ENERGY-EFFICIENT HYBRID SECURED ROUTING FOR 5G VEHICULAR AD HOC NETWORK (VANET)

Zerihun Tamiru Fufa

A Thesis Submitted to

The Department of Electronics and Communication Engineering
School of Electrical Engineering and Computing

Presented in Partial Fulfillment of the Requirement for the Master's of Science Degree in Electronics and Communication Engineering

Office of Graduate Studies

Adama Science and Technology University

July 2021

Adama, Ethiopia

ENERGY-EFFICIENT HYBRID SECURED ROUTING FOR 5G VEHICULAR AD HOC NETWORK (VANET)

Zerihun Tamiru Fufa

Advisor: Dr. Rajaveerappa Devadoss (PhD)

Co-Advisor: Mr. Shanko Chura (PhD Candidate)

A Thesis Submitted to the

Department of Electronics and Communication Engineering

School of Electrical Engineering and Computing

Presented in Partial Fulfillment of the Requirement for the Master's of Science Degree in Electronics and Communication Engineering

Office of Graduate Studies

Adama Science and Technology University

July 2021

Adama, Ethiopia

DECLARATION

I hereby declare that this Master thesis entitled “Energy-Efficient Hybrid Secured Routing for 5G Vehicular Ad hoc Network (VANET)” is my original work. That is, it has not been submitted for the award of any other academic degree, diploma, or certificate in any other university. All sources of materials that are used for this thesis have been duly acknowledged through citation.

Name of the student	Signature	Date

RECOMMENDATION

We, the advisors of the thesis, hereby certify that we have read the revised version of the thesis entitled “Energy-Efficient Hybrid Secured Routing for 5G Vehicular Ad hoc Network (VANET)” prepared under our guidance by Zerihun Tamiru Fufa submitted in partial fulfillment for the degree of Master’s of Science in Electronics and Communication Engineering. Therefore, we recommend the submission of a revised version of the thesis to the department following the applicable procedures.

____________________________	_______________	_______________
Major Advisor	Signature	Date
____________________________	_______________	_______________
Co-Advisor	Signature	Date

APPROVAL SHEET

We, the advisors of the thesis entitled “Energy-Efficient Hybrid Secured Routing for 5G Vehicular Ad hoc Network (VANET)” and developed by Zerihun Tamiru, hereby certify that the recommendation and suggestions made by the board of examiners are appropriately incorporated into the final version of the thesis.

Major Advisor	Signature	Date
Co-Advisor	Signature	Date

We, the undersigned, members of the Board of Examiners of the thesis by Zerihun Tamiru have read and evaluated the thesis entitled “Energy-Efficient Hybrid Secured Routing for 5G Vehicular Ad hoc Network (VANET)” and examined the candidate during open defence. This is, therefore, to certify that the thesis is accepted for partial fulfillment of the requirement of degree of Masters of Science in Electronics and Communication Engineering.

Chairperson	Signature	Date
Internal Examiner	Signature	Date
External Examiner	Signature	Date

Final approval and acceptance of the thesis is contingent upon the submission of its final copy to the Office of Postgraduate Studies (OPGS) through the Department Graduate Council (DGC) and School Graduate Committee (SGC).

Department Head	Signature	Date
School Dean	Signature	Date
Office of Postgraduate Studies, Dean	Signature	Date

ACKNOWLEDGMENT

First and foremost, I would like to thank Almighty God for giving me all the help and strength to complete my thesis.

Second, I would like to express my deepest appreciation to my advisor Dr. D. Rajaveerappa and my co-advisor Mr. Shanko Chura for their continuous encouragement and guidance throughout the research work.

Finally, I acknowledge ECE Dept. and School of Electrical and Computing, Adama, Ethiopia for giving opportunity and active environment for pursuing my research work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

5G	Fifth Generation
AOA	Angle of Arrival
ASPR	Adaptive Shortest Path Routing
BER	Bit Error Rate
CV	Connected Vehicle
CBF	Centralized Bellman-Ford algorithm
DoA	Direction of Arrival
DOS	Denial of Services
DBF	Distributed Bellman-Ford
DSRC	Dedicated Short Range Communication
DVR	Distance Vector Routing
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineering
ITS	Intelligent Transportation Systems
LMS	Least Mean Square
LSR	Link State Routing
MAC	Media Access Control
MIMO	Multiple Inputs Multiple Outputs
MATLAB	Matrix Laboratory
OBU	On-Board Units
RSU	Road Side Units

SNR	Signal to Noise Ratio
SOI	Signal of Interest
SPR	Shortest Path Routing
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
VANET	Vehicular Ad hoc Network
WSN	Wireless Sensor Network

ABSTRACT

These days, road accidents and traffic jams have increased significantly on the route due to the higher number of vehicles. Vehicular Ad hoc Networks (VANETs) are effective intelligent transportation systems in decreasing accidents and traffic congestions. Vehicular communications deal with not only information about traffic and road conditions but also involved user-specific information such as their route and time-critical information. However, the information transmission is vulnerable to eavesdropping and link failure due to the high mobility of the vehicles. In this research, analysis of Secured Routing to provide information to the legitimate nodes in the presence of unwanted eavesdroppers is done. The hybrid energy-efficient routing algorithm is used for better stability of the connected vehicle. The beamforming technique is applied to prevent the eavesdropper from intercepting confidential information using an array of antennas. A combined detailed analytical model of min norm DoA, LMS adaptive beamforming, hybrid route based on Dijkstra and Bellman-Ford algorithm showed a greater secrecy rate. The simulation is carried out in MATLAB 2014a MEX file package software. The result obtained such as energy efficiency and secrecy rate are convincing compared to the previous result content in the literature.

Keywords: *Vehicular Ad hock Network (VANET), Secured Routing, LMS, Min norm.*

CHAPTER ONE

1. INTRODUCTION

1.1 Background of the Study

These days most people use vehicular transports to transit between various places. An increase in vehicular traffic on street networks has led to rising road queues and fatalities. Traffic congestion and driving problems, in turn, raised street accidents and deaths due to lack of information about the street. These can be lessened by affording proper knowledge about street conditions and the neighbouring environment to the driving public via an Intelligent Transportation System (ITS).

VANET is one of the promising technologies for ITS. It is a special class of mobile ad hoc networks (MANETs) in which vehicles act like moving nodes [1]. In VANET vehicles are equipped with networked communications for exchanging information between vehicles as well as intelligent device and radio interface roadside units (RSUs). The vehicular network allows vehicles to instantly send messages to other vehicles or infrastructures. These networks are adapted to support the highly dynamic nature of the vehicles as network nodes, fulfill their mobility requirements [2]. It enables a car that detects a hazardous situation to warn other drivers on the road. Using this type of communication, drivers can handle time-critical information such as road or weather conditions and crashes, breakdowns, or emergency vehicle on-site warning.

VANET communication takes place through a wireless medium. This information must be delivered to other neighbouring vehicles timely without delay within limited time. If a single event-driven message is lost or a safety message is delayed, it could end in loss of life. Due to the rapid topology of vehicle mobility, there is high link failure [3]. Efficient routing is necessary to enable the vehicles in making the best routing decision.

VANET wireless media is also vulnerable to user information eavesdropping, interference, and jamming [4]. To preserve the privacy of users' information, their actual identities, locational data needs to be protected from undesirable intrusion [5]. Multi antenna is one of the powerful techniques for secure vehicular communication.

The technology advancement in fifth Generation (5G) wireless network that uses massive Multiple-Input Multiple Out-put (MIMO) antenna array system can be used for VANET security issue due to its spectral efficiency and low latency. Relay operation is used for no line-of-sight blocked sender and receiver vehicle link due to the mm-wave short wave length loss from penetration and reflection. The antenna array uses several antenna elements and signals received at each antenna element is adaptively combined to improve the overall performance in vehicular communication [6]. Different technique such as Direction of Arrival (DoA), and an adaptive beam forming is very essential in the signal processing [7, 8]. In beam forming technique, signal directional transmission for enhanced gain and enlarged coverage can be achieved. The DoA algorithm also calculates the direction of arrival of all incoming signals.

In this thesis, a high data rate and reduced latency of massive MIMO 5G technology are used for vehicular secure routing. Beam steering antennas form narrow directional beams with relatively low side lobes so that the beams are steered towards an intended target of information transmission and reception of vehicular nodes. Smart beam steering antennas can be steered in any direction at high speeds and also in real-time which helps to collect vehicles network topology. The beam steering technique is done to change the direction of the radiation pattern of the antenna to get the antenna output in the desired vehicle direction. Antenna with enhanced gain and steerable radiation patterns also used to reduce interference saves power, increases gain and directivity of the antenna.

1.2 Statement of the Problem

Dramatically increasing in a population of vehicles lead to vehicular traffic congestion rising road queues and fatalities. The congestion creates difficulty for a vehicle to find out the best route and further leads to a collision. Avoiding this traffic problem requires proper knowledge about street conditions and the neighbouring environment. The VANET routing paths frequently fail due to the high mobility caused by sudden changes in the direction of vehicles. Route planning techniques are one of the main tasks of the VANET communication to find an optimal route from a source node to the next node. The sharing of alert messages between the vehicles must also able to take the right decision safely without delay or low latency of information to reduce collision. Due to the openness of wireless transmission medium, information transmission between the vehicles also faces serious security threats in the network. The major concern for vehicular users is the loss of privacy, after all, nobody wants his/her vehicle to be telling everybody where it is at all times. The existing research on VANET is focused only on the improvement of the routing discovery, but, the research on secure routing is relatively weak.

1.3 Objectives of the Thesis

1.3.1 General Objective

The general objective of this thesis is to improve energy efficiency and secrecy of information transmission in 5G Vehicular ad hoc Network (VANET) using hybrid routing.

1.3.2 Specific Objectives

Particularly the specific objectives of this thesis work are:

- To use min norm DoA algorithm to identify the time varying VANET topology.
- To develop a hybrid routing algorithm to save energy and time of finding the route.
- To identify the direction of incoming signal of interest and eaves dropper to improve the secrecy of information in a particular route.
- To develop a mathematical model using antenna grouping technique to improve secrecy rate.
- To improve SNR of the transmitted information in particular route using adaptive LMS beam forming algorithm.

1.4 Significance of the Study

VANETs is one of the promising technologies for ITS. The vehicular network allows vehicles to instantly send messages to other vehicles or infrastructures. This communication allows a car to detects a hazardous situation to warn other drivers on the road. This study contributes to the reduction of traffic congestion which minimizes road accidents and save human life and property. It has an environmental factor in reduction of the emission of exhaust gas.

1.5 Scope of the Thesis

The VANET has many applications in ITS as street safety and passenger comfort. The communications range from a single node to an internet connection using infrastructure and ad hoc networks. During information transmission, the wireless ad hoc net is vulnerable to various security attacks. However, in this thesis information transmission confidentiality in ad hoc network routed from source node to next node is studied.

1.6 Thesis Organization

The remaining part of the thesis is organized as follows: Chapter 2 includes a literature review on the introduction of VANET routing and security, technological advancement of the array antenna in VANETs. Chapter 3 describes the methodology undertaken in the research. Chapter 4 explains the results with a brief discussion. Finally, Chapter 5 discusses the conclusion and recommendation for future work.

CHAPTER TWO

2. LITERATURE REVIEW

2.1 Introduction of Vehicular Communications

The amount of traffic accidents is in rapid growth with an increase in Vehicular. According to World Health Organization, road accidents annually cause approximately 1.2 million deaths worldwide [9]. This is one of the main incentives for the development of ITS. VANET emerged as an ITS technology to help a group of vehicles to set up and maintain communication among themselves without using any central base station or controller. Ad hoc network is preferable for its ease of deployment, speed of deployment, and decreased dependence on infrastructure considering VANET dynamic topology [10, 11, 12, 13].

Table 2.1: Comparision of MANET and VANET [10]

Parameters	**MANET**	**VANET**
Energy limitation	Low	High
Change in network topology	Slow	Frequent and very fat
Node mobility	Low	High
Network size	Medium	Large
Range	Up to 100m	Up to 600m
Location dependency	Low	High
Moving pattern	Regular	Random

In VANET all nodes have capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers to discover and maintain routes to other nodes in the network. The moving cars used as nodes in a network so each vehicle can receive and transmit to others message through the wireless ad hoc network [15, 16]. The communication between vehicular nodes can take place in two different manners either Vehicle to Vehicle (V2V) communication or vehicle to RSU communication [12]. The VANET communications help in transmitting information about the road condition such as location, speed data, and other alerts of traffic condition to another vehicle.

