresponding lifetime of the neighbor information in the routing table.

3.2 Cross-layer metrics

To improve different performance metrics, various cross-layering approaches are utilized where different OSI layer information is exchanged. AODV is a popular distance vector proactive routing algorithm. In our research we investigate a modified version of AODV routing protocol, based on route discovery by utilizing Physical Layer information instead of the minimum hop count approach of the default distance vector algorithm.

The research also elaborates how the proposed model uses the received SNR to find its route. In this subsection, cross-layer metrics used in the proposed algorithm are defined.

In this work, the MAC and routing layer layers are considered. In order to improve security, these two layers are considered with minimum features.

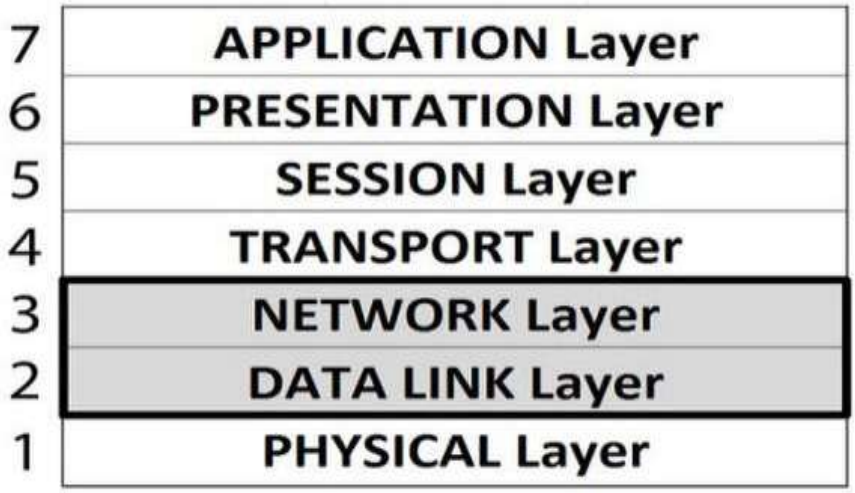

Figure 3.1 Cross layer design

More optimized algorithms can be design by allowing MAC layers to provide information to Network layer regarding:

In MAC layer, some information can be analyzed such as contention, fairness, scheduling, Network layer facilitate in optimal path selection

based on information received from and MAC layer. The most important information or feedback in our research to improve the security and get rid of malicious nodes, the number of requests sent from the nodes is shown to indicate whether the node is malicious or not.

The malicious nodes exploit the advantage of the short path in AODV routing protocol to continuously broadcast themselves in the network which sends a very large number of requests to weaken and destroy the network.

The cross layer design is used to determine the number of requests for the nodes and compare them with the rest of the other nodes and send the information to the network, to know if the track has malicious nodes or not to detect them and tack the best route to send and clean the network from all malicious nodes thus maintain the security of the network and improve some of performance measures.

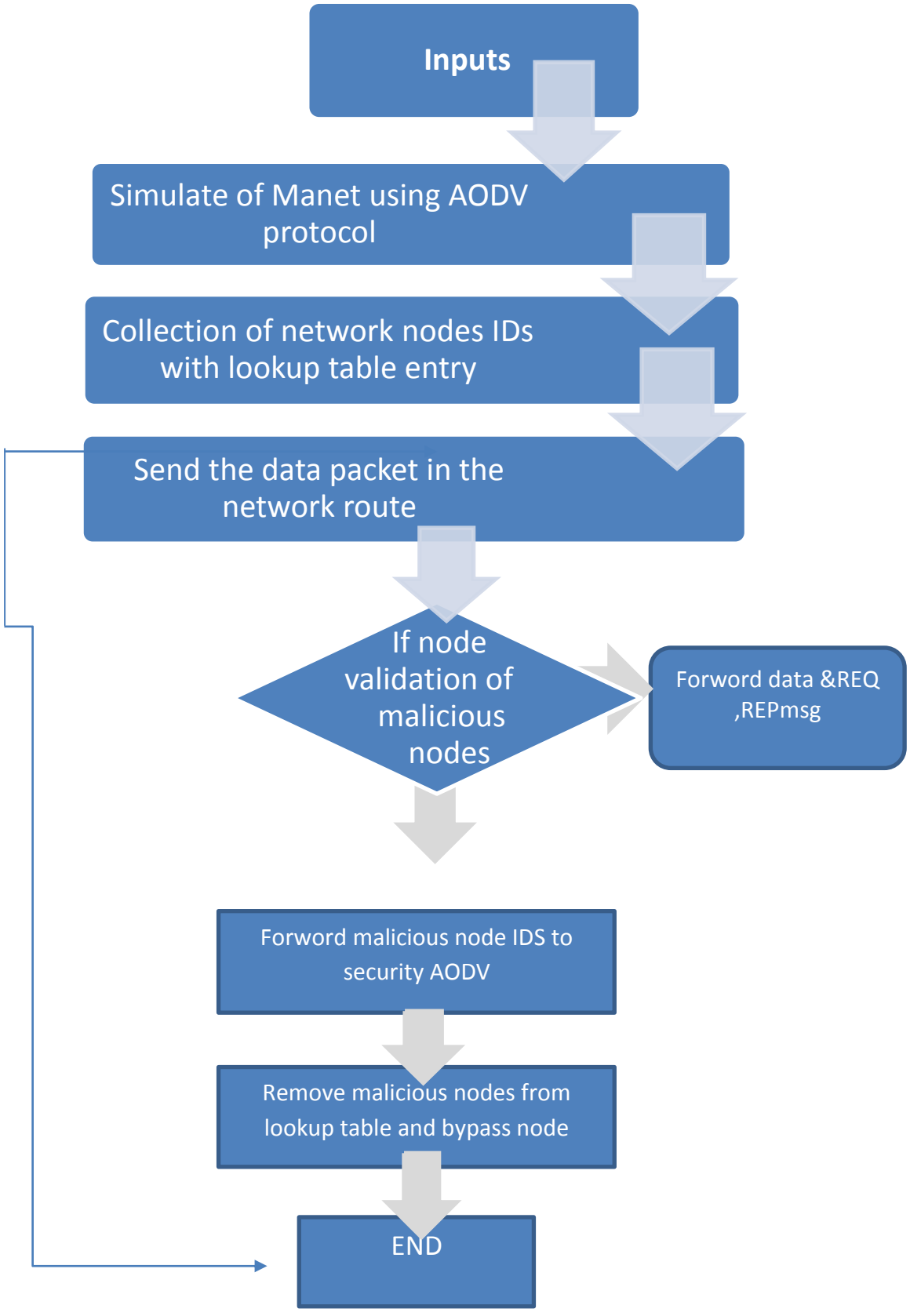

Figure 3.2: AODV Enhanced Routing Protocol

step1: After the implementation of the Manet system network to send data between nodes and use AODV routing protocol ,the record of each node and the details of the data are verified to find out the statistics related to the number of packets, data received and send etc…

step2: When the data packet is available in the network, the MAC listen to the data packet and inform the network layer of the data

packet that is modifying the information in the AODV

step3: The malicious node that attacks all data packets for another nodes, thus cannot receive data between them .

Step4: The advantage of this feature is in the statistics of AODV that can be used to detect the harmful behavior of the node

Step5: If a node only receives data packets and does not forward them, it may be the malicious node

Step6: The system used to delete the malicious node IDs From the table and notify the rest of the nodes to resent the data packet in a clean path.

3.3 AODV Vs Enhanced AODV By Cross Layer Design

AODV:

- In MANET, the network layer finds the path for transmission of data bits and the data link layer manages the state of data transmission. Here both the layers don't depend on each other for their function which results in wastage of resources.

- The route maintenance overhead in AODV increases as the network mobility is high and the topology changes frequently

- The established routes are to be changed as the nodes move away; it results in low performance as many packets are dropped when some active route on the path move away significantly.

Malicious nodes can unchanged the hop count and forward the packet that will also contribute in path attraction for destination as it could have a low hop count path.

EAODV:

-To improve point one in AODV, cross layer functionality comes to rescue which improves the utility rate of resources.

- The cross layer interact with data link layer to obtain the performance data of link. Path hop count and link data are used to select the route. In , a judgment for the service flow to choose the best path, which improves the accuracy of the routing selection and the quality of services.

- The Mac layer calculates the number of requests sent from the nodes and informs network layer to know if the track has malicious nodes or not to detect them and tack the best route to send and clean the network from all malicious nodes thus maintain the security of the network and improve some of performance measures.

-The malicious node is identified and removed immediately and its performance results are indicated better.

3.4 AODV performance metrics :

3.4.1 Throughput

Throughput is the average rate of successful message delivery over a communication channel or it is a measure of how fast we can actually send data through a network.

The Throughput formula is in Equation (3.1):

$$Throughput = \frac{Totalresivepacket * packetsize * 8}{simulationtimeinsec} \quad (3.1)$$

3.4.2End to End Delay

It is the time taken for an entire message to completely arrive at the destination from the source. Evaluation of end-to-end delay mostly depends on the following components.

The End to end delay formula is in Equation (3.2):

$$Nd = Td + Rd + Pd \quad (3.2)$$

Nd : Node Delay Time ms, Td : Transmission Delay Time in ms, Rd : Receiving Delay Time in ms, Pd : Processing Delay time in ms.