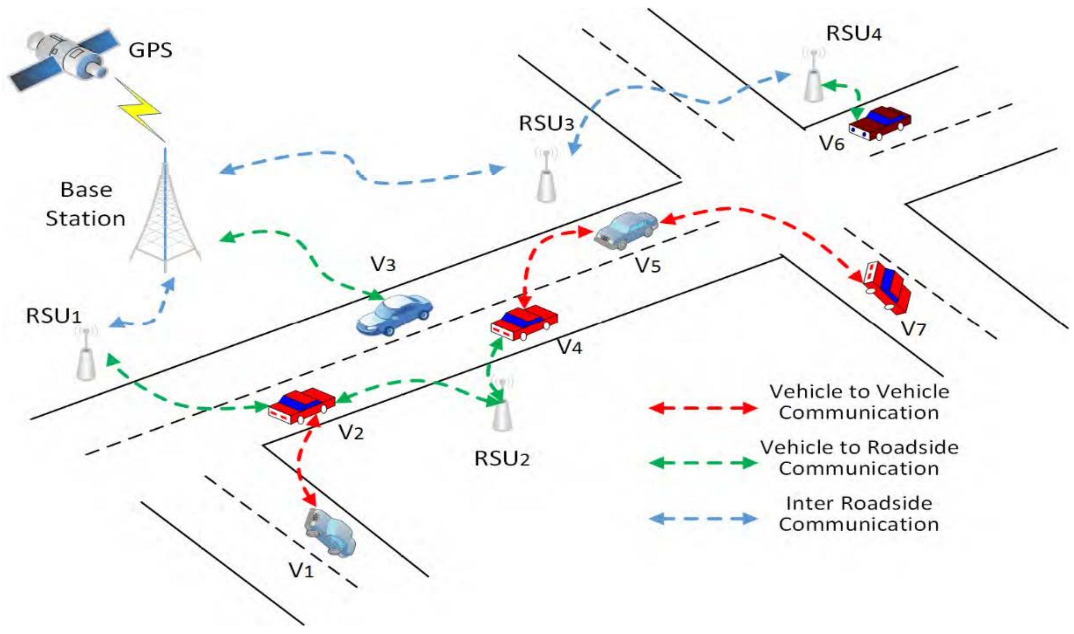


Figure 2.1: VANET Communication [17]

The VANET communication uses different equipment to that enable to establish communication between vehicle and other infrastructure or pedestrian.

2.1.1 VANET Component

VANET comprise vehicles equipped with a wireless device communicating with each other and RSU. The network infrastructure such as the base station or an access point is not required to create VANET, although fixed nodes can be used in VANET in the form of RSU.

Onboard Unit (OBU): This equipment is transceiver installed in vehicles for exchanging data with RSU as well as the other vehicular OBU in collaboration with computing devices. OBU draw power from the vehicular batteries. The OBU contains sensors to gather data about surrounding conditions. Of this equipment, the GPS receiver is utilized to supply geographic data in terms of the location of vehicles. Speed sensors are utilized to gather recordings such as velocity and compromising data. Forward- and rear-facing sensors are utilized to monitor events occurring to the front and rear of vehicles. These monitored and collected recordings are transmitted as messages to neighboring vehicles via wireless media [18].

Roadside Unit: It is typically stationary unit that is installed alongside streets or in fixed sites to include parking or street intersection locations. RSU resemble OBU in that they contain transceivers, antennae, processors, and sensor clusters. Each RSU is intended to provide wireless services to vehicle users.

RSU can be connected to the backbone of the internet through wireless or wired and provides the services such as periodic re-transmission of a message in sparsely populated roads and advertisement services.

The features of VANETs essentially blend the properties of wireless media and the features of various topologies in infrastructure and ad hoc modes. The node mobility in VANET varies with directions and velocities [13, 19]. All nodes in VANET are highly mobile and vehicles interconnect with each other in sessions of only a few seconds. Therefore, secure protocols necessitate significant interaction among senders and receivers. This wireless transmitting media properties lead to particular security issues associated with the nature of transmissions in wireless environments as well as communication security [20].

2.2 VANET Security and Routing Protocol.

2.2.1 Security Issue in VANET

In VANET communication it is very important to secure the information transmission so that it cannot be accessed by malicious users or attackers [21] [22] [23]. To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. There are security goals to be achieved in wireless system [24].

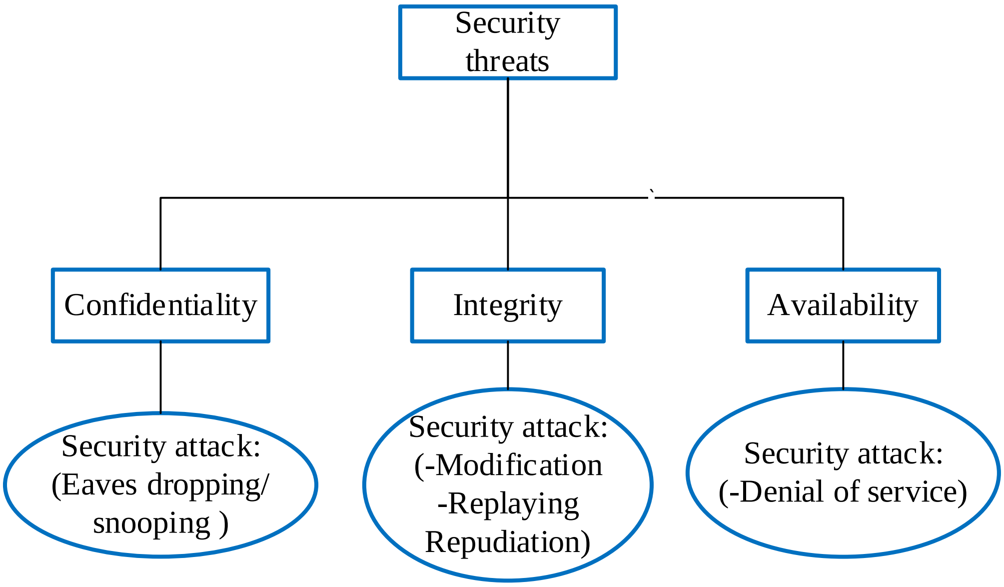


Figure 2.2: Taxonomy of security goals and attacks threatening [24]

Snooping or Eavesdropping: This refers to un authorized access to or interception of data. It is among the more significant attacks against confidentiality over VANETs. To perform such attacks, adversaries can either be in a car that is stopped or moving or else in false RSUs, to demonstrate they form parts of the main network. The illegal aim is to retrieve confidential information. When there are some obstacles between the source and the receivers, since no direct communication link exists, the information should be forwarded by a relay. If a source transmits information to two receiving nodes, the information transmitted to one node may needs to be kept secret from the other node. Here the node that receives information is the destination and the other node is eavesdropper. To overcome the security issue there is different mechanisms.

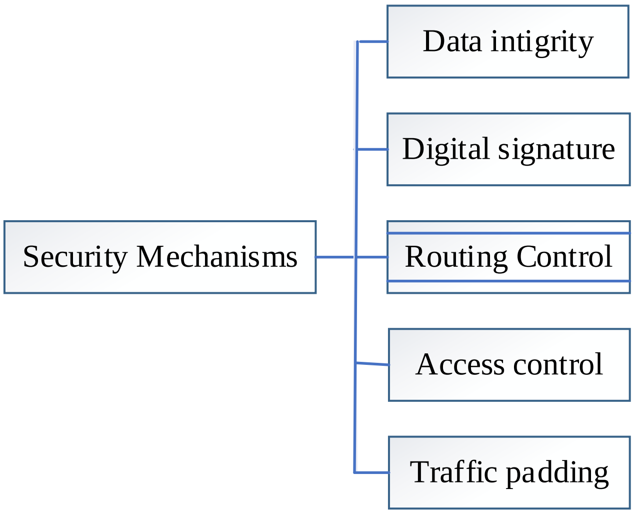


Figure 2.3: Security mechanisms [24]

Routing control security mechanism: It is selecting and continuously changing different available routes between the sender and the receiver to prevent opponent from eavesdropping on a particular route.

2.2.2 VANETs Routing Algorithm

Routing is the process of finding a communication path from a source station to a destination using suitable methods and algorithms to achieve high performance in the network [25]. Such protocols must deal with the typical limitations of the Ad-hoc network like high power consumption, low bandwidth, and error rates. The communication between two vehicular nodes can be a single-hop or multi-hop and the routing protocol decides the route from source to destination for the multi-hop communication [26]. Low latency and reliable end-to-end data delivery are the two main factors for efficient routing protocols. Also Computing the shortest path between two vehicular nodes in road networks is a challenging task in vehicle routing. The routing algorithms must be able to handle scenarios where links may fail and new links may be formed dynamically [27].

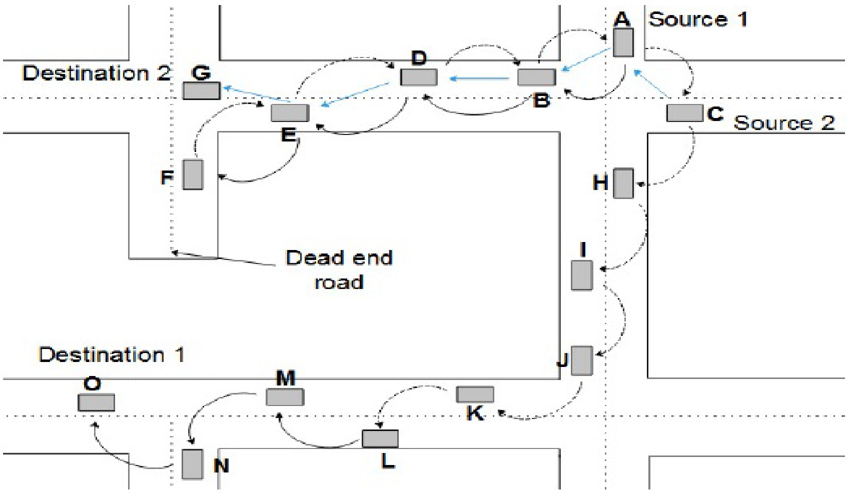


Figure 2.4: Routing scenario [28]

Proactive Routing: This routing protocols is mostly based on shortest path algorithms. It is table-driven protocols and they maintain information of all connected stations in the form of a table. This network maintains only the routes that are currently in use, so reducing the burden on the network when only a few of all available routes are in use at any time. In proactive protocols, each network node stores information on routes to all possible destinations at all times. The advantage of this approach is that when a routing request is needed, it can be initiated with minimal delay. The disadvantage is the overhead in the form of control messages that are required to establish and maintain all routes subject to frequent failure.

Proactive protocols use a route discovery phase before sending any data. Indeed, routes are calculated and maintained up to date continuously by transmitting periodic routing information on the network. Each time a node wants to transmit a packet, the packet is sent only if a route to the destination is established. Otherwise, the packet will wait in a queue until a route has been found. Those types of protocols are difficult to maintain in a highly dynamic nature of VANET [29] .

Reactive (on-demand) Routing: In this case routes are established on as-needed basis. This approach requires less control information, particularly when the network topology is rapidly changing or when the data burst or directed to only a small subset of the network nodes that are unknown in advance. The disadvantage of such an approach is that route requests can experience a large delay before being propagated from the source node, as a route to the destination has to first be determined.

Route discovery is used when a source node needs to forward a packet to a particular destination, but does not have a corresponding route stored in its cache. In this case, the source node floods a query packet through the network. Intermediary nodes append their own identity to the query and forward it unless they are either the destination node or have a route for the destination stored in their cache. Nodes that do not forward the query send a reply message back to the source. When the reply arrives back to the source, the newly discovered route is stored in the source's cache and routing can commence. Reactive protocols present lower overhead than proactive protocols, but the end-to-end delay is more important due to the route discovery phase started every time a packet needs to be sent. The reactive protocols present inconveniences in VANET where the transmission requires a low end to end delay [30].

Hybrid Routing: Routing algorithms in this class incorporate elements of both proactive and reactive protocols. Two immediate strategies for routing in wireless networks are minimum energy routing, in which the link metric is the energy required to send a wireless transmission over the link, and minimum hop routing, in which the link metric is constant for all links [31].

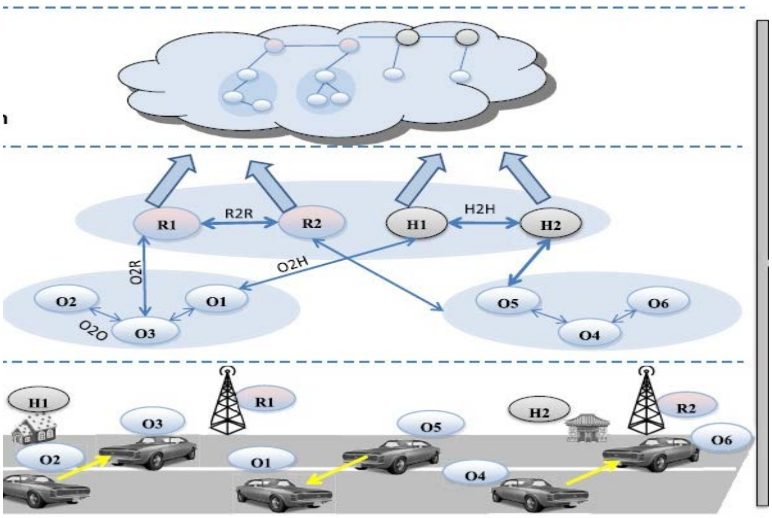


Figure 2.5: Social interconnection of vehicles [13]

Minimum hop routing sometimes minimizes the end-to-end routing delay in a network. In reality, such approach tends to use the same subset of links to transmit the network's traffic. This leads to congested routes which in turn lead to relatively long routing delays.

2.3 Technology Advancement in VANETs

There exist several technologies that enable Ad-hoc networking or to interconnect vehicles. The most popular one is Wi-Fi. Protocols [32]. Further, wide-area networking (WAN) technologies such as 2G/GPRS, /3G/UMTS, 4G/LTE, and beyond technologies have also been used for vehicle-to-back-office communication, but these from location accuracy which could be improved by a secondary mechanism such as GPS [33]. Wireless Access for Vehicular Environment (WAVE) is required to support the intelligent transportation system application in short-range communication [12]. It also demands the low latency requested by the real-time communication.

Table 2.2: Active safety latency requirements

Latency requirements	**Units/seconds**
Traffic signal violation warning	0.1
Curve speed warning	1.0
Emergency electronic brake lights	0.1
Pre-crash sensing	0.002
Lane changing warning	0.1
Stop sign movement assistance	0.1

As Table 2.2 above indicate the safety of vehicular communication information transmission with high speed. If the information delayed it may result in loss of life and property. There massive antenna technology is current technology to relay information by beamforming technique.

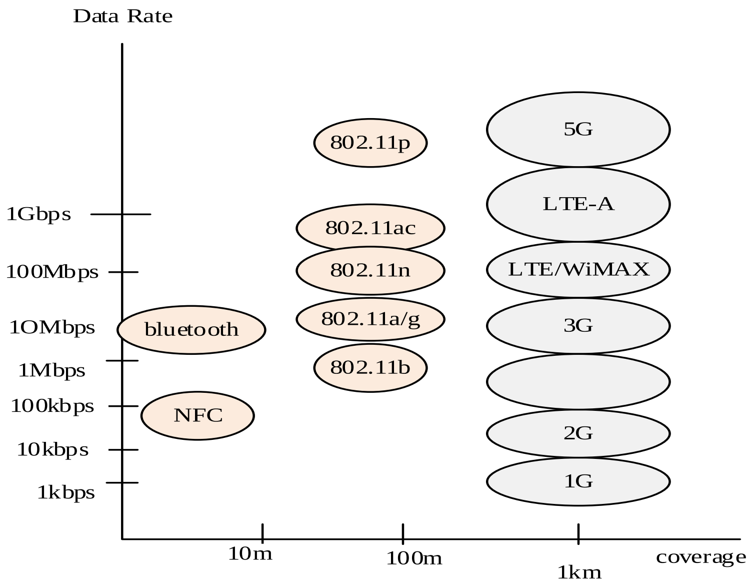


Figure 2.6: Comparison of emerging Ad hoc wireless communication

The Ad hoc network wireless information transmission coverage and date rate is highly increasing with the technology advancement especially smart antenna system.

2.3.1 Antenna Array Technology

A single antenna element is not suitable in VANET because of its inflexibility to modify its radiation pattern. An array of antennas systems increases the system capacity by focusing on the desired node making use of appropriate control algorithms and thereby nulling the radiation pattern in the direction of the undesired node. A smart antenna system is integration between array antenna elements and digital signal processing techniques. Array signal processing involves the manipulation of signals induced on the elements of an array antenna.

The signal processing technique uses a combination of two algorithms, a direction of arrival (DoA) algorithm, and an adaptive beamforming algorithm. The DoA algorithm calculates the direction of arrival of all incoming signals. Then, the adaptive beamforming algorithm is used to update the system parameters. The weights of each element change the phase shift and amplitude attenuation of the received signal so that the main beam is steered toward the desired signal direction and nulls are placed in the directions of the interference [34].

2.3.2 Antenna Beamforming

Beamforming is an advanced signal processing technique that, when employed along with an array of transmitters or receivers, is capable of controlling the 'directionality of' or 'sensitivity to' a particular radiation pattern. It enables focusing the signal from multiple antennas into one strong beam, minimizing energy inside lobes at the transmitter end [35]. At the receiver, beamforming refers to a kind of spatial multiplexing that combines the received signals to add up in a certain direction, and rejecting the signals coming from any other direction, and considering them as interference [36].

In a 5G beamforming is referred to the transmission of a signal in a narrower shape from a transmitter to a receiver in such a way that only the intended user can retrieve the information while rejecting interference from other directions [28]. While transmitting, the main lobe of the antenna pattern is directed towards a certain direction using the phase and amplitude of each antenna element in an array. While receiving, the individual response of each antenna element is combined to get the desired signal in the desired direction. Beamforming is required on both the transmitter side and receiver side. when it is done on the transmitter side it is called transmit beamforming and when it is done on the receiver side it is called receive beamforming.

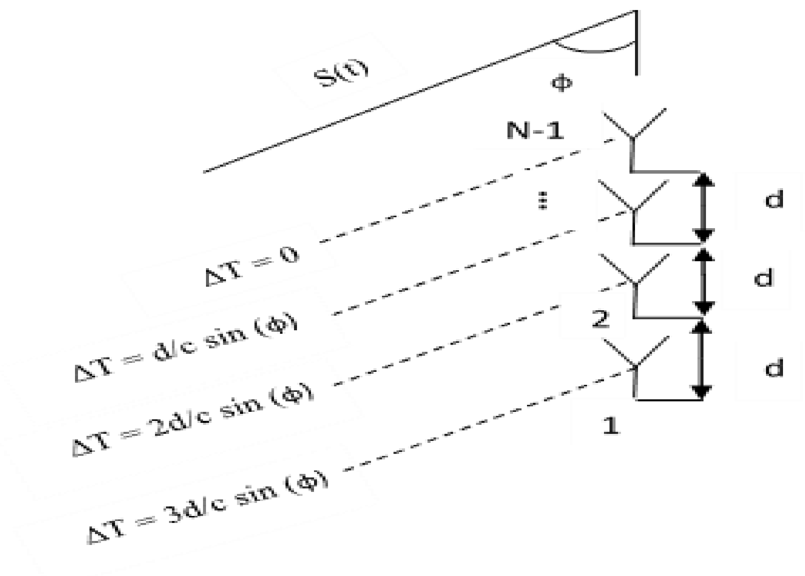


Figure 2.7: Relationship between DoA of signal and time delay

In a uniform linear array, elements are fed with currents of equal magnitude and having a uniform progressive phase shift along the line. The pattern of such an array can be obtained as before by adding vectorially the field strengths due to each of the elements.

Beamformers, in general, require knowledge of the direction of arrival (DOA) of the desired signal or the time delay caused by the DOA and transmit channel characteristics. Direction-of-arrival (DOA) algorithm plays a crucial role in smart antenna system to ensure that the antenna array can estimate the direction of the incoming signal and thus, with the aid of adaptive beamforming, point the array beam towards the estimated direction [38, 39, 7].

2.4 Related Works

Traditional security has been focused on the higher layers of communication networks, rather than the physical layer. For data confidentiality, encryption is the primary scheme of ensuring secrecy, which works well in most current systems. However, in emerging wireless networking architectures, issues of key management or computational complexity cause the implementation of data encryption to be difficult [40]. For wireless ad hoc networks, with the number of devices involved, information may be transmitted through many intermediate nodes from the source to the destination, which increases the probability of losing a key.

The achievable secrecy rate for cell free massive multiple-input multiple outputs in the presence of single antenna eavesdropper at physical layer security (PLS) has been widely utilized for secure data transmission by considering the physical properties of the radio channel based on Shannon's theory in [38]. However, the best routing of information is not described in the article.

In [41], a system that combine information on congestion from sensors installed on the road and from inter-vehicle communication through rumor is proposed. A cost function that considers dynamic metrics on segments along with expiry, delay, and uncertainty was also proposed. The main limitation of this approach is how much congestion information on what roads are to be exchanged between 'roadside units and vehicles' and between the vehicles was not clear.

In [42] proactive routing protocols in which tables containing routing information are continuously refreshed by regular receipt of information from neighboring nodes, hence, the route to any destination is already known when needed thereby minimizing the latency is investigated. However, this maintenance of routing tables becomes expensive with the increasing mobility.

In [43] by using reactive routing protocols, a query floods into the network only when a routing path from a certain source to destination is required and the discovered route is stored until the destined node becomes inaccessible. In this case latency is high, however, it avoids unnecessary control messages to be used and the bandwidth required is low. The position-based routing protocols utilize the geographic location of the vehicular nodes to decide the next hop during data transmission [44].

In [14], the authors proposed a method where RSUs on each end of roads calculate passing vehicle's travel time, averages the travel time for a certain number of vehicles, and broadcast the data to other vehicles and traffic information centers. To calculate the travel time for a road segment, a bidirectional communication scheme between the vehicles and RSU is established. Also, vehicle OBUs are underutilized since they do not perform route planning and travel time calculation of their own as RSU does that processing on vehicles' behalf.

In [45], the author Performed a comparative analysis of on-field measurements of four different antenna types (monopole antenna, patched antenna, a dipole antenna, and Yagi antenna) for vehicular networks. The radiation patterns show that the correlation of the received signals is dependent on the mobility of vehicles concerning a particular RSU.

CHAPTER THREE

3. SYSTEM MODEL

3.1 Introduction

In this research work, a related secondary source of data from different books and previous research on security, wireless routing and, massive antenna system was revised. Based on the literature review, the methodology undertaken in this study to improve the secrecy and routing of VANET is as follows:

3.2 Materials

In this thesis, a MATLAB/R2014a MEX file package software is used for the simulation. The MATLAB version of the packages necessary for VANET simulation.

3.3 Methods

Arising from the research gap in previous research on routing and security of information transmission in VANET, different algorithms are developed to overcome those problem in this research work. The system model and the process flow of the algorithm is given at the end of this chapter.

3.3.1 System Design

In the thesis, first shortest path algorithm best fit the vehicular ad hoc network routing algorithm is developed by combining the Bellman-Ford and Dijkstra shortest path routing algorithms after collecting the network topology of VANET. The algorithm is selected for maintainability and simplicity. The network topology is collected by steering the beam in all directions using DoA estimation. After the shortest path is found by applying a hybrid algorithm re-checks the presence of eavesdropper between the source and next node using the min norm algorithm. Then it uses the beamforming technique to send the main beam to the desired node while put null in the direction eavesdropper. Finally, the quality of transmitted information sent to destination is checked with LMS algorithm to improve the Signal to Noise Ratio (SNR).

3.4 Shortest Path Routing (SPR)

Discovering an efficient VANET routing protocol is needs to meet its highly dynamic feature, and challenges of the information in the network send from vehicle to vehicle that is moving with speed and also the increasing and decreasing density of vehicles. Each link has a cost associated with it in each direction, define the cost of a path between two nodes as the sum of the costs of the links traversed.

Travel time is based on the lowest delay value, in this case, the fastest route rather than the shortest one is considered. The fastest route is the path through which the vehicle can reach its destination or next node with minimum travel time from single source. Node count and travel distance is based on the number of vehicles while travel distance is the basic criterion for shortest path finding. The Bellman and Dijkstra algorithms depends on finding the single source shortest path searching of the route from the source location to the next node or destination. In this vehicular communication, Vertex is considered as node where the edge is link connecting the node.

Dijkstra Algorithm: It is a process of finding the path with the lowest cost from source node to all other nodes. It determines the shortest path based on the cost or distance calculation between the two nodes. It is finding the shortest paths from a given source node to all other nodes by developing the paths in order of increasing path length.

G = set of nodes in the network

S = source node

Z = set of nodes so far incorporated by the algorithm

T = number of links available

G = (Z, T)

Proceeding S in stages, by the *Kth* stage, the shortest path *S* to *k* nodes closest to (least cost way from) the source node will be determined that is these nodes are in a set Z. At stage *(k+1)*, the node not in G that has the shortest path from the source nodes is added to Z. As each node is added to Z, its path from the source is defined.

W (i, j) = low cost from node i to node j; *w (i, i) =0; w (i, j)* =∞ if the two nodes are not directly connected; *w (i, j)* ≥*0* if the two nodes are directly connected because the algorithm assign the current cost value of the source node plus the cost value of the next no.

L(n) = cost of the least-cost path from node *S* to node *G* that is currently known to the algorithm. This is the cost of the least-cost path of the graph from *S* to *N*.

The algorithm has three steps.

Step 1. [Initialization] $Z = \{S\}$

The initial path cost to the neighbouring nodes is simply link cost which means L(n) = w (s, n) for $n \neq s$

Step 2 [Get Next Node] find $x \notin Z$ such that L(x) = minL(j)

Step 3: [update least-Cost Paths]

L(n) = *min [L(n), L(x) + w (x, n)]* for all n different from Z. If the latter term is the minimum, the path from S to n is now the path from *S* to *x* concatenated with the edge from *x* to *n*.

The algorithm terminates when all nodes have been added to Z. At termination, the value *L(x)* associated with each node x is the cost (length) of the least cost path from *s* to *x*. Also, Z defines the least cost path from S to each other node. One iteration of steps 2 and 3 adds one new node to Z and defines the least cost path from S to that node. That path passes only through nodes that are in Z. To see this, consider the following line of reasoning. After k iterations, there are k nodes in Z, and the least cost path from S to each of these nodes has been defined. Now consider all possible paths from S to nodes, not in Z. Among those paths, there is one of the least costs that passes exclusively through nodes in Z end with a direct link from some node in Z to a node, not in Z. This node is added to Z and the associated path is defined as the least-cost path for that node.

Step 2 and 3 in the algorithm are repeated until Z = G or until final paths have been assigned to all nodes in the network.

Bellman-Ford Algorithm: This determines the shortest path based on the number of nodes or vehicles. It finds the shortest paths from every source node to a particular destination node. This works when the arc length is negative. It can be stated as finding the shortest paths from a given source node subject to the constraint that the paths contain most one link, then find the shortest paths with a constraint of paths at most two links, and so on. This algorithm also proceeds in 3 different stages.