3.4.3 Bit Rate

The number of bits that are processed per unit of time, in another words, it measure how much data is transmitted in a given amount of time.

the bit rate formula is in Equation (3.3)

$$Bitrate = \frac{packetsize}{simulationTime} \quad (3.3)$$

3.4.4 Packet Delivery Ratio (PDR)

It is the ratio of the total data bits received to total data bits sent from source to destination .

The packet delivery ratio formula is in Equation (3.4):

$$PDR = \frac{numberofsuccessfulreceivedpackets}{totalpacketssendfromthesource} \quad (3.4)$$

3.5 Simulation scenario

The proposed EN-AODV protocol's performance is analyzed using mat-lab simulator. The simulator is applied with traditional (normal) AODV and with proposed enhanced algorithm based EN-AODV by Various cross-layering approaches are utilized to improve the performance of MANETs and their associated routing protocols. Our research investigated a modified version of AODV routing protocol utilizing Mac Layer in-formations send to network layer to determine the shortest and optimal path, and results are

obtained for assessment. The network is planned and implemented using network simulator with number of nodes from 200 to 600, that are initially placed randomly and are free to move anywhere within its area.

The lookup table is then created where the number of request , ID for each node, and the distance between any node and nodes around it, we do a request from source to destination and often go through most nodes in the network, after that, the shortest path is found from source to destination , in case of the enhanced algorithm ,the malicious nodes are defined by the number of request; if its value is too large to be greater than a specific value, the node is immediately classified as a malicious node, the malicious nodes is removed and the path continues until it reaches the destination. All variables are then calculated according to the following: the distance between the contracts, the number of malicious contracts, delay in each node and the results are finally extracted. The proposed EN-AODV protocol has shown good progress over the security parameters like PDR, Delay, bit rate and throughput is maintained. PDR, bit rate, throughput is increased and delay is reduced compared to the traditional AODV. The performance of the proposed protocol is also represented graphically where it clearly shows the betterment of the parameters. And the various in the number of malicious nodes are also shown.

3.6Simulation Construction

The code for the AODV has written in mat-lab code, where attached in the APPENDX. For the performance metrics improvements evaluation of the system the results of the algorithm represented in Chapter 4.

CHAPTER FOUR

Results and Discussion

CHAPTER FOUR

Results and Discussion

In the previous chapters the explanation of how the Enhanced AODV work has been expanded, so in this Chapter the simulation results for the actual process of the AODV, AODV enhanced by cross layer performance metrics and the evaluation of the system performance will be discussed, which investigates the effect of cross layer design performance for security in AODV.

4.1 Simulation the Improvement of the AODV routing protocol Performance Metrics:

In this section, the simulation results for the AODV routing protocol performance metrics improvement are represented. By compare normal Ado with an enhanced Ado routing protocol by cross layer design system from performance point of view.

Figures 4.1 &Figure 4.2 illustrates the number of malicious nodes in a network as a simulation results, for two difference number of malicious nodes, and how the this value affected to other values.

Figure 4.1 illustrate network in blue color use enhanced AODV after remove malicious node all the values is zero, and in red color use normal AODV with maximum number of malicious nodes equal30.

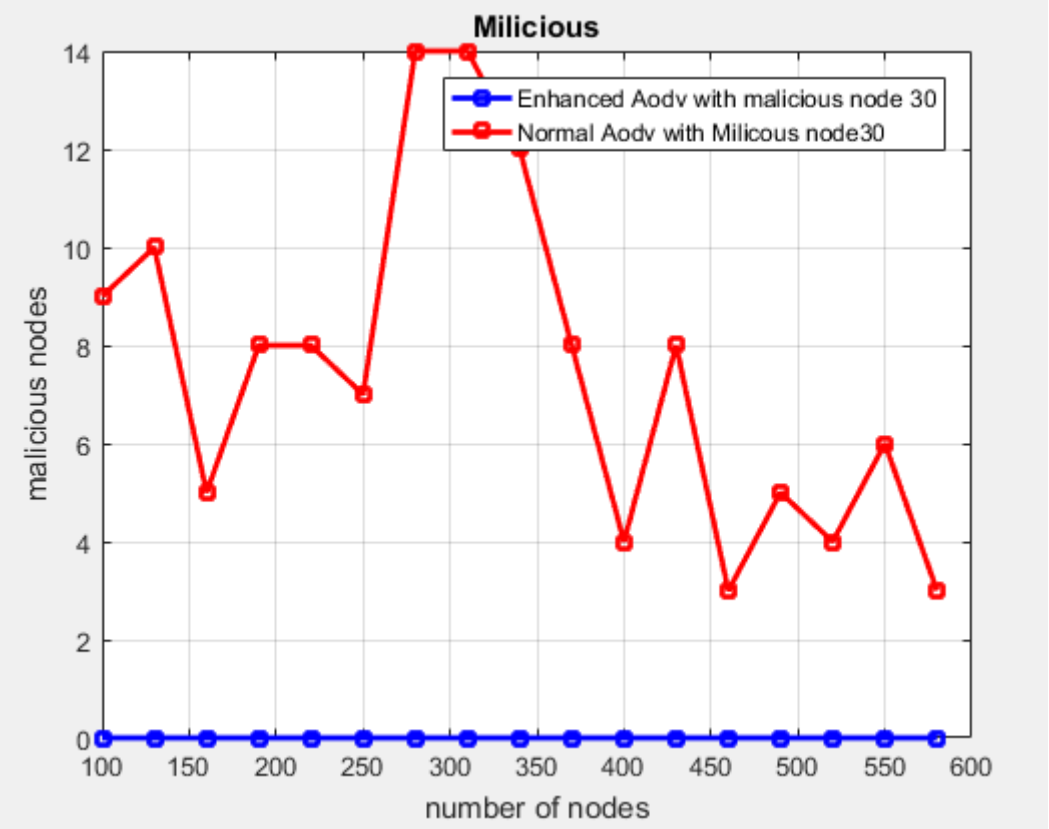

Figure 4.1 Comparison of number of active malicious nodes for normal AODV and Enhanced AODV with number of malicious nodes (30)

Figure 4.2 illustrate network in blue color use enhanced AODV after remove malicious node all the values is zero, and in red color use normal AODV with maximum number of malicious nodes equal 90.

Compare to the first drawing with a lower number of malicious nodes, we notice in this network when increase the maximum number of malicious nodes, the number of malicious nodes that appear over the network is larger, And the negative impact on the performance metrics will be larger .

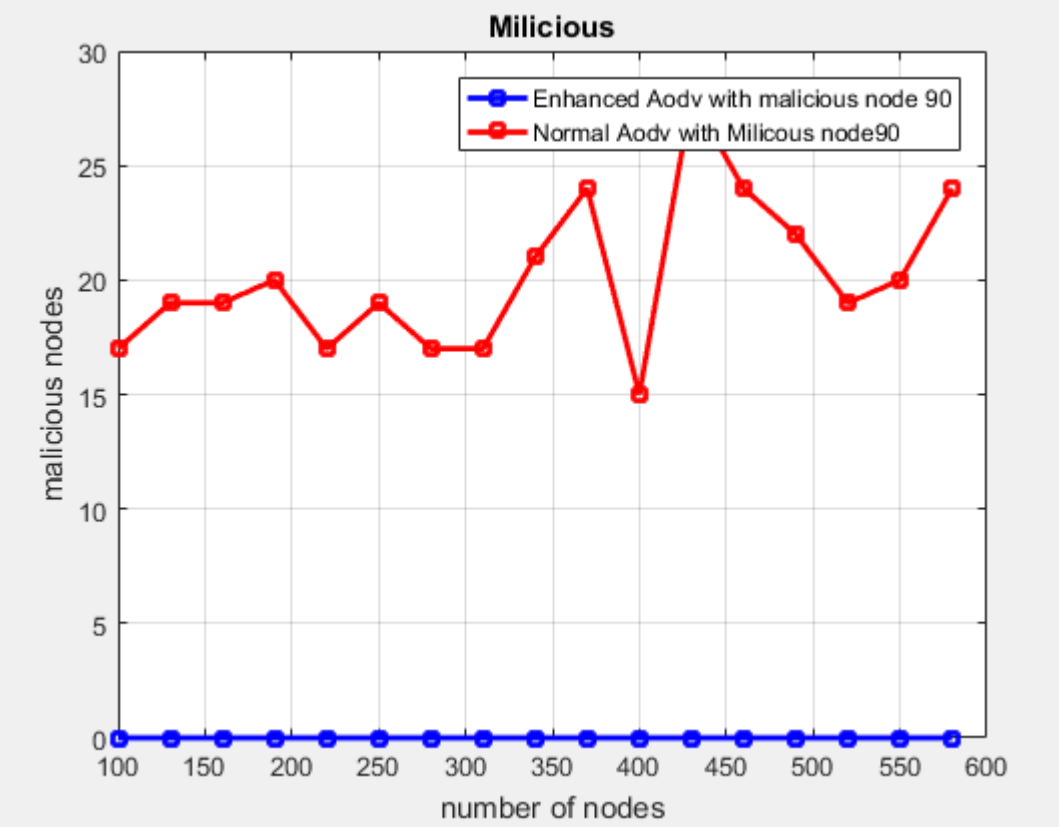

Figure 4.2 Comparison of number of active malicious nodes for normal AODV and Enhanced AODV with max number of malicious nodes (90)

4.1.1 **System Throughput Enhancement**

Equation (3.1) describe the Throughput is the average rate of successful message delivery over a communication channel or it is a measure of how fast we can actually send data through a network over the total simulation time.