S = source node

W (I, j) link cost from node I to node j: w (I, j) = 0 if the node is directly connected, w (I, j) = ∞, where the node is not directly connected.

m= maximum number of links in a path at the current stage of the algorithm

$L_{m(n)}$ cost of the least path from node m to node n under the constraint of no more than m links.

1. [Initialization]

$L_{m(n)} = \infty$, for all n different from s

$L_{m(n)} = 0$ for all m

2. [Update]

For each successive m ≥ 0; For each n different from s, compute

$L_{m+1}(n) = \min[L_m(j) + w(j, n)]$

Connect n with predecessor node j that achieves the minimum and eliminate any connection of n with a different predecessor node formed during an earlier iteration. The path from s to n terminates with the link from j to n.

For iteration of step 2 with *m=k* and each destination node, the algorithm compares potential paths from *s* to n of length *k+1* with the path that existed at the end of the previous iteration. If the previous, shorter, path has less cost, then that path is retained.

Otherwise, a new path with length *K+1* is defined from s to n; this path consists of a path of length k from *s* to some node *j*, plus a direct node from node *j* defined in the previous iteration.

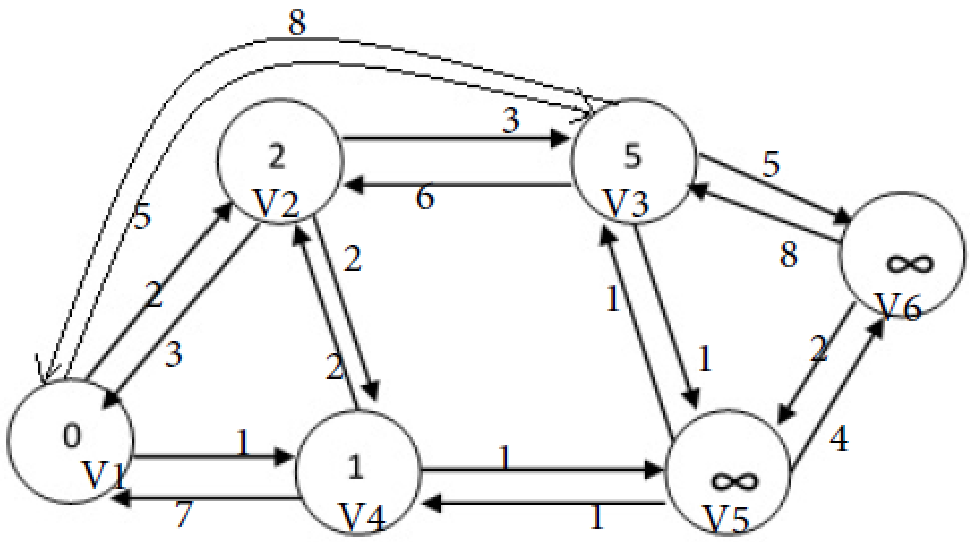


Figure 3.1 VANET Shortest path routing topology

The list cost routing algorithm for Bellman and Dijkstra in above figure is

Dijkstra and Bellman algorithm routing table considering V1 as source node and V6 as a destination node.

Table 3.1: Routing table: (a) Dijikstra (b) Bellman

Iter.	G	L	Path	L3	Path	L4	path	L5	path	L6	path
1	{1}	2	(1-2)	5	(1-3)	1	(1-4)	∞	-	∞	-
2	{1,4}	2	(1-2)	4	(1-4-3)	1	(1-4)	2	(1-4-5)	∞	-
3	{1,2,4}	2	(1-2)	4	(1-3-4)	1	(1-4)	2	(1-4-5)	∞	-
4	{1,2,4,5}	2	(1-2)	3	(1-4-5-3)	1	(1-4)	2	(1-4-5)	4	(1-4-5-6)
5	{1,2,3,4,5}	2	(1-2)	3	(1-4-5-3)	1	(1-4)	2	(1-4-5)	4	(1-4-5-6)
6	{1,2,3,4,5,6}	2	(1-2)	3	(1-4-5-3)	1	(1-4)	2	(1-4-5)	4	(1-4-5-6)

(a)

k	L_k2	Path	L_k3	Path	L_k4	path	L_k5	path	L_k6	path
0	∞	(-)	∞	(-)	∞	(-)	∞	-	∞	-
1	2	(1-2)	5	(1-3)	1	(1-4)	∞	(-)	∞	-
2	2	(1-2)	4	(1-4-3)	1	(1-4)	2	(1-4-5)	10	(1-3-6)
3	2	(1-2)	3	(1-4-5-3)	1	(1-4)	2	(1-4-5)	4	(1-4-5-6)
4	2	(1-2)	3	(1-4-5-3)	1	(1-4)	2	(1-4-5)	4	(1-4-5-6)

(b)

Hybrid Algorithm: It is the combination of the Dijkstra and Bellman-Ford algorithm that can calculate an initial best route from the original vehicle node to its desired next node. Again, it re-calculates the best route due to an update in link failure. whenever the link failed it checks for update of nearby node other wise the vehicles carry on forwarding the information.

In Bellman, step 2 above the calculation for node n involves knowledge of the link cost to all neighboring nodes to node n. Each can maintain a set of costs and associated paths for every other node in the network and exchange this information with its direct neighbors from time to time. In step3 Dijkstra algorithm on other hand appears to require that each node must have complete topological information about the network. that is each node must know the link cost of all links in the network. Thus, for this algorithm information must exchange with all other nodes. In general evaluation of the relative merits of two algorithms should consider the processing time of the algorithms and the number of information that must be collected from other nodes in the network.

3.4.1 Complexity Comparison of Bellman and Dijkstra Algorithm

Time complexity of Bellman-Ford when it does not use priority queue is $(\lfloor L \rfloor)[N]-1$

N = number of nodes

L = number of links

O = order

$0([L])[N]$

$O(N^2)$

If there is a complete graph then the total number of links are: $(N(N-1)/2)$ and requires $(N-1)$ time or iteration. The complexity $(N(N-1)/2) * \ (N-1) = O(N^3)$. But in Dijkstra algorithm For N number of nodes, the N node must be checked. So, the time complexity of Dijkstra algorithm is $O[N^2]$. The complexity of Bellman Ford algorithm is greater than that of Dijkstra.

When the link connecting the nodes is positive, Dijkstra's algorithm solves the shortest path problem with fewer computations. But if the topology has negative links Bellman Ford algorithm is appropriate instead of Dijkstra. The running time of Bellman is $O(V^2)E$ and that of Dijkstra is $O(N^3 + NE)$

3.5 Antenna Beamforming Technique for Secure Routing

The radiation pattern of an antenna is somewhat wide and offers low directivity. We need directive antennas to be designed for specific applications to have hassle-free long-distance communication. We can achieve this by increasing the size of the antenna or by forming an array of radiating elements. The antenna formed by several radiating elements is called an array. The vector addition of the fields radiated by every single element of the array gives the total field. When the fields from the elements interfere constructively adding up each other giving rise to radiation pattern in the desired direction and interfere with destructively canceling each other giving rise to nulls in the undesired direction.

Usually, the signals received at the different antennas are multiplied with complex weights and then adaptively weights are summed up. There are two types of smart antennas, viz., switched (fixed beamformer) beam smart antenna, and adaptive smart antenna. In switched beam smart antenna, the antenna system has several fixed beam patterns. But for vehicular communication adaptive smart antenna is appropriate. Because beam can be steered in any direction according to DoA estimation and at the same time null can be generated in the direction of the interferer.

Adaptive beamforming algorithms compute the weights by minimizing the error between the array output and the desired signal until the weights reach their optimum values. The direction control of the signal is done by adjusting the weights of the signal phase amplitudes of multiple antennas.

3.5.1 Adaptive Antenna Array

A smart antenna is an array antenna that uses adaptive beamforming algorithms to steer the main beam toward the desired signal direction and reject the interfering signals of the same frequency from other directions without moving the antenna. An antenna array is a system of similar antennas oriented similarly to get greater directivity in the desired direction. One of the most significant features of the system is it can reject any strong interference which is coming from a different source of transmission. The rejection is performed using a set of feedback loops so that the radiation pattern of the antenna system may have a deep null in the direction of the interference.

Signal processor consisting of multichannel tapped delay lines with variable weights. A certain constraint is imposed on these weights utilizing the equip phase relation of the desired signal component and the weights are controlled through feedback loops so that the system may cancel the interference component.

The general array output is given by

$$y = \tilde{\omega}^H.\bar{\alpha} = \omega_1 e^{-j\kappa d sin\theta}\omega_2 \omega_3 e^{j\kappa d sin\theta} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots [1]$$

Where $\bar{A} = [\bar{\alpha}_{\mathbf{0}}\ \bar{\alpha}_{\mathbf{1}}\ \bar{\alpha}_{\mathbf{2}}]$ matrix of steering vectors

$\tilde{\omega}^H =$ is array weight

The purpose of the beamforming is to generate a beam of a necessary shape and to direct it to the desired location in real-time while suppressing interference. In adaptive array systems, there are no predefined beams, but the antenna diagram changes its shape and direction toward each dedicated vehicle adaptively, providing more degrees of freedom. These techniques are based on the so-called weighting approach. This means that the complex weights $wi\ are$ instantaneously calculated by an adaptive algorithm, to direct the maximum antenna radiation pattern toward the intended vehicle and to steer null toward interference sources. In this sense, adaptive beamforming is an iterative approximation of optimal beamforming. The adaptive antenna array is capable of adapting to the varying signal environments automatically and forms beams in the directions of the desired signals by steering nulls in the directions of interfering signals. Elements are fed with a current of equal magnitude with uniform progressive phase shift along the line. The DOA algorithm calculates the direction of arrival of all incoming signals. Then, the adaptive beamforming

algorithm is used to update the system parameters $\tilde{\omega} = [\omega_1\, \omega_2\ \dots\ \omega_M]$ .The weights of each element change the phase shift and amplitude attenuation of the received signal so that the main beam is steered to ward the desired signal direction and nulls are placed in the directions of the interference

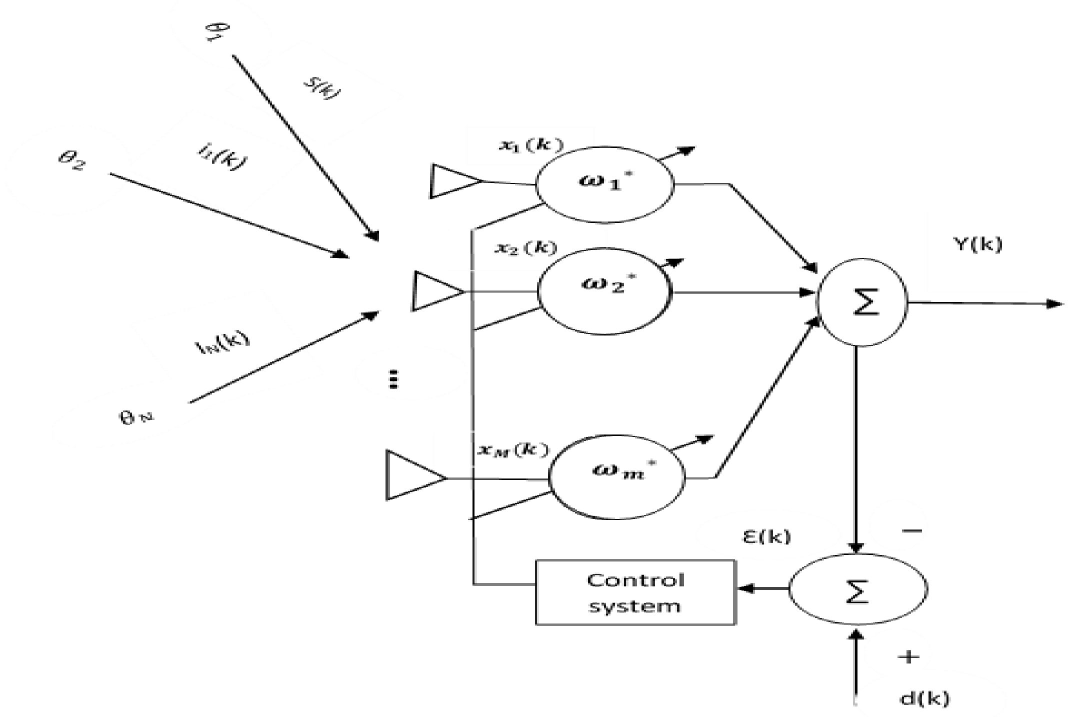


Figure 3.2 : An adaptive beamforming array antenna .

3.5.2 Array Correlation Matrix

The output of adaptive beamformer, at time k, is given by a linear combination of the data at the N antenna elements, can be expressed as: $y(\kappa) = \tilde{\omega}^T . \ddot{x}(\kappa)$

The superscript T denotes transpose, the received signal vector is

$$\ddot{x}(\kappa) = \bar{\alpha}_0\, S(k) + ([\bar{\alpha}_0\ \bar{\alpha}_1\ \ \dots \bar{\alpha}_N] . \begin{bmatrix} i_1\,(k) \\ i_2\,(k) \\ \vdots \\ i_N(k) \end{bmatrix} + \acute{n}(\mathrm{k}) \quad \dots\dots\dots\dots\dots\dots\dots\dots \quad [2]$$

$\ddot{x}_s(k)$ = desired signal weights

$\ddot{x}_i(k)$ = interfacing signal vector

$\acute{n}(\mathrm{k})$ = zero mean Gaussian noise for each channel

$$y(k) = \tilde{\omega}^H . [\ddot{x}_i(k) + \acute{n}(\mathrm{k})] \qquad [3]$$

$$= \tilde{\omega}^H . [\ddot{x}_s(k) + \bar{u}(k)\ ] \qquad [4]$$

To optimize the element weights, we seek to minimize the mean squared error between the array output and the reference signal d(t).

$$W_{opt} = {R_{xx}}^{-1} r_{xd} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [5]$$

Where $R_{xx} = x(k)x^T(k)$ is the signal covariance matrix and $r_{xd} = d^*(k)$x(k)

The adaptive beamforming algorithms compute the weights by minimizing the error between the array output and the desired signal until the weights reach their optimum values.

3.5.3 Minimum Variance Distortion Less Response (MVDR) Beamformer

This algorithm ensures that the signal from desired direction remain undistorted by the eavesdropper. The formed beam pattern concentrates or targeted to the DoA of interest.

From the weighted array out put $y(k) = \tilde{\omega}^T . \ddot{x}(\kappa) = \tilde{\omega}^H . \bar{\alpha}_0 S(k) + \tilde{\omega}^H \hat{u}$, for distortion less response $\tilde{\omega}^H \bar{\alpha}_0$ must be 1.

$$y(k) = S(k)\tilde{\omega}^H . \hat{u} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [6]$$

Hence the expected value of $y(k)$ becomes $[y(k)] = S(k)$, From this the variance of $y(k)$ is formulated as:

$$\sigma^2 \, MV = E[|\tilde{\omega}^H \, \ddot{x}(\kappa)|^2] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [7]$$

3.5.4 Min norm DoA Estimation

For linear arrays if the min norm represented by MN

$$\mathrm{MN} = \frac{(\hat{u}^T \bar{E}_N {\bar{E}_N}^H \hat{u}_1)^2}{\left|\bar{a}(\theta)^H \bar{E}_N {\bar{E}_N}^H \hat{u}_1\right|^2} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [8]$$

Where $\bar{a}$ = array steering vector

$\bar{E}_N$ = subspace of M-S eigen vectors

M = number of array antenna elements

S = number of arriving signals

$\hat{u}_1$ = Cartesian basis vectors

3.5.5 LMS Adaptive Beamforming Algorithm

The least mean square is an adaptive algorithm that produces the least mean squares of the error signal (the difference between the desired and the actual signal. It is a gradient method of steepest descent based on the error at the current time, where the iterative procedure is used making successive corrections to the weight vector in the direction of the negative of the gradient vector which eventually leads to the minimum mean square error. The weights that minimize the mean squared error in the output signal, where the error is the difference between the output signal and a reference signal**,** which ideally is the transmitted information which also maximizes the SNR. If $d(k)$ is a reference signal sampled at the output instant k and correlated with the desired signal $\ddot{x}(k)$ then the error signal is $\boldsymbol{\varepsilon}(\boldsymbol{\kappa})$ **is**

$$\boldsymbol{\varepsilon}(\boldsymbol{\kappa}) = d(k) - \tilde{\omega}^H(k)\ddot{x}(k) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots. [9]$$

The squared error is given as

$$D = E[|d|]^2 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots.\dots\dots\dots\dots.\dots\dots.. \quad [10]$$

$$\tilde{\omega}_{opt} = \hat{R}_{xx}{}^{-1}\,\hat{r} \qquad \dots\dots\dots\dots\dots\dots.\dots\dots\dots\dots\dots\dots\dots.. \quad [11]$$

$$\hat{r}(k) \approx d^*(k)\ddot{x}(k) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad [12]$$

$$\tilde{\omega}(k+1) = \tilde{\omega}(k) - \frac{1}{2}\mu\Delta_{\tilde{\omega}}\left(J(\tilde{\omega})\right) \dots\dots\dots\dots\dots\dots\dots..\dots\dots.... \quad [13]$$

$$\tilde{\omega}(k+1) = \tilde{\omega}(k) - \mu\left[\hat{R}_{xx}\tilde{\omega} - \hat{r}\right] \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots.. \quad [14]$$

$$= \tilde{\omega}(k) + \mu e^*(k)\ddot{x}(k) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots.. \quad [15]$$

$$e(k) = d(k) - \tilde{\omega}^H(k)\ddot{x}(k) \quad = error\ signal \dots\dots\dots\dots\dots\dots\dots\dots\dots \quad [16]$$

Where in $\tilde{\omega}^H$ H denotes Hermitian (complex conjugate) transpose, and μ is the step size.

For uniform linear antenna array with an interelement spacing of '$d\alpha\theta$'. Antennas are excited with a progressive phase shift of α, The array factor for N element linear array is:

$$AF = \sum_{n=0}^{N=1} A_n{}^{jn\frac{2\pi d}{\lambda}cos\theta+\alpha} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad [17]$$

Where to generate the main beam at wavelength λ to ward the desired beam direction θ^0 from the broadside direction, the progressive phase shift is

$$\alpha = \frac{-2\pi d}{\lambda} cos\theta^0 \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots.. \quad [18]$$

3.6 System Model for Hybrid secure Routing

Node that receives information is called the destination (d), and the other node is called the eavesdropper (e). Source node(s) transmits information to relay node. Here the relay is equipped with M antennas elements. Since the signal sent to both receivers needs to be forwarded by the relay, and the relay may ask them to feedback Channel State Information (CSI), and assume that the relay can obtain all the CSIs. The noise at any node is assumed additive white complex Gaussian noise with zero-mean and variance in this consideration. Some group of the relay antenna receives the confidential information, while the other group receives signals and converts them into energy and also identify the eavesdropper direction.

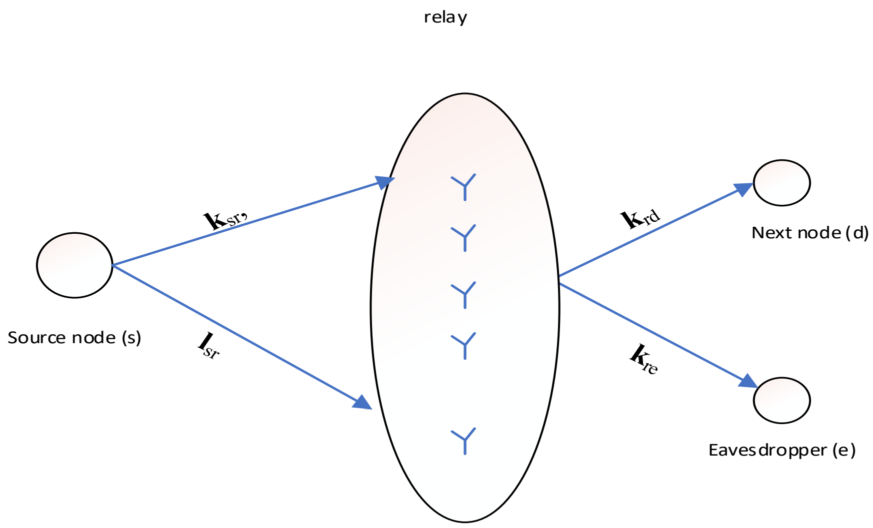


Figure 3.3: System Model for Hybird Secured Routing

3.6.1 Hybrid Routing Information Secrecy Analysis

The simulation results were carried out varying the number of antenna number for different beamforming algorithm considering total M = 64 number of antennas used in the relay. It is then subdivided N and K, where each contains 32 antenna arrays. The K antenna further sub divided to L and I, each contains 16 antenna arrays so that, M = N + K = N+K+I. the Antenna in the subset of N used to relay information, where antenna in the subset of K used to beamforming. The channel coefficient vector between the source and the antennas in the subset is denoted as $\mathbf{k}_{sr}$, while the channel coefficient vector between the source and the antennas in the subset ***N*** as $\mathbf{l}_{sr}$. The channel coefficient vectors from the antennas in the subset K to the destination and the eavesdropper are denoted by $\mathbf{k}_{rd}$ and $\mathbf{k}_{re}$, respectively.

In the first stage, the source transmits symbol ***x*** with unit power, i.e., $\boldsymbol{E}[|x|^2] = 1$, where ***E*** [.] denotes expectation. The source has a transmit power constraint P_s. The received signal of the relay can be expressed as:

$$y_r = \sqrt{Ps}k_{sr}x + n_r \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [19]$$

Where, $nr \sim CN(0, \sigma^2 I_N)$ are the additive noise in the channel. The received signal of the $i-th(i = 1,2, \ldots, M-n)$antenna in the subset $\boldsymbol{N}$ can be expressed as:

$$r_i = \sqrt{P_s} I_{sr} x + n_r \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots .. \ldots \ldots \ldots \ldots \ldots \ldots ..[20]$$

Assume that the signal is converted to energy with the efficiency of α, and. $\alpha \epsilon (0,1)$ as the harvested energy is also used in the relay, the total power of forwarding signals in the second stage will be:

$$P_{r'} = P_r + P_r \alpha \sum_{i=1}^{M-N} |r_i|^2 \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots [21]$$

$$= P_r + \alpha \sum_{i=1}^{M-N} (P_s |I_{sr}|^2 + \sigma^2) \ldots \ldots \ldots \ldots \ldots \ldots \ldots .. \ldots \ldots \ldots \ldots \ldots \ldots ....[22]$$

$$= P_r + \alpha P_s \|I_{sr}\|^2 + \alpha (M-N) \sigma^2 \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots . \ldots \ldots \ldots \ldots \ldots \ldots ..[23]$$

In the second stage, the relay forwards information by the antennas in the subset N. The transmitted signal of the relay is denoted by, $x_r = W_{yr}$where $\boldsymbol{W}$ is a diagonal matrix composed of a beamforming vector

$\omega = [\omega_{1,} \omega_1 \ \ldots, \omega_N]^T$ i.e., $W = diag(\omega)$, i.e., $\mathbf{x}_r$ can be rewritten as:

$$x_r = W_{yr} = \sqrt{P_s} W k_{sr} x + W_{nr} = \sqrt{P_s} diag(k_{sr}) \omega x + diag(\omega) n_r \ldots \ldots \ldots \ldots \ldots \ldots .. [24]$$

The received signals at the destination and the eavesdropper are:

$$y_d = {k_{rd}}^T x_r + n_d = \sqrt{P_s} {k_{rd}}^T diag(k_{sr}) \omega x + {n_r}^T diag(h_{rd}) \omega + n_{d.} \ldots \ldots [25]$$

$$y_e = {k_{re}}^T x_r + n_e = \sqrt{P_s} {k_{re}}^T diag(k_{sr}) \omega x + {n_r}^T diag(k_{re}) \omega + n_e \ldots \ldots .. [26]$$

where the superscript T denotes matrix transpose, n_d and n_e, respectively, represent the noise at the destination and the eavesdropper. The SNRs (Signal to Noise Ratios) at the destination and the eavesdropper can be calculated as:

$$\gamma_{rd} = \frac{P_s \omega^H diag({k_{sr}}^*) {k_{rd}}^* {k_{rd}}^T diag(k_{sr}) \omega}{\sigma^2 \omega^H diag({k_{rd}}^*) diag(k_{rd}) \omega + \sigma^2} \ldots \ldots \ldots \ldots \ldots \ldots . \ldots \ldots \ldots [27]$$

$$\gamma_{re} = \frac{P_s \omega^H diag(k_{sr}^*) k_{re}^* k_{re}^T diag(k_{sr})\omega}{\sigma^2 \omega^2 diag(k_{re}^*) diag(k_{re})\omega + \sigma^2} \ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots\ldots\ldots\ldots[28]$$

The secrecy rate is defined as a max, $\{R_d - R_e, 0\}$where R_d and R_e are, respectively, the rates at the destination and the eavesdropper.

$$R_d = \frac{1}{2}\log(1+\gamma_{rd})\, and R_e = \frac{1}{2}\log(1+\gamma_{re}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..[29]$$

Thus, the secrecy rate is:

$$R_s = \frac{1}{2}\log(1+\gamma_{rd}) - \frac{1}{2}\log(1+\gamma_{re}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..[30]$$

3.6.2 Hybrid Secure Routing Process Flow

The routing of information from the source node to the next node or destination follows the following four steps.

1. The source node checks the availability of a nearby node to send the required information. Using the min norm algorithm, it scans the direction of arrival available neighbor nodes to construct VANET topology to prefer the shortest secure route.
2. From the constructed VANET topology it selects the shortest path applying whether Bellman-Ford or Dijkstra depending on the number of links and nodes available.
3. Then the presence of an eavesdropper is checked before sending the signal along the selected route. If the eaves dropper does not find in the route selected it sends the message, otherwise it applies min norm beamforming algorithm to steer the antenna pattern towards the intended node and null the direction of the eavesdropper identified.
4. Finally, the LMS algorithm is applied to improve the SNR or signal quality that can be deteriorated from interferences and sends to the destination node.