How efficient the throughput is used is illustrated in Figure 4.3, Figure 4.4 show two networks use AODV algorithm with different number of malicious nodes, that proportional to the throughput showed in Figure 4.3 which is consist on the used 30 maximum number of malicious nodes in the network ,network in red color use enhanced AODV after remove malicious node the values of the throughput is more increase than that network that use normal AODV algorithm.

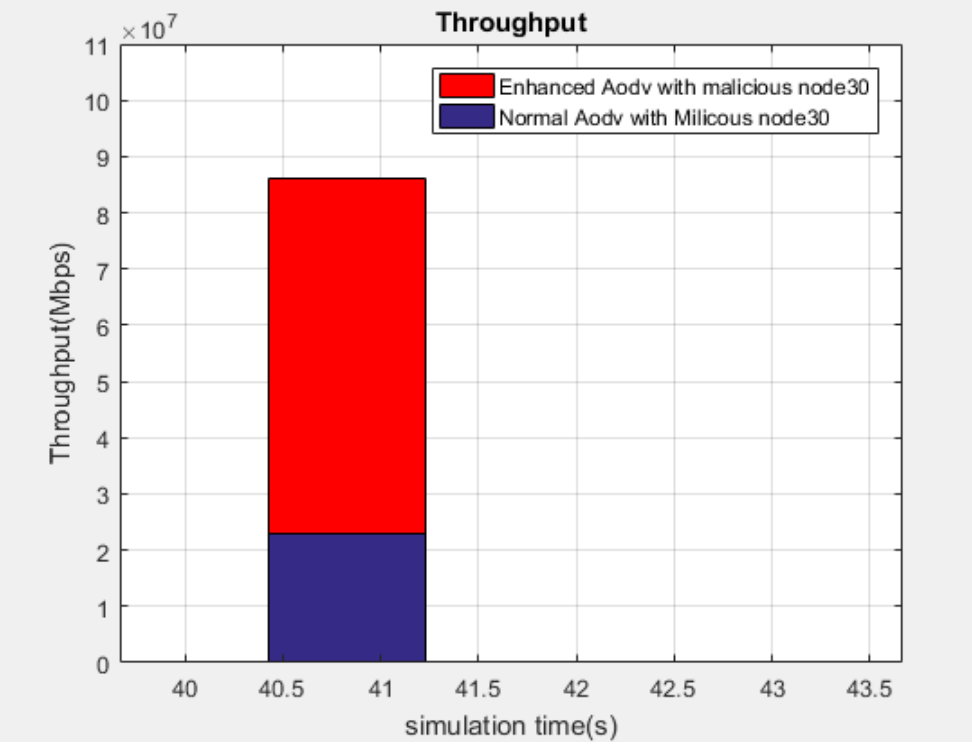

Figure 4.3 Comparison of Throughput of normal AODV with Enhanced AODV with max number of malicious nodes (30)

In Figure 4.4 the throughputs for the same network in an enhanced AODV system with red color is also more increase than the normal AODV with blue color, but when increase the number of malicious nodes to 90.its more less than enhanced one in the figure 4.3. That is, the higher number of malicious nodes, the value of throughput is significantly reduced for both different systems in the network. Because the network when sending the packet through the malicious nodes then it selectivity drop the packets and average rate of successful message delivery over a communication channel will be decrease.

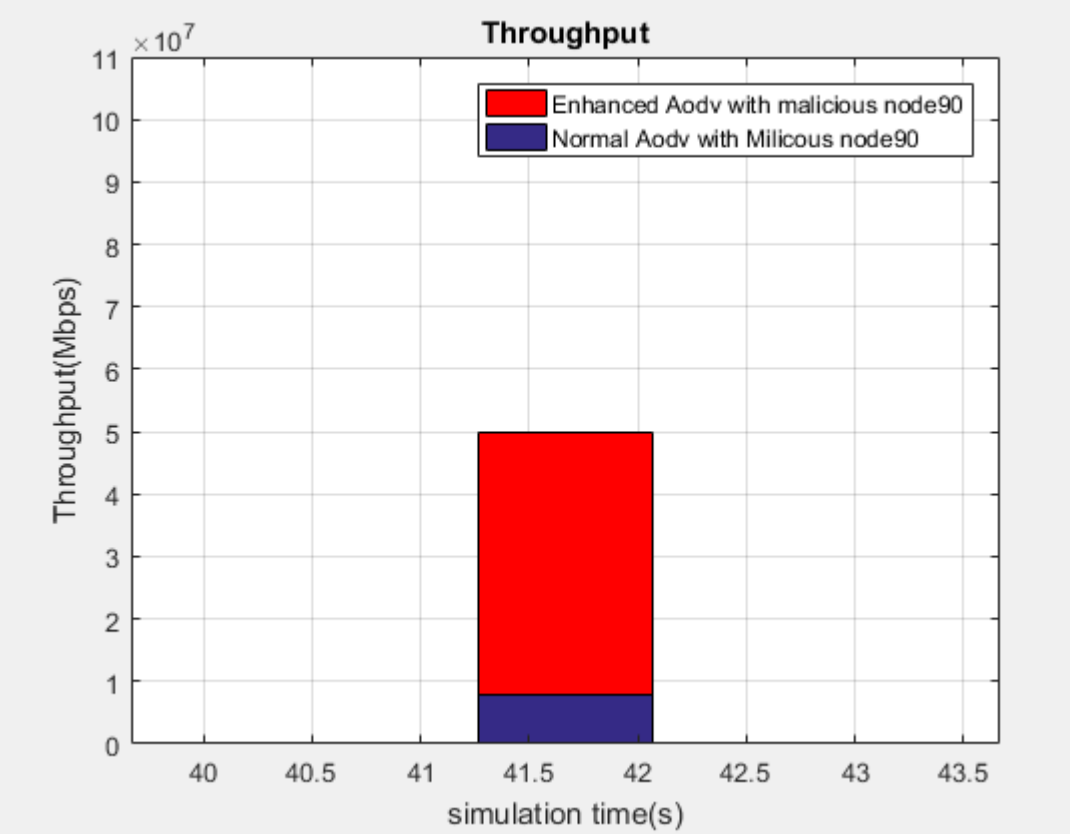

Figure 4.4 Comparison of Throughput of normal AODV with

Enhanced AODV with max number of malicious nodes (90)

4.1.2 Improvement of bit rate of the System

The number of bits sends each second is the system bit rate, which is depend on the total packet received and simulation time .

Figures 4.5 &Figure 4.6 illustrates the bit rate values as a simulation results, for[network] have used two difference maximum number of malicious nodes, and how the variety of the number of malicious affects in this values.

Figure 4.5 illustrate network in blue color use enhanced AODV after remove malicious node and in red color use normal AODV with maximum 30 number of malicious nodes , each network have almost decrease a bit rate with increase the number of nodes.

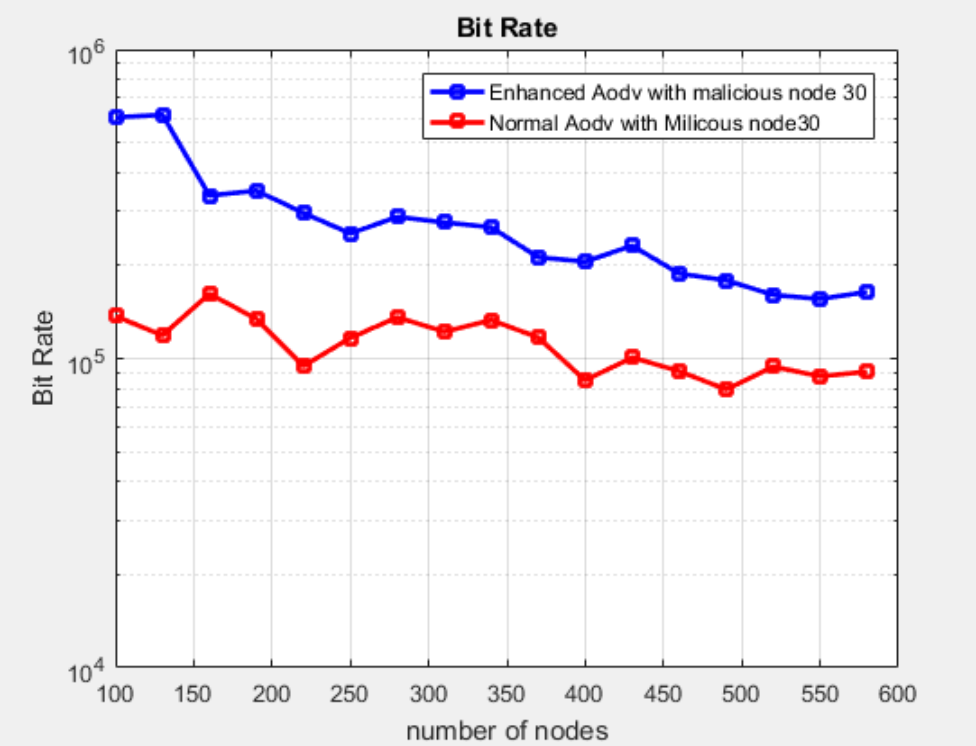

Figure 4.5 Comparison of bit rate of normal AODV with Enhanced AODV with max number of malicious nodes (30)

Figure 4.6 illustrate the same network with the different number of malicious nodes (60), in case of enhanced AODV shown in blue color, the values of bit rate are affected by increase the number of malicious nodes and it will be decrease. In case of normal AODV shown in red color we notice that by increasing the number of malicious nodes, the value of bit rate is significantly reduced.