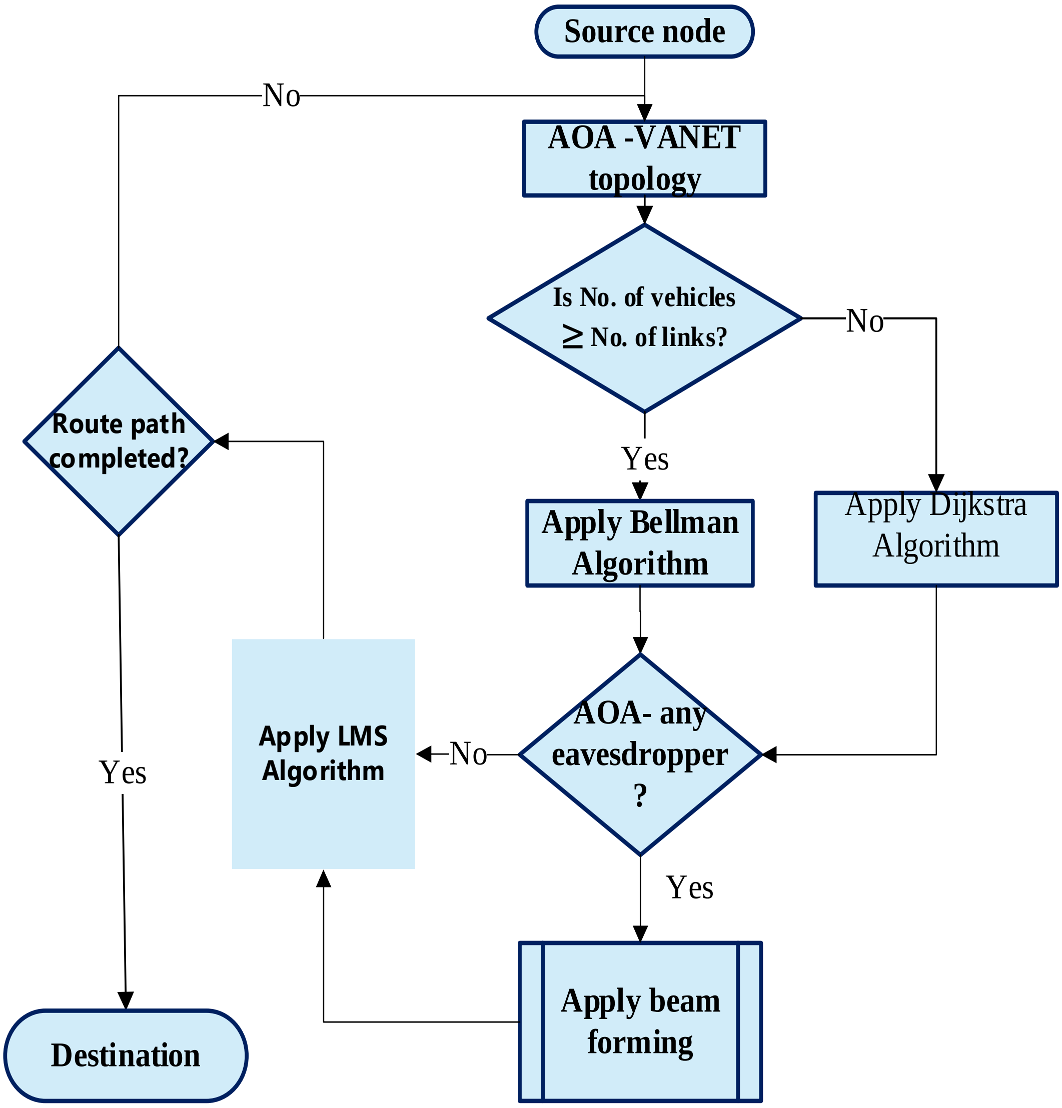


Figure 3.4: Flow chart of the overall system

CHAPTER FOUR

4. RESULTS AND DISCUSSIONS

In this section different parameters are given for simulation in the form Table and the result is briefly explained. Different antenna subset is used for relaying information and beamforming technique considering 64 total number of the antenna array in the relay.

Min norm algorithm for topology identification: To identify the direction of arrival of all incoming signal neighbour to the source node, the min norm algorithm is used.

Table 4.1: Parameters used in Min norm algorithm for identifying network topology.

Number of antenna elements	L = 16
Antenna Elements separation	0.5 λ
No of intended signals	3
The angle of arrival of signal of nearby nodes	-10°,5°,25°

Based on the parameter listed in table 4.1 above, the simulation is carried out and the following direction of arrival of the three signal is obtained. By beam steering or scanning of signal around 360° the dynamic network topology of VANET identified that there is arrival of the signal at different angle.

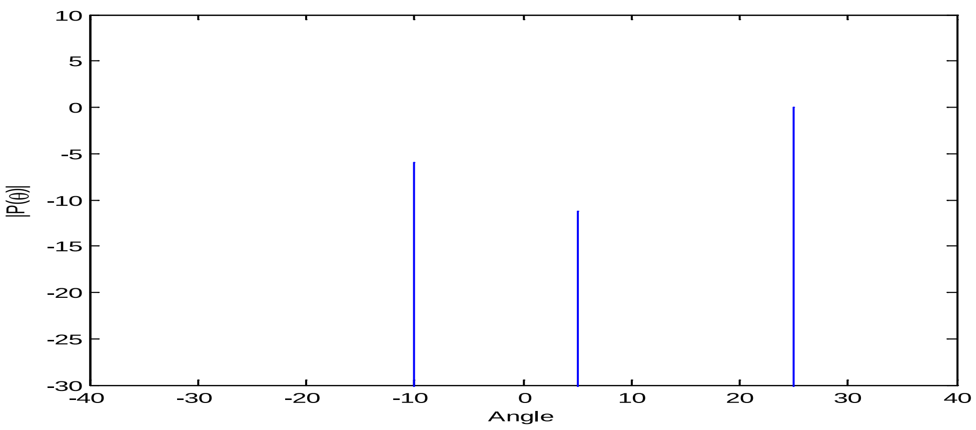
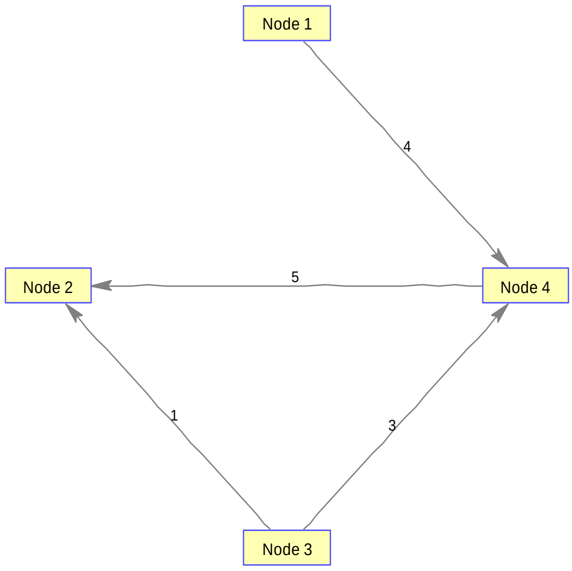


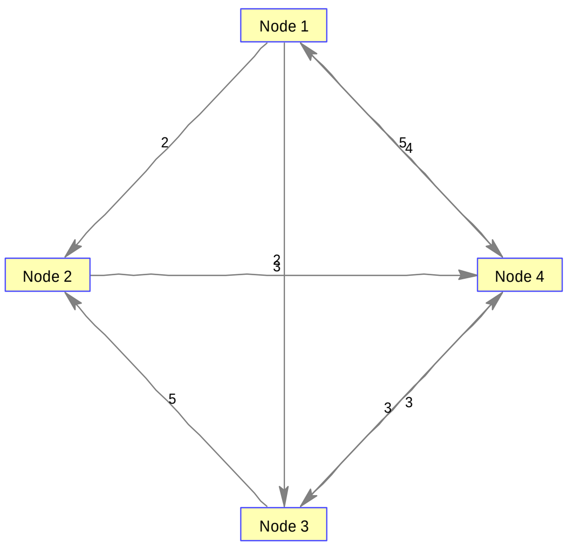
Figure 4.1: The DoA of three neighbour nods

The three signals are identified by steering the beam direction 360° using min nor algorithm. Those signals of interest are identified as coming from angle of -10°,5° and 25°.

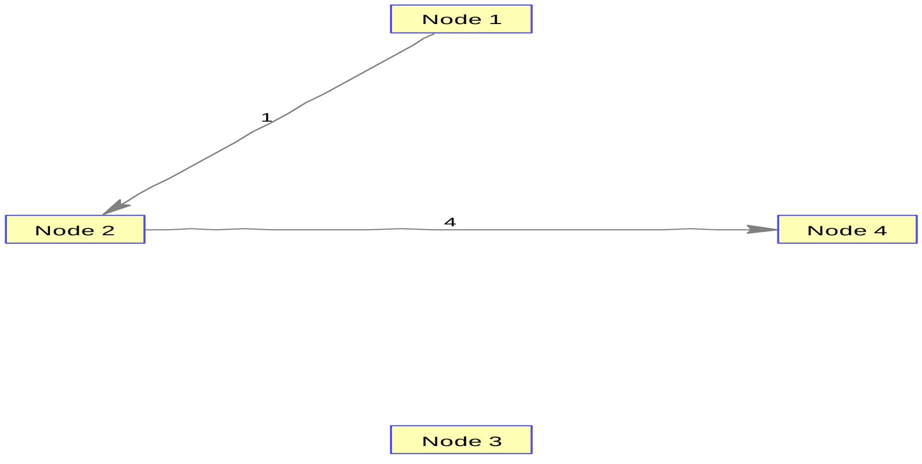
VANET network topology: Three signals nearby the source node links each other and form network topology. The following four node topology is constructed from the source node the other three nodes identified using the min norm algorithm.



(a)



(b)



(c)

Figure 4.2: Number of links for four vehicles:(a) 4-link,(b) 8-link,(c) 2-link

As shown in the above figure the number of links changes dynamically results in a network topology change. The number of links figures above are4,8 and 2 in (a), (b), and (c) respectively. The varies in link number is arise from vehicular node movements. So, based on the number of link hybrid Bellman and Dijkstra algorithm is applied. The cost value based on distance and time taken is given in table below:

Table 4.2: Cost value for Bellman and Digistra algorithm for four vehicle nodes

a = Bellman

0	1	∞	5
∞	0	∞	∞
∞	1	0	3
∞	5	∞	0

b = Dijkstra

0	2	2	5
7	0	6	3
7	5	0	3
4	6	0	3

c = Bellman

0	1	∞	5
∞	0	∞	4
∞	∞	0	∞
∞	∞	∞	0

The cost value shows Bellman Ford algorithm is efficient for link numbers less than or equal to number of nodes, while Dijkstra algorithm is best while link available is grater than the number of nodes.

Hybrid Dijkstra and Bellman routing: VANET topology may be more complex around a junction or intersection area. Hybrid Bellman and Dijkstra algorithm calculate the shortest path in which information can be routed. Six vehicles at intersection area may create the following topology.

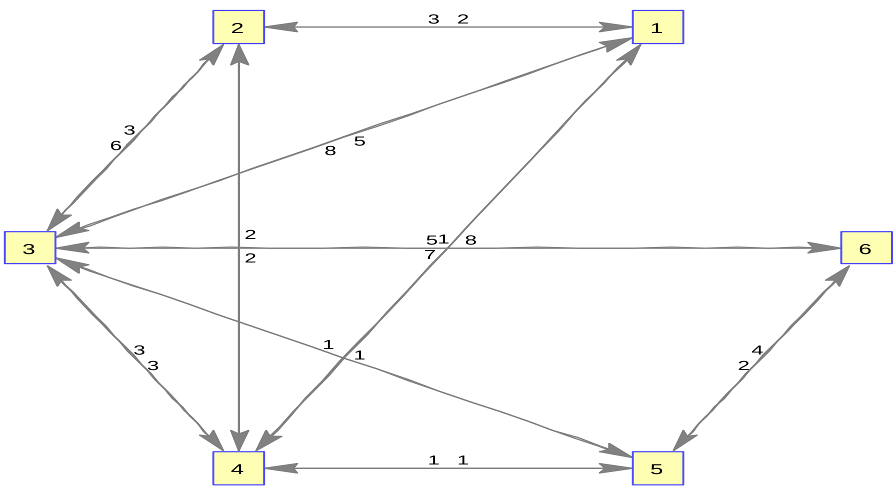


Figure 4.3: VANET toplogy for 6 nodes

Let say the 1st vehicle (source node) needs to send information to 6th vehicle (destination node). In this case the source node checks the nearby node and create a link based on the link cost.

Table 4.3: Cost value of Digistra and Bellman algorithm

Dijkstra cost

0	2	1	3	2	4
3	0	2	3	3	5
7	4	2	0	1	3
5	2	0	2	1	3
6	3	1	1	0	3
10	7	5	5	4	0

Bellman cost

0	2	3	1	2	4
3	0	3	2	3	5
7	4	0	2	1	3
5	2	2	0	1	3
6	3	1	1	0	2
10	7	5	5	4	0

The Digistra algorithm does not work with negtive edge weights. In the table given above the column refers nodes where the row refers link that connect two nodes. The node cost value is updated based on its own previous value and the cost of vistied node. Then visited node incorporated to the source node in continous iteration. This process continues until the 6th node is visited and information reached the destination. By running the program the following routing table is obtained.

Table 4.4: Routing table for Dijkstra and Bellman Algorithm

Dijkstra

1	2	0	0	0	0
1	4	5	3	0	0
1	4	0	0	0	0
1	4	5	0	0	0
1	4	5	6	0	0
2	1	0	0	0	0
2	0	0	0	0	0
2	3	0	0	0	0
2	4	0	0	0	0
2	4	5	0	0	0
2	4	5	6	0	0
3	5	4	2	1	0
3	5	4	2	0	0
3	0	0	0	0	0
3	5	4	0	0	0
3	5	0	0	0	0
3	5	6	0	0	0
4	2	1	0	0	0
4	2	0	0	0	0
4	5	3	0	0	0
4	0	0	0	0	0
4	5	0	0	0	0
4	5	6	0	0	0
5	4	2	1	0	0
5	4	2	0	0	0
5	3	0	0	0	0
5	4	0	0	0	0
5	0	0	0	0	0
5	6	0	0	0	0
6	5	4	2	1	1
6	5	4	2	0	0
6	5	3	0	0	0
6	5	4	0	0	0
6	5	0	0	0	0
6	0	0	0	0	0

Bellman

1	0	0	0	0	0
1	2	0	0	0	0
1	4	5	3	0	0
1	4	0	0	0	0
1	4	5	0	0	0
1	4	5	6	0	0
2	1	0	0	0	0
2	0	0	0	0	0
2	3	0	0	0	0
2	4	0	0	0	0
2	4	5	0	0	0
2	4	5	6	0	0
3	5	4	2	1	0
3	5	4	2	0	0
3	0	0	0	0	0
3	5	4	0	0	0
3	5	0	0	0	0
3	5	6	0	0	0
4	2	1	0	0	0
4	2	0	0	0	0
4	5	3	0	0	0
4	0	0	0	0	0
4	5	0	0	0	0
4	5	6	0	0	0
5	4	2	1	0	0
5	4	2	0	0	0
5	3	0	0	0	0
5	4	0	0	0	0
5	0	0	0	0	0
5	6	0	0	0	0
6	5	4	2	1	0
6	5	4	2	0	0
6	5	3	0	0	0
6	5	4	0	0	0
6	5	0	0	0	0
6	0	0	0	0	0

Based on the result the algorithm source node prefers the shortest path to relay information timely using less energy.

The combined Bellman Dijkstra visit a five node and the spinning tree is determined at the instant of time.

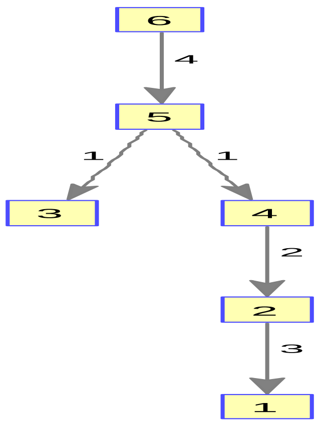
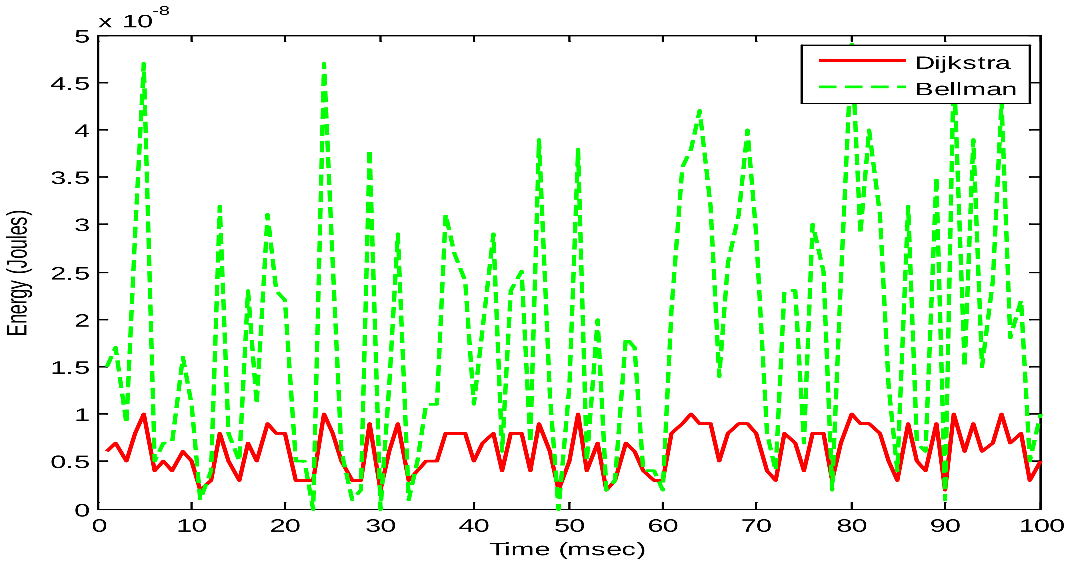


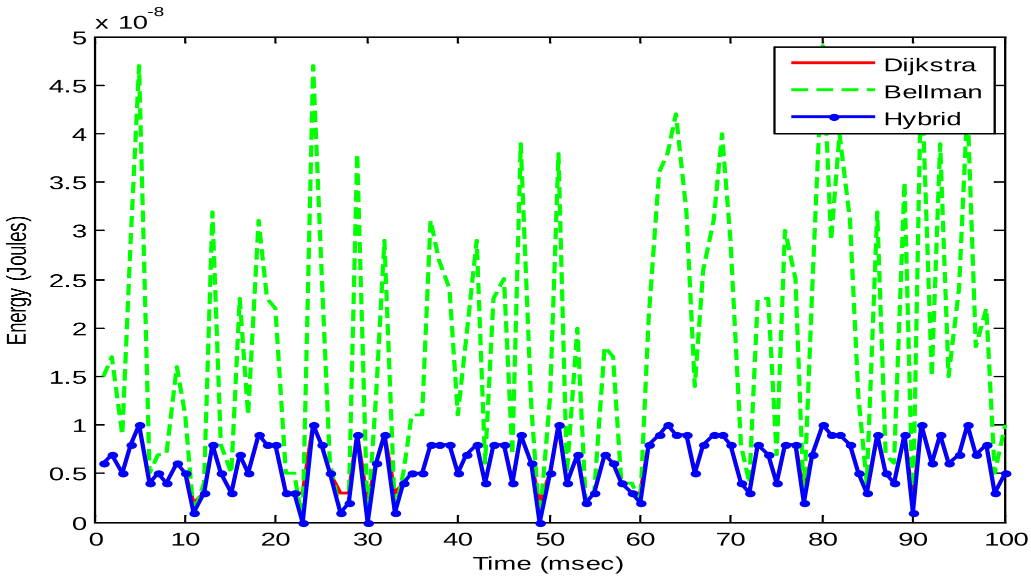
Figure 4.4: Spinning tree of the shortest route

The shortest path is selected applying the Bellman and Dijkstra algorithm alternatively. The spinning tree is taken running the algorithm.

Analysis of energy efficiency in hybrid routing: Combining the Bellman and Dijkstra algorithm the time efficient routing is obtained. This enables the link stability and un interruption of information flow from the source node to the next node which saves energy finding to the new route.



(a)



(b)

Figure 4.5: Energy efficieny Vs time. (a) Bellman vs Digikstra and (b) Hybrid algorithm

The Bellman algorithm use high energy for complex topology because it checks for every node in the topology from time to time. It calculates link cost to neighbor cost and total path cost to the node. On other hand, the Dijkstra algorithm uses less energy for computation. The Dijkstra algorithm do not consider the negative weight in the topology. It requires only the topological information about the network. So, less processing time and less power is utilized by this algorithm.

Table 4.5: Energy comparision of Belman,Digikstra and Hybrid Algorithm in 100ms

time (msec)	Energy (Joule)		
	Bellman	Dijkstra	Hybrid
10	0.15	0.25	0.15
20	3	0.8	0.8
30	0.1	0.35	0.1
40	1	0.5	0.5
50	0.1	0.4	0.1
60	0.35	0.4	0.35
70	4	0.7	0.7
80	0.3	0.4	0.3
90	0.1	0.2	0.1
100	0.2	0.3	0.2

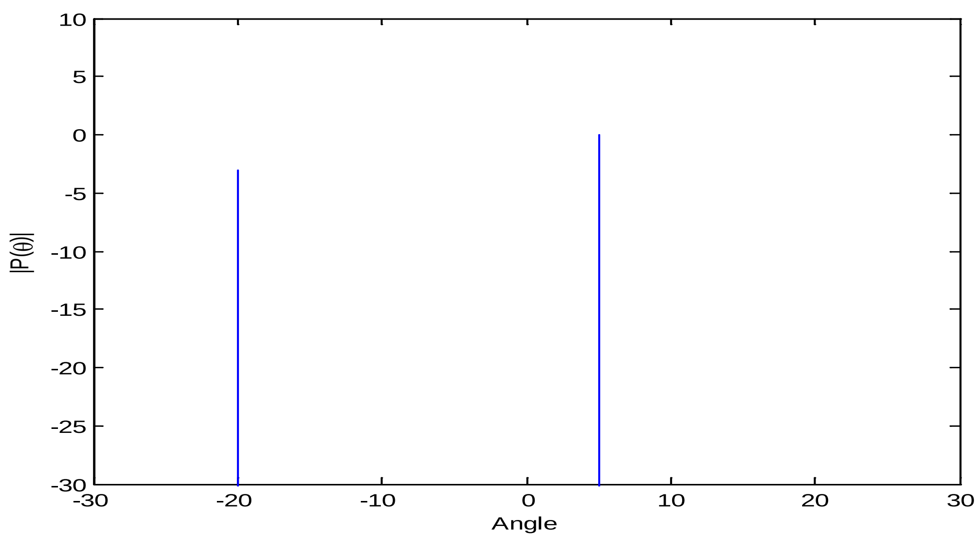
Hybrid routing combines the two algorithm provides efficient routing strategy. Dijkstra algorithm is not effective for negative weight even though its computational speed is faster than that of Bellman.

Secrecy analysis of the hybrid routing: The wireless transmission of information from the source node to the next node vulnerability is improved the array antenna beam forming technique. The presence of eave dropper is again analysed by scanning the incoming using min norm algorithm.

Table 4.6: Parametrs used in Min norm algorithm to identify DoA osf eavesdropper.

Number of antenna elements	I = 16
Antenna Elements separation	0.5 λ
No of incoming signals	2
Angle of arrival of signal of the interest	5°
Angle of arrival of eavesdropper	-20°

Steering the beam direction around 360° finds if any eaves dropper exists in the route between the source node and the next node information being is transmitted.



(a)

Figure 4.6: Power received vs Angle of incoming signals.

Two signals are identified from two different direction. Based on the power received from two direction, Signal of interest is identified at 5° and eaves dropper is detected at -20°.

routing the information to the intended direction of node while nulling the direction of the identified eaves dropper is executed by MVDR fixed beam forming algorithm. The number of antennas used for the MVDR beamforming techniques is by varying the antenna number 8 to 32 by an increment of one.