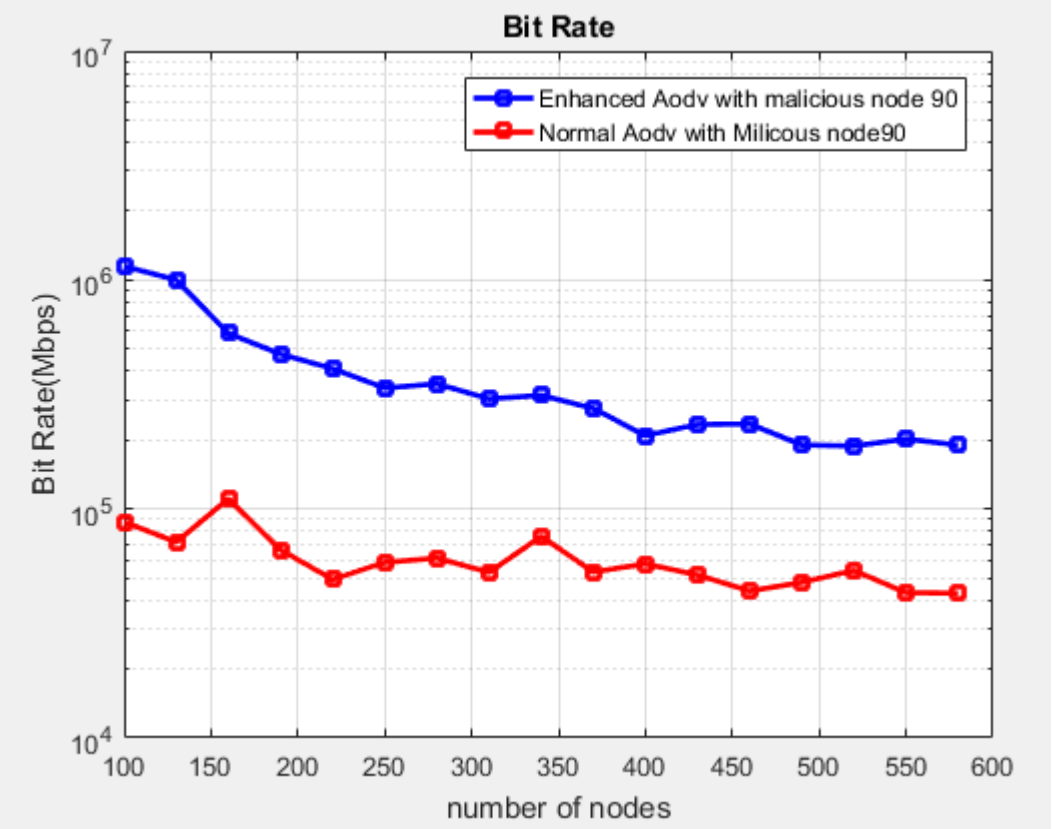

Figure 4.6 Comparison of bi trate of normal AODV with

Enhanced AODV with max number of malicious nodes (90)

4.1.3 Packet ratio enhancement

According to these values the packet ratio calculated using Equation (3.4), in the evolution of AODV networks performance metrics the packet ratio is the ratio of the total data bits received to total data bits sent from source to destination .

Which shows a huge difference between network in system use enhanced AODV and network in system use normal AODV with number of malicious node equal 30 as showing in Figure (4.7) .The enhanced AODV illustrated in a blue color and the normal AODV in red color, All packet ratio values can be observed decrease with increase the number of nodes in the network, but the network in system use normal AODV is more

decrease than enhanced one, which cause degradation in the system performance.

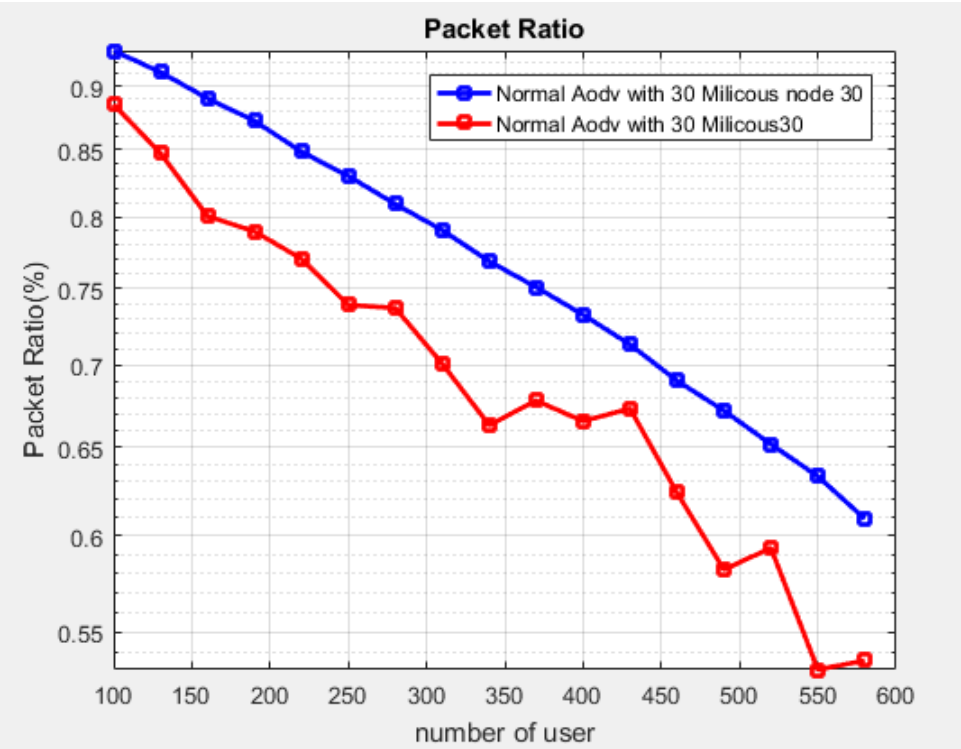

Figure 4.7 Comparison of packet delivery ratio of normal AODV with Enhanced AODV with max number of malicious nodes (30)

As shown in the figure (4.8), when the number of malicious nodes is increased, the values of packet ratio are significantly reduced, because the malicious nodes block the packet reception and increase the amount of losses in the network, thus reducing the packet receiving rate much less than packet sending.

The network that uses the normal AODV system with number of malicious nodes (90) reduces the packet ratio larger than the normal AODV network which has 30 malicious nodes. That the optimization system shown in blue color is not affected by malicious nodes after they have been detected and removed. Which improves the performance of the system 10 % compared to the normal AODV.

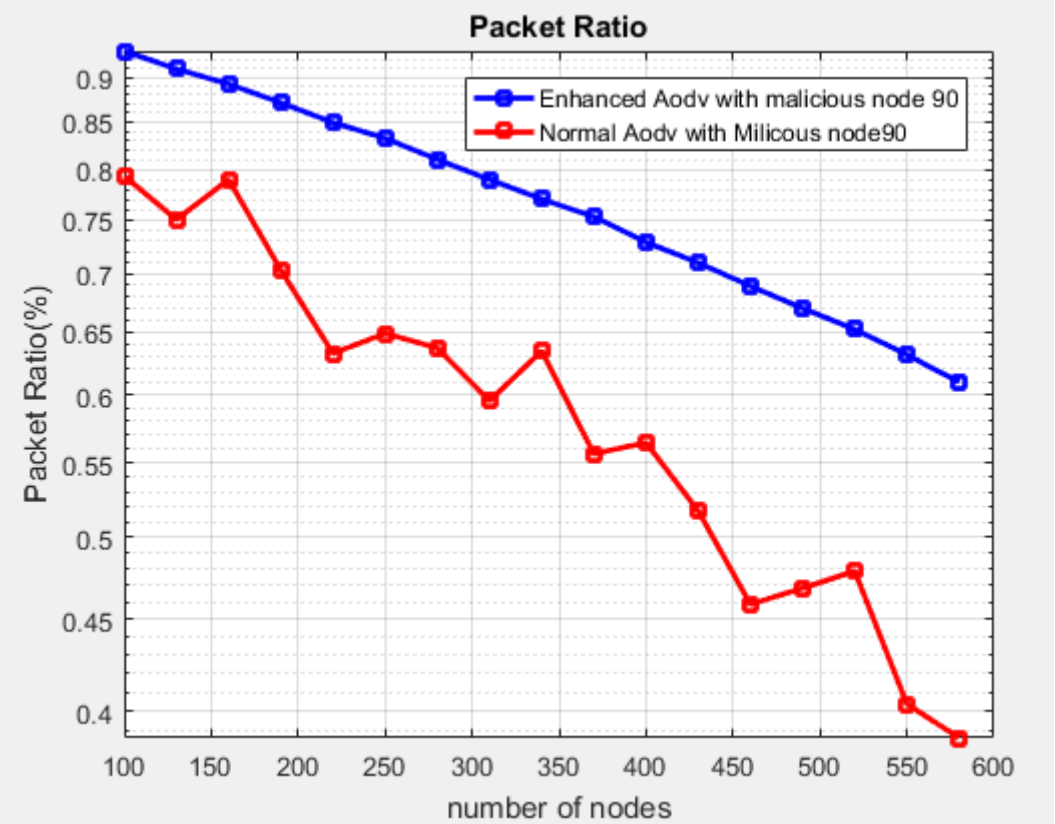

Figure 4.8 Comparison of packet delivery ratio of normal AODV with Enhanced AODV with max number of malicious nodes (90)

4.1.4 Corresponding End to end delay Increasing

The time taken for an entire message to completely arrive at the destination from the source called end to end delay.

Figures 4.9 illustrates the end to end delay values as a simulation results, for two different systems, and how the variety of the number of malicious nodes affects in this values.

Figure 4.9 illustrate network use enhanced AODV system in blue color use (30 maximum number of Malicious nodes) and same network use normal AODV in red color with (30 malicious nodes), each system have increase in end to end delay, but the normal AODV in red color has more increase in end to end delay than the enhanced AODV in blue color.

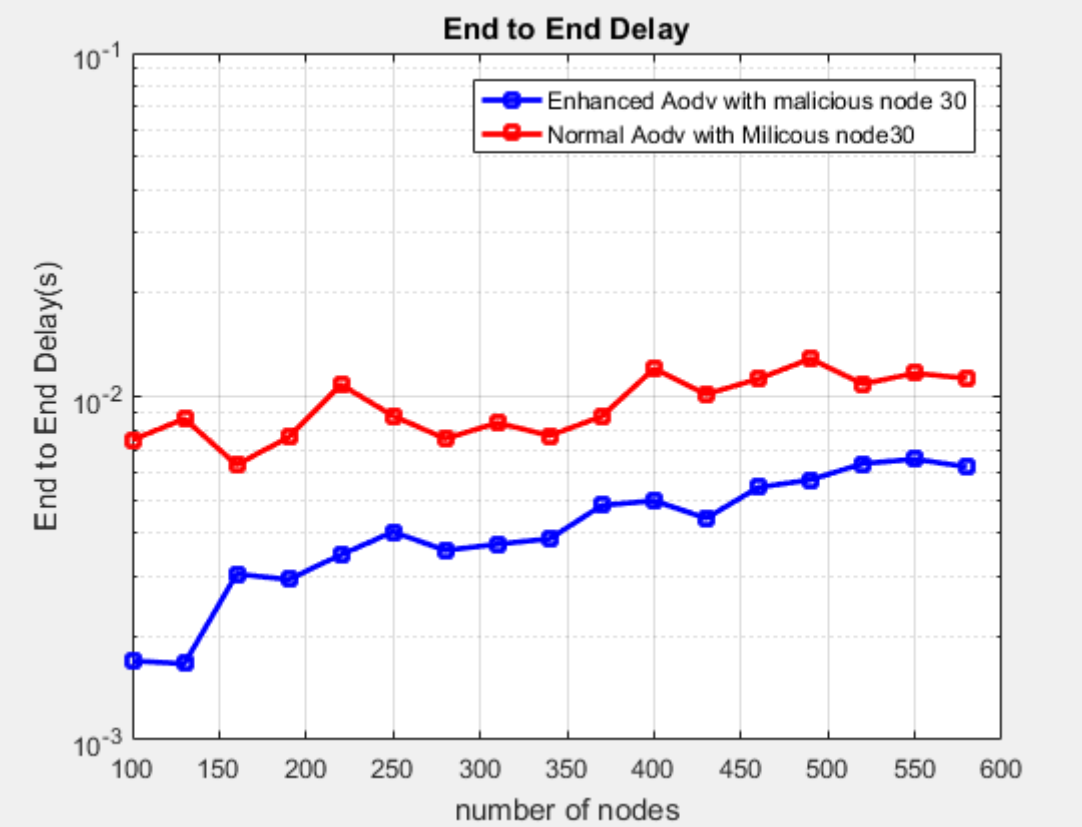

Figure 4.9 Comparison of end to end delay t of normal AODV with Enhanced AODV with max number of malicious nodes (30)

on the contrary, Figure 4.10 illustrate the same network with maximum number of malicious node equal (90), we observation the network uses enhanced AODV with blue color not affected by increase the number of malicious nodes, compared to network use normal AODV with the number of malicious nodes equal 90, the end to end delay more increase from network with the number of malicious nodes equal 30.

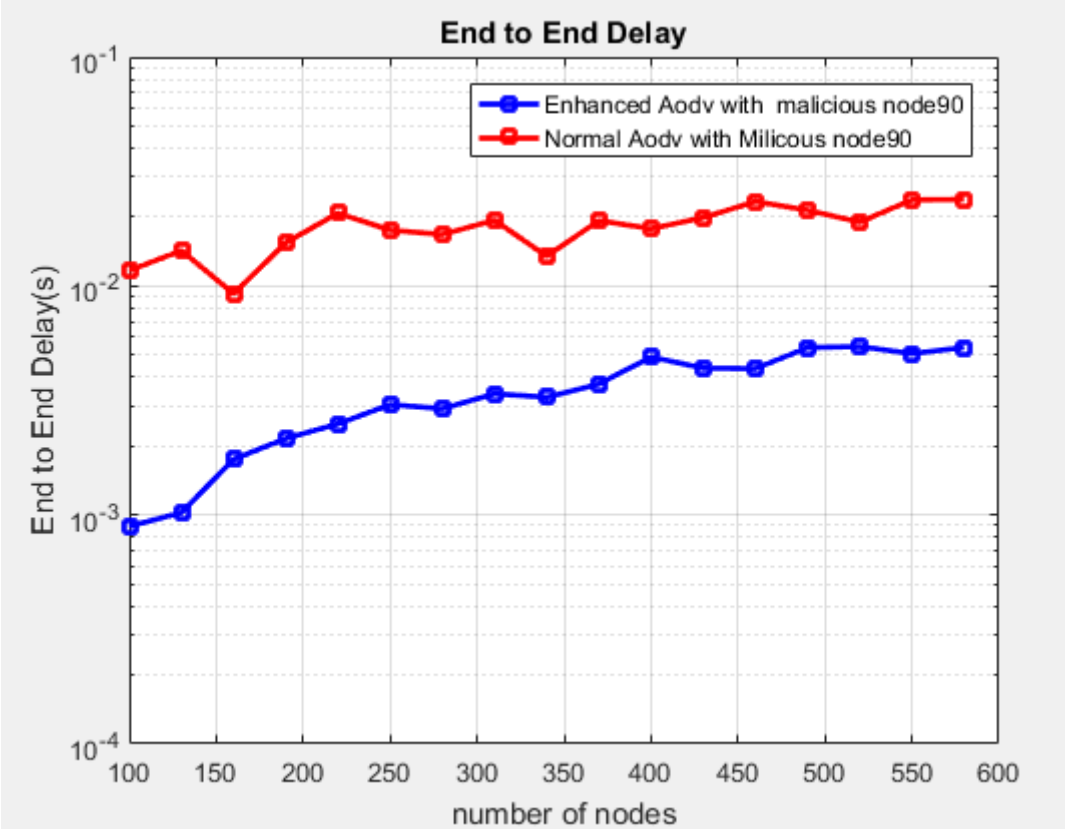

Figure 4.10 Comparison of end to end delay of normal AODV with Enhanced AODV with max number of malicious nodes (90)

:Noticeable

.The simulate results look like comparative study (Aodv Vs EN.Aodv)

.Pseudo code is attached in the last chapter

Table 4.1 Compression between Two networks for Different Systems

Enhanced AODV	Normal AODV	Performance metrics
7.9140	1.1238	Throughput(Mbps)
6.2595	1.3447	bit rate(Mbps)
0.0016	0.0076	End to end delay (sec)
0.9313	0.8463	Packet delivery ratio(%)

CHAPTER FIVE

Conclusion and Recommendations

CHAPTER FIVE

Conclusion and Recommendations

5.1 Conclusion

A wireless MANET presents a greater security problem than conventional wired and wireless networks due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities; Routing security plays an important role in the security of the entire network. routing security is possible to find an idea that can work efficiently against all kinds of attacks, As in normal AODV a malicious node can come in path and our approach proves to be more secure as it provide an alternate malicious free path to source, and propose a feasible solution for it in the AODV protocol, This research illustrates methods, algorithms and techniques used to improve security in AODV protocol. It also gives information about different cross-layering techniques that are used in which different layers from protocol stack communications with each other via exchange of information. Enhanced AODV increase security based on cross layer design has a problem in end to end delay taken for deliver the packet. Compare with normal AODV provide end to end delay without any security. The total performance improvement gained when cross layer design is used. In which, the end to end delay which has average of values equal 7.9140 the overall improvement increasing in the bit rate and Packet delivery ratio, and Throughput with average of values are 6.2595, 0.0016, 0.9313 respectively. From above graph in malicious scenario it can be easily conclude that when there is increase of malicious node in any scenario proposed SE enhanced-AODV proves to be more secure with that delivering a high throughput, PDR and high number of receive packets as compared to normal AODV.

5.2 Recommendations

Cross layer design consider a modern technique in the communication system and Ad hoc networks, but it's Take more time in AODV, it is recommended for this technique to be designed by simple minimum delay.