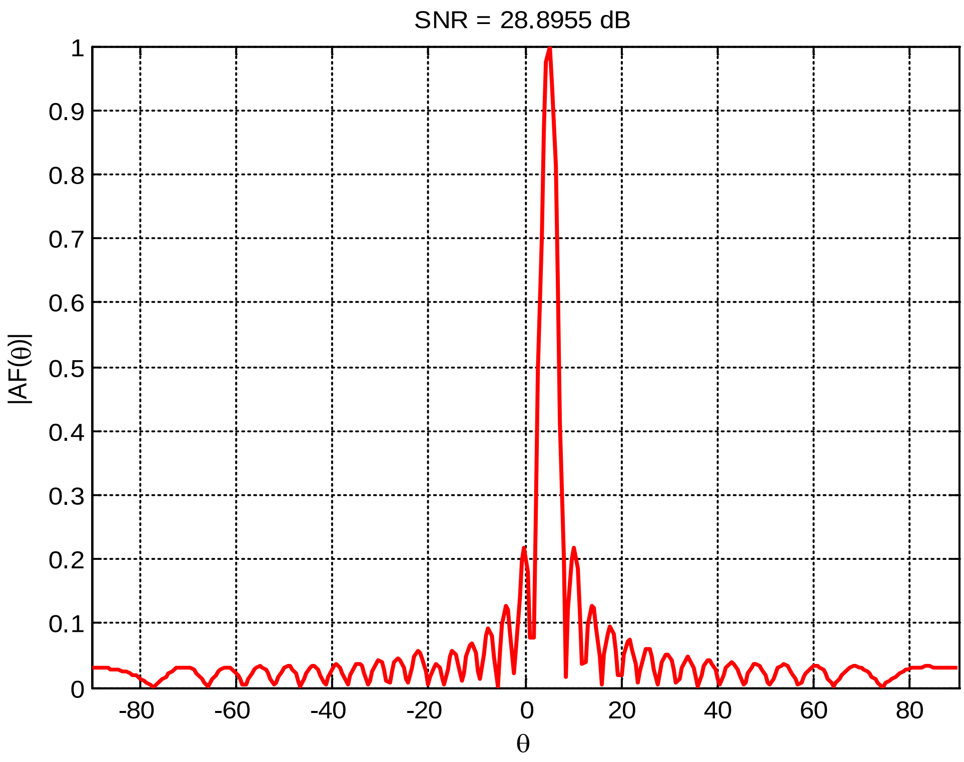
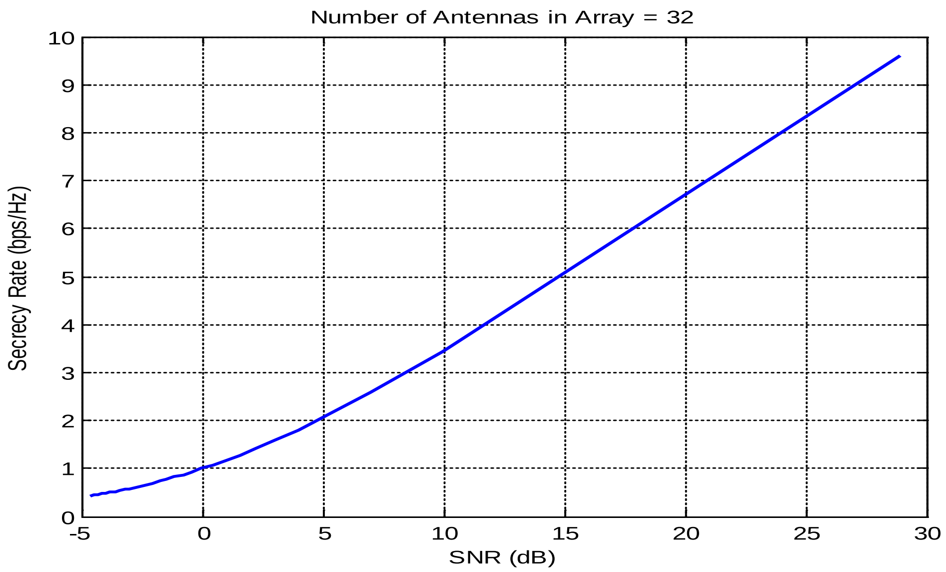
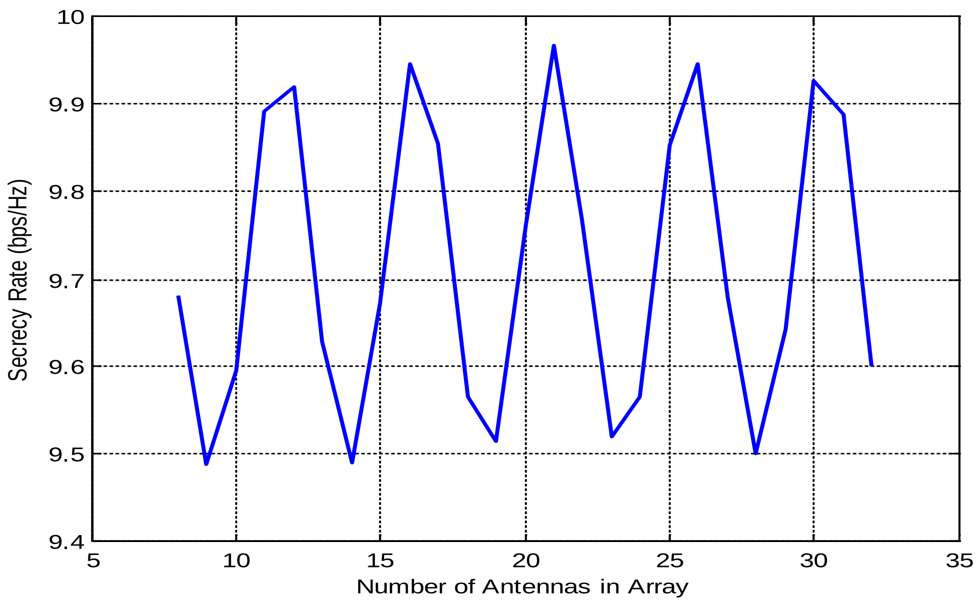


Figure 4.7: Angle of arrival vs Antenna facor for MVDR secure routing

Using adaptive beamforming technique, the beam pattern steered or shifted to the identified signal of interest direction identified while null is put at eaves dropper incoming signal direction. The secrecy rate and SNR of the transmitted signal is shown in figure below.



(a)

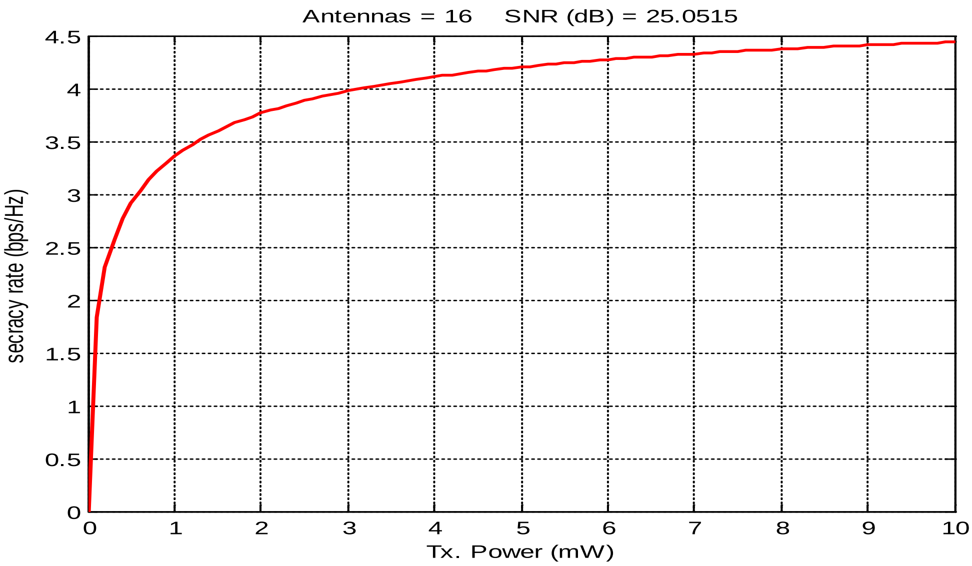


(b)

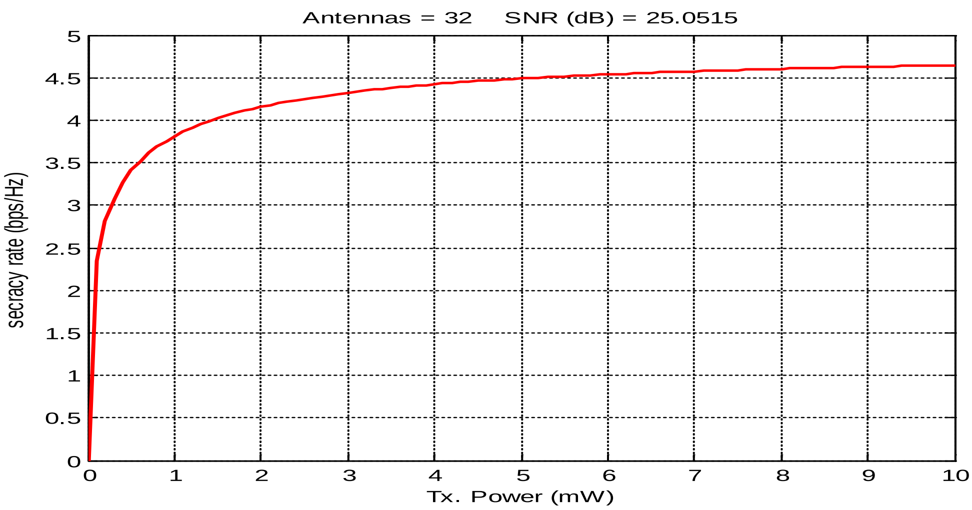
Figure 4.8: (a) Secrecy Rate Vs SNR and (b) Secrecy rate Vs number of antenna in array

As shown figure 4.6 (a) the quality of information transmission from the source node to next node is increase with the improvement of secrecy rate, where Figure (b) indicate that the secrecy rate increase with increment of the number of antennas from 8 to 14. However, further increase the number has no effect on improvement of the secrecy. So, it is an optimum number used here to attain the required secrecy.

Antenna grouping for secrecy: the secrecy rate increases with the increment in antenna transmitting power that means the beamforming technique to focus the direction of main beam pattern to specific required location. Here the side lobes become decreased and the eaves dropper cannot intercept the confidential information.



(a)



(b)

Figure 4.9: Secracy rate comparision for (a) 16 antenna (b) 32 antenna

The result shows that the transmitting power of antennas Tx power feed to the antenna can be saved by using more number of antenna to attain the same secrecy rate.

Table 4.7: Secrecy rate compararion for two antenna array with the same transmitting power

Transmitting power (mW)	Secrecy rate	
	16 antennas	32 antennas
1	3.4	3.8
2	3.7	4.1
3	4	4.4
5	4.1	4.5
6	4.2	4.51
7	4.3	4.55
8	4.4	4.6
9	4.45	4.65
10	4.48	4.7

From the table it is clear that for the same transmitting power to the group of antenna, the array antenna with more number of elements gives more secrecy with minimum power consumption which save energy.

LMS algorithm to analyse SNR: Transmitted signal may be subjected to different interferences other than eaves dropper. Therefore, the quality of transmitted signal is improved by using adaptive beamforming to increase the SNR.

Table 4.8: Parameters for LMS algorithm

Number of antenna elements	K = 16
Antenna Element separation	0.5 λ
No of signals	2
Angle of arrival of signal of interest	5
Angle of arrival for interference signal	-15
Channel variance	0.1

Now the error in transmitting the information is calculated calculated using the LMSE algorithm. The simulated least mean square error indicates the error of desired signal and eavesdropping trying to retrieve information after applying n number of iterations. The error decreases by increasing the number of antenna elements. The information is then routed with improved signal quality using adaptive beamforming LMS algorithm

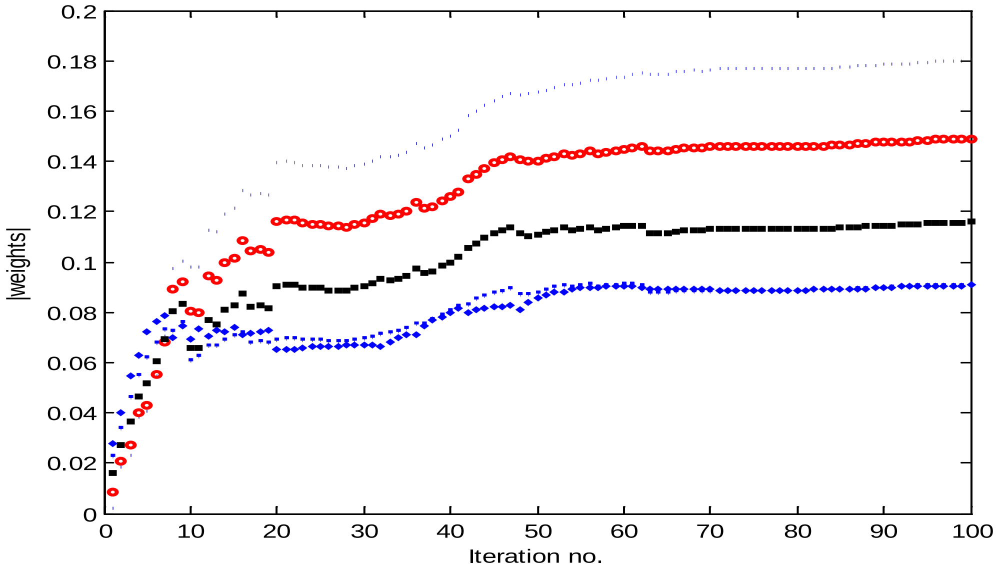
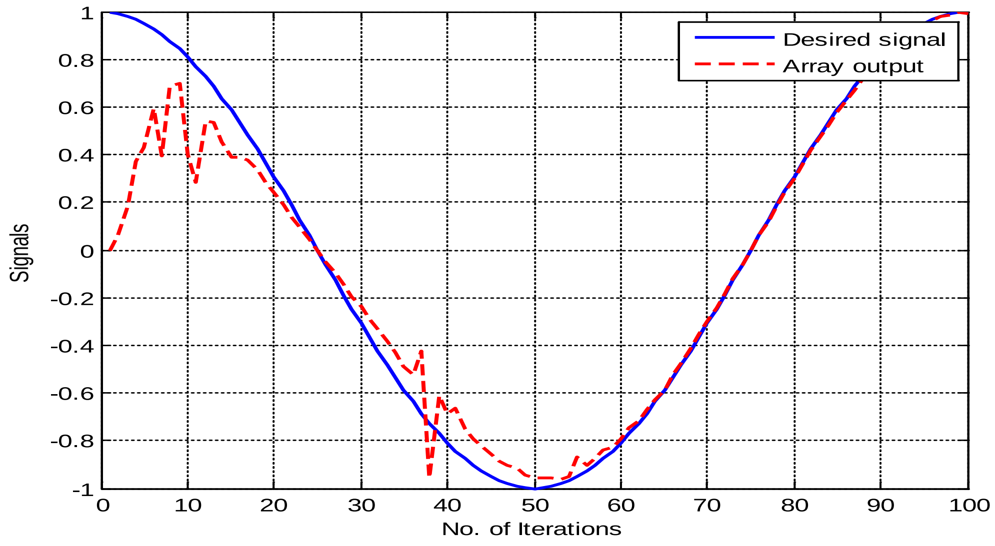