Additional research is recommended in the other parameter that this research has not covered like overhead, quality of service (QOS)...est., and simulate it in a different programmable language such as NS2 to evaluate its effects in the system performance, and reach to complementary results to this research.

Continue research in the AODV security problem and seek a solution with other feed-back in-formations between different layers and compare the achieved results. The future work may provide an encryption scheme for secured packet transmission and also to provide virtual energy for source nodes participating in the routing to still more enhance reliability in MANET routing.

Reference

[1]J.Viterbi Selected Areas in Communications,vol.8,pp.641-9,May1990.

[2] Routing Problems in Mobile Ad hoc Networks (MANET) , [39]Aijaz Ahmad Anchari1 , Asifa Amin2 , Suhail Ashraf3, July 2017.

[3] [ENCRYPT - SECURITY IMPROVED AD HOC ON DEMAND DISTANCEVECTOR ROUTING PROTOCOL (En-SIm AODV)], B. Karthikeyan1, N. Kanimozhi2 and S. Hari Ganesh11 , www.arpnjournals.com1092, © 2013.

[4] [Towards Secure Multi-path Routing for Wireless Mobile Ad-Hoc Networks], Arjun P. Athreya and Patrick Taguefarjun.athreya , patrick.tagueg@sv.cmu.edu.

[5] CROSS-LAYER DESIGN IN4G WIRELESS TERMINAL, Gustavo,Carn Eiro, April 2004

[6] [Efficient Data Transmission In WSN using AODV Protocol], Wayne StarkAchilleasAnastasopoulos, Shihya Chang, http:/www.ijeat.org 2019.

[7] [CROSS LAYER DESIGNS TO OPTIMIZE THE POWERCONSUMPTION IN WIRELESS SENSOR NETWORKS], 1K.LAKSHMISUDHA, 2Dr.C.ARUN1, E-mail: 1kondakalakshmisudha@yahoo.com, 2carunece@gmail.com20th, April 2014.

[8] [REVIEW OF CROSS LAYER DESIGN] , Mr.M.D.Nikose ,Bhagwati Chaturvedi

[9] Cross Layer MAC design for performance optimization of routing protocols in MANETs, P.K.Alima Beebi, February 2011, P a g ehttp://ijacsa.thesai.org/ , Email:haleemamca@gmail.com, sulava_it@gmail.com, maneranjit@gmail.com

[10] [Optimized AODV Routing Protocol for MANET using Cross Layer], PendharkarNivedita Arvindkumar1, Anurag Paliwal2, June 2014 ,www.ijsr.net.

[11] [A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks] , Elizabeth M. Royer, Santa BarbaraChai-KeongToh.

[12] [Mobile Ad Hoc Network Routing Protocols and Cross-Layer Design], Liang Qin and Thomas Kunz, August 2004.

[13] [Cross-Layer Optimization of AODV Routing Protocol For Mobile Ad-Hoc Network(MANET)] , Muhammed Kamrul Islam, ICCSEE 2013, e-mail: kamrul8766@yahoo.com

[14] [Multiple Cross-Layer Design Based Complete Architecture for Mobile Ad-hoc Networks] , R.Venkatachalam , Dr.A.KrishnanDeanK, Vol. 5, No. 1, 2009.

[15] [QoS in Mobile Ad Hoc Networks], Lei Chen and Wendi Heinzelman, wheinzel_@ece.rochester.edu

[16] [Mobile Ad hoc Networking (MANET)], Network Working Group S. Corson Request, 1999.

[17] [Routing Protocols for Mobile Ad-hoc Networks] JohanssonQericsson.comTony.LarssonQera-t.ericsson.se Nicklas.HedmanQlu.erisoft.seBartosz Mielczarek Mikael Degermark

[18] [An Overview of AODV Routing Protocol], Prashant Kumar Maurya1, Gaurav Sharma2, Vaishali Sahu3, Ashish Roberts4, Mahendra Srivastava5
May-June 2012
www.ijmer.com

[19] [Cross-Layer Optimization of AODV Routing Protocol For Mobile Ad-Hoc Network(MANET)] , Muhammed Kamrul Islam, ICCSEE 2013, e-mail: kamrul8766@yahoo.com

[20] [Routing Protocols for Mobile Ad-hoc Networks] JohanssonQericsson.comTony.LarssonQera-t.ericsson.se Nicklas.HedmanQlu.erisoft.seBartosz Mielczarek Mikael Degermark

[21] [Improving AODV protocol through cross layer design in MANET] , Nidhishkumar P. Modi1, Krunal J. Panchal2, (www.ijedr.org) , © 2014 .

[22] [On-demand Multipath Distance Vector Routing in Ad Hoc Networks] , Mahesh K. Marina Samir R. Das, E-mail: mmarina, sdas@ececs.uc.edu

[23] [Performance analysis of AODV, DSR, OLSR and DSDV, Routing Protocols], S.Mohapatraa, P.Kanungob, (2012).

[24] [An implementation of security policy by using ID in Ad hoc routing for mobile network], NaincyJuneja(M.TECH C.S.E) , juneja@gmail.com, April 2014 .

[25] [A DEFENSE SYSTEM ON DDOS ATTACKS IN MOBILE AD HOC NETWORKS] , Yu Wang Joe, May 10th, 2007.

[26] [Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks], Charles E. Perkins, Elizabeth M. Royer, Samir R. Das and Mahesh K. Marina

[27] [A DEFENSE SYSTEM ON DDOS ATTACKS IN MOBILE AD HOC NETWORKS], XuanYuDoctor , May 10th, 2007.

[28] [Trusted AODV Routing Optimization in Manet], 1V. Keerthika and 2N. Dr.RR&Dr.SR, 10.5829/idosi.mejsr.2016 .

[29] [A Trust Model Based Routing Protocol for Secure Ad Hoc Networks], [26] Xiaoqi Li, Michael R. Lyu, and JiangchuanLiu , ljc_@cse.cuhk.edu.hk.

[30] [Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks], Dr.S.PalaniswamiRegistrar, , 2009A.

[31] [An implementation of security policy by using ID in Ad hoc routing for mobile network], NaincyJuneja(M.TECH C.S.E) , juneja@gmail.com, April 2014 .

[32] [An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)], Rajdeep S. Shaktawat, July 2014.

[33] Routing Problems in Mobile Ad hoc Networks (MANET) , [39]Aijaz Ahmad Anchari1 , Asifa Amin2 , Suhail Ashraf3, July 2017.

[34] [An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)], Rajdeep S. Shaktawat, July 2014.

[35] [ENCRYPT - SECURITY IMPROVED AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL (En-SIm AODV)],

B. Karthikeyan1, N. Kanimozhi2 and S. Hari Ganesh1, www.arpnjournals.com, JANUARY 2016 .

[36] [Implementation of secure AODV in MANET], Rizwan Akhtar, Imran Memon, Noor Ul Amin, Mohsin Shah , rizwanakhtarpk@gmail.com, March 2013.

[37] [An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)], Rajdeep S. Shaktawat, July 2014.

[38] [An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)], Rajdeep S. Shaktawat, July 2014.

[39] [An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)], Rajdeep S. Shaktawat, July 2014.

[40] [Routing Security inWireless Ad Hoc Networks] , Hongmei Deng, Wei Li, and Dharma P. Agrawal.

[41] [Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks], Dr.S.PalaniswamiRegistrar, , 2009A.

[42] [Efficient Data Transmission In WSN using AODV Protocol], Wayne StarkAchilleasAnastasopoulos, Shihya Chang, http:/www.ijeat.org 2019.

Appendix

Enhanced AODV Routing protocol

```
%% Initial Condition
clc,clearall,closeall,clf;
%% Input
E_T_E    = [];
T        = [];
BR       = [];
N        = [];
M        = [];
PR       = [];

E_T_E_old    = [];
T_old        = [];
BR_old       = [];
N_old        = [];
M_old        = [];
PR_old       = [];

E_T_E_new    = [];
T_new        = [];
BR_new       = [];
N_new        = [];
M_new        = [];
PR_new       = [];
ST = [];
TRPN = [];
TRPO = [];
for  Miliciouc_Node1 = [90 30]
tic
forNumber_of_Nodes = 100:30:600

Nuber_of_Nodes       = Number_of_Nodes;

%Number_of_Nodes      = ceil(50*rand+50);                  %
Input Number  of Nodes
%Miliciouc_Node       = 0;%ceil(0.1*Number_of_Nodes);
Miliciouc_Node       =
ceil(Number_of_Nodes*rand(1,Miliciouc_Node1));
Postion_Node_X       = 9*rand(1 , Number_of_Nodes)+1;     %
Postion of Nodes on X axis
Postion_Node_Y       = 9*rand(1 , Number_of_Nodes)+1;     %
Postion of Nodes on Y axis
Look_up_Table        = [];                          % Initial
Value for LookUp Table for Nodes
Evaluation_DATA      = [];
Evaluation_DATA_old      = [];
Evaluation_DATA_new      = [];
```

```
roots                = [];
Delay_for_Nodes      = 1e-6;
Delay_for_Milicious = 3e-4;
Dis_bet_Nodes        = 100e-6;
Packet_Size          = 512;
%% Body
%% Evaluate Look up Table for Each Node Asume that Each
Node Connected to Closest Nodes
%
forNode_num = 1 :Number_of_Nodes
% Search Closest Nodes for all Nodes
[Four_Nodes_iddist_propagation] = ...
Find_Closest_Nodes(Node_num,Postion_Node_X,Postion_Node_Y)
;          % Find Closest Four Nodes for Specific Node_Num
if(sum(Node_num == Miliciouc_Node) >= 1)
dist_propagation(1) = ceil(100*rand+101);
else
dist_propagation(1) = ceil(10*rand + 10);
end
Look_up_Table = [Look_up_TableFour_Nodes_id'
dist_propagation'] ;    % Put the Closest Nodes for each
Node_Num on LookUp Table
% In Which Insert the LookUp Table for Others Nodes
Sequentlly
% For each count it will Update LookUP for New Node
end
a=[];b=[];
a = find(sqrt((Postion_Node_X).^2+(Postion_Node_Y).^2) ==
max(sqrt((Postion_Node_X).^2+(Postion_Node_Y).^2)));
b = find(sqrt((Postion_Node_X).^2+(Postion_Node_Y).^2) ==
min(sqrt((Postion_Node_X).^2+(Postion_Node_Y).^2)));

%Look_up_Table(:,1) = [];
% Remove First Column for Initial Value Normally equal
Zero
forijk = 1:2

Source      = a(1);%ceil(Number_of_Nodes*rand);
Distination = b(1);%ceil(Number_of_Nodes*rand);
prev_rep = Distination*2-1;
roots = [];
%ST = [];
[rootssend_replayMiliciouc] =
Find_Short_Root(Source,Distination,Look_up_Table);
roots_valid = Look_up_Table(1,2*(1 : Number_of_Nodes) -
1);
% send_replay_O= [];
[send_replay_O] =
Connecti_Orinted(Source,Distination,roots_valid,Postion_No
de_X,Postion_Node_Y);
```

```
[OLD_Root, NEW_Root] =
ADOV_Enhanced_root(Miliciouc_Node,send_replay_O,Look_up_Ta
ble,Postion_Node_X,Postion_Node_Y);
[data_frame_old, data_frame_new] =
Evaluate_Data(ijk,Source,Distination,OLD_Root,
NEW_Root,Look_up_Table);
% roots
% send_replay_O = [send_replay_ODistination]
remove_ind = find(roots == Distination);
roots(remove_ind+1:end) = [];
Distance_to_find_root = sum(Look_up_Table(2,roots*2));
Number_Of_Nodes1 = length(roots);
data_frame =
[ijk;Source;Distination;Distance_to_find_root;Number_Of_No
des1;Miliciouc];
Evaluation_DATA = [Evaluation_DATAdata_frame];
Evaluation_DATA_old = [Evaluation_DATA_olddata_frame_old];
Evaluation_DATA_new = [Evaluation_DATA_newdata_frame_new];
% fprintf("
_____________________________________________________________
_____________ \n")
% fprintf("
_____________________________________________________________
_____________ \n")
% fprintf("
_____________________________________________________________
_____________ \n")
% fprintf("|NO       |SOURCE  |Distination |DIS_ROOT
|NUM_NODE  |MIicious_NODE|\n")
% fprintf("
=============================================================
============ \n")
% fprintf("|%2d       %2d      |%2d          |%4.2d
|%4d      |%4d         |\n",Evaluation_DATA)
%
fprintf("\n|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~|\n");
% Postion_Node_X      = 9*rand(1 , Number_of_Nodes)+1;
% Postion of Nodes on X axis
% Postion_Node_Y      = 9*rand(1 , Number_of_Nodes)+1;
% Postion of Nodes on Y axis
%pause(3);
% roots;
% send_replay_O;
% Quart;
%% OutPUT
% Insert Which Nodes
%Node_order = 10;
%index = 2*Node_order - 1;
x = Postion_Node_X;
y = Postion_Node_Y;
```

```
L = Look_up_Table;
% figure(1)
% if (Number_of_Nodes>=200)
% figure(1)
% plot(x,y,'*'),hold on
%
% text(x(Source),y(Source),num2str(Source))
% text(x(Distination),y(Distination),num2str(Distination))
%
%
% index = 2*roots(1) - 1;
% k=0;
% for rrr = roots
% if(rem(k,2) == 1)
% for IN_M = 1:length(Miliciouc_Node)
%     in = 2*Miliciouc_Node(IN_M) - 1;
%     figure(1)
% plot([x(L(1,in)) x(L(2,in))],[y(L(1,in)) y(L(2,in))],'r-
');
% plot([x(L(1,in)) x(L(3,in))],[y(L(1,in)) y(L(3,in))],'r-
');
% plot([x(L(1,in)) x(L(4,in))],[y(L(1,in)) y(L(4,in))],'r-
');
% plot([x(L(1,in)) x(L(5,in))],[y(L(1,in)) y(L(5,in))],'r-
');
% % 'LineWidth',2,'MarkerSize',5,...
% %         'MarkerEdgeColor','R')
% end
% else
% for IN_M = 1:length(Miliciouc_Node)
%     in = 2*Miliciouc_Node(IN_M) - 1;
%     figure(1)
% plot([x(L(1,in)) x(L(2,in))],[y(L(1,in))
y(L(2,in))],'C.-');
% plot([x(L(1,in)) x(L(3,in))],[y(L(1,in))
y(L(3,in))],'C.-');
% plot([x(L(1,in)) x(L(4,in))],[y(L(1,in))
y(L(4,in))],'C.-');
% plot([x(L(1,in)) x(L(5,in))],[y(L(1,in))
y(L(5,in))],'C.-');
% % 'LineWidth',2,'MarkerSize',5,...
% %         'MarkerEdgeColor','R')
% end
% end
% index_curr = 2*rrr - 1;
% k=k+1;
% if k >= length(roots)-5
%     if (rrr == Distination)
%         figure(1)
```

```
%         plot([x(L(1,index))
x(L(1,index_curr))],[y(L(1,index)) y(L(1,index_curr))],'m-
S','linewidth',1),
%         plot(x(L(1,index_curr)), y(L(1,index_curr)),'--
gs',...
%         'LineWidth',2,...
%         'MarkerSize',5,...
%         'MarkerEdgeColor','b',...
%         'MarkerFaceColor',[0.5,0.5,0.5]);
%     for i = (length(send_replay_O)):-1:1
%        % if(send_replay_O(i) > 1)
%                figure(1)
%               plot([x(L(1,prev_rep))
x(L(1,send_replay_O(i)*2-1))],[y(L(1,prev_rep))
y(L(1,send_replay_O(i)*2-1))],'m-S','linewidth',3),
%               prev_rep = send_replay_O(i)*2-1;
%               pause(5/100);
%         %end
%     end
%     else
%         figure(1)
%         plot([x(L(1,index))
x(L(1,index_curr))],[y(L(1,index)) y(L(1,index_curr))],'k-
d','linewidth',1),
%     end
% else
%      figure(1)
%     plot([x(L(1,index))
x(L(1,index_curr))],[y(L(1,index)) y(L(1,index_curr))],'b-
s','linewidth',1),
% end
% index = 2*rrr - 1;
% pause(5/100000);
% end
% end
% hold off
end

Bit_Rate =
Packet_Size./(Delay_for_Nodes*Evaluation_DATA(5,:)+Delay_f
or_Milicious*Evaluation_DATA(6,:)+Dis_bet_Nodes*Evaluation
_DATA(4,:));
Bit_Rate_old =
Packet_Size./(Delay_for_Nodes*Evaluation_DATA_old(5,:)+Del
ay_for_Milicious*Evaluation_DATA_old(6,:)+Dis_bet_Nodes*Ev
aluation_DATA_old(4,:));
Bit_Rate_new =
Packet_Size./(Delay_for_Nodes*Evaluation_DATA_new(5,:)+Del
ay_for_Milicious*Evaluation_DATA_new(6,:)+Dis_bet_Nodes*Ev
aluation_DATA_new(4,:));
Bit_Rate = sum(Bit_Rate)/length(Bit_Rate);
```

```
Bit_Rate_old = sum(Bit_Rate_old)/length(Bit_Rate_old);
Bit_Rate_new = sum(Bit_Rate_new)/length(Bit_Rate_new);
BR = [BR Bit_Rate];
BR_old = [BR_oldBit_Rate_old];
BR_new = [BR_newBit_Rate_new];
End_to_End_Delay =
ijk*(Delay_for_Nodes*Evaluation_DATA(5,:)+Delay_for_Milici
ous*Evaluation_DATA(6,:)+Dis_bet_Nodes*Evaluation_DATA(4,:
));
End_to_End_Delay_old =
ijk*(Delay_for_Nodes*Evaluation_DATA_old(5,:)+Delay_for_Mi
licious*Evaluation_DATA_old(6,:)+Dis_bet_Nodes*Evaluation_
DATA_old(4,:));
End_to_End_Delay_new =
ijk*(Delay_for_Nodes*Evaluation_DATA_new(5,:)+Delay_for_Mi
licious*Evaluation_DATA_new(6,:)+Dis_bet_Nodes*Evaluation_
DATA_new(4,:));
End_to_End_Delay
=sum(End_to_End_Delay)/length(End_to_End_Delay);
End_to_End_Delay_old
=sum(End_to_End_Delay_old)/length(End_to_End_Delay_old);
End_to_End_Delay_new
=sum(End_to_End_Delay_new)/length(End_to_End_Delay_new);
E_T_E = [E_T_E End_to_End_Delay];
E_T_E_old = [E_T_E_oldEnd_to_End_Delay_old];
E_T_E_new = [E_T_E_newEnd_to_End_Delay_new];
N = [ NNumber_of_Nodes];
ML =
sum(Evaluation_DATA(6,:))/length(Evaluation_DATA(6,:));
ML_old =
sum(Evaluation_DATA_old(6,:))/length(Evaluation_DATA_old(6
,:));
ML_new =
sum(Evaluation_DATA_new(6,:))/length(Evaluation_DATA_new(6
,:));
M = [M ML];
M_old = [M_oldML_old];
M_new = [M_newML_new];
Throuput = ijk*Packet_Size*8./(sum(End_to_End_Delay));
Throuput_old =
ijk*Packet_Size*8./(sum(End_to_End_Delay_old));
Throuput_new =
ijk*Packet_Size*8./(sum(End_to_End_Delay_new));
T = [T Throuput];
T_old = [T_oldThrouput_old];
T_new = [T_newThrouput_new];
Received_P = 0.01*sum(Evaluation_DATA(6,:));
Received_P_old = 0.01*sum(Evaluation_DATA_old(6,:));
Received_P_new = 0.01*sum(Evaluation_DATA_new(6,:));
Packet_Delivary_Ratio = ijk / (ijk+Received_P) -
(Number_of_Nodes/1500+0.005*rand);
```

```
Packet_Delivary_Ratio_old = ijk / (ijk+Received_P_old) -
(Number_of_Nodes/1500+0.005*rand);
Packet_Delivary_Ratio_new = ijk / (ijk+Received_P_new) -
(Number_of_Nodes/1500+0.005*rand);
PR = [ PRPacket_Delivary_Ratio];
PR_old = [ PR_oldPacket_Delivary_Ratio_old];
PR_new = [ PR_newPacket_Delivary_Ratio_new];

end
Simulation_time = toc;
ST = [ST Simulation_time];
TRPN = [TRPN sum(T_new)]
TRPO = [TRPO sum(T_old)]
if (Miliciouc_Node1 == 90)
% figure(2),hold off
% [ST,T_new] = reorder(ST,T_new);
% loglog(ST,T_new,'b-
S','linewidth',2),title('Throughput'),hold on
% [ST,T_old] = reorder(ST,T_old);
% loglog(ST,T_old,'r-
S','linewidth',2),title('Throughput'),legend(['NO Milicous
' num2str(Miliciouc_Node1)],['Milicous'
num2str(Miliciouc_Node1)]),grid,hold off
% %disp('M_30__________:')
% %disp([ST' N'])
% T_new = [];
% T_old = [];
% ST    = [];
figure(4),hold off
semilogy(N,E_T_E_new,'b-S','linewidth',2),title('End to
End Delay'),hold on
semilogy(N,E_T_E_old,'r-S','linewidth',2),title('End to
End Delay'),legend(['Enhanced Aodv with malicious node '
num2str(Miliciouc_Node1)],['Normal Aodv with Milicous
node' num2str(Miliciouc_Node1)]),grid,holdoff
E_T_E_new = [];
E_T_E_old = [];
xlabel('number of nodes')
ylabel('End to End Delay(s)')

figure(6),hold off
semilogy(N,BR_new,'b-S','linewidth',2),title('Bit Rate'),
hold on
semilogy(N,BR_old,'r-S','linewidth',2),title('Bit
Rate'),legend(['Enhanced Aodv with malicious node
'num2str(Miliciouc_Node1)],['Normal Aodv with Milicous
node' num2str(Miliciouc_Node1)]),grid,holdoff
BR_new = [];
BR_old = [];
xlabel('number of nodes')
ylabel('Bit Rate(Mbps)')
```

```
figure(8),hold off
plot(N,M_new,'b-S','linewidth',2),title('Milicious'), hold
on
plot(N,M_old,'r-
S','linewidth',2),title('Milicious'),legend(['Enhanced
Aodv with malicious node '
num2str(Miliciouc_Node1)],['Normal Aodv with Milicous
node' num2str(Miliciouc_Node1)]),grid,holdoff
M_new = [];
M_old = [];
xlabel('number of nodes')
ylabel('malicious nodes')


figure(10),hold off
semilogy(N,PR_new,'b-S','linewidth',2),title('Packet
Ratio'), hold on
semilogy(N,PR_old,'r-S','linewidth',2),title('Packet
Ratio'),legend(['Enhanced Aodv with malicious node '
num2str(Miliciouc_Node1)],['Normal Aodv with Milicous
node' num2str(Miliciouc_Node1)]),grid,holdoff
PR_new = [];
PR_old = [];
N = [];
xlabel('number of nodes')
ylabel('Packet Ratio(%)')


else
figure(3)
%[ST,T_new] = reorder(ST,T_new);
bar(ST,TRPN,0.4),title('Throughput'),legend(['Enhanced
Aodv with malicious node '
num2str(Miliciouc_Node1)],['Normal Aodv with Milicous
node' num2str(Miliciouc_Node1)]),grid
text(ST(1),TRPN(1)+0.2e7)
xlabel('number of nodes')
ylabel('Throughput(Mbp)')
%[ST,T_old] = reorder(ST,T_old);


figure(33)
bar(ST,TRPO,0.9),title('Throughput'),legend(['Enhanced
Aodv with malicious node
'num2str(Miliciouc_Node1)],['Normal Aodv with Milicous
node' num2str(Miliciouc_Node1)]),grid
text(ST(2),TRPO(2)+0.2e7)
xlabel('number of nodes')
ylabel('Throughput(Mbp)')
%disp('M_90__________:')
```

```
%disp([ST' N'])


figure(5),hold off
semilogy(N,E_T_E_new,'b-S','linewidth',2),title('End to
End Delay'),hold on
semilogy(N,E_T_E_old,'r-S','linewidth',2),title('End to
End Delay'),legend(['Enhanced Aodv with malicious node '
num2str(Miliciouc_Node1)],['Normal Aodv with Milicous'
num2str(Miliciouc_Node1)]),grid,holdoff
xlabel('number of nodes')
ylabel('End to End Delay(s)')

figure(7),hold off
semilogy(N,BR_new,'b-S','linewidth',2),title('Bit Rate'),
hold on
semilogy(N,BR_old,'r-S','linewidth',2),title('Bit
Rate'),legend(['Enhanced Aodv with malicious node '
num2str(Miliciouc_Node1)],['Normal Aodv with Milicous'
num2str(Miliciouc_Node1)]),grid,holdoff
xlabel('number of nodes')
ylabel('Bit Rate(Mbps)')

figure(9),hold off
plot(N,M_new,'b-S','linewidth',2),title('Milicious'), hold
on
plot(N,M_old,'r-
S','linewidth',2),title('Milicious'),legend(['Enhanced
Aodv with malicious node '
num2str(Miliciouc_Node1)],['Normal Aodv with Milicous'
num2str(Miliciouc_Node1)]),grid,holdoff
xlabel('number of nodes')
ylabel('malicious nodes')

figure(11),hold off
semilogy(N,PR_new,'b-S','linewidth',2),title('Packet
Ratio'), hold on
semilogy(N,PR_old,'r-S','linewidth',2),title('Packet
Ratio'),legend(['Enhanced Aodv with malicious node '
num2str(Miliciouc_Node1)],['Normal Aodv with Milicous'
num2str(Miliciouc_Node1)]),grid,holdoff
xlabel('number of nodes')
ylabel('Packet Ratio(%)')

end
% if (Miliciouc_Node1 ==0)
% figure(31)
% semilogy(N,T,'b-S','linewidth',2),title('Throughput')
% figure(61)
% semilogy(N,E_T_E,'b-S','linewidth',2),title('End to End
Delay')
```

```
% figure(51)
% semilogy(N,BR,'b-S','linewidth',2),title('Bit Rate')
% figure(71)
% semilogy(N,M,'b-S','linewidth',2),title('Milicious')
% figure(91)
% semilogy(N,PR,'b-S','linewidth',2),title('Packet Ratio')
% T=[];E_T_E=[];BR=[];M=[];N=[];PR=[];
% else
% figure(32)
% semilogy(N,T,'r-
S','linewidth',2),title('Throughput'),grid
% figure(62)
% semilogy(N,E_T_E,'r-S','linewidth',2),title('End to End
Delay'),grid
% figure(52)
% semilogy(N,BR,'r-S','linewidth',2),title('Bit
Rate'),grid
% figure(72)
% semilogy(N,M,'r-
S','linewidth',2),title('Milicious'),grid
% figure(92)
% semilogy(N,PR,'r-S','linewidth',2),title('Packet
Ratio'),grid
% end
end

Mean_Throughput_old     = mean(T_old);
Mean_Delay_old          = mean(E_T_E_old);
Mean_BitRate_old        = mean(BR_old);
Mean_PacketRatiao_old   = mean(PR_old);

Mean_Throughput_new     = mean(T_new );
Mean_Delay_new          = mean(E_T_E_new );
Mean_BitRate_new        = mean(BR_new );
Mean_PacketRatiao_new   = mean(PR_new );

disp(['     Thr       ''De          ''BR         ''PR
'])
disp([Mean_Throughput_oldMean_Delay_oldMean_BitRate_oldMea
n_PacketRatiao_old])
disp([Mean_Throughput_newMean_Delay_newMean_BitRate_newMea
n_PacketRatiao_new])
```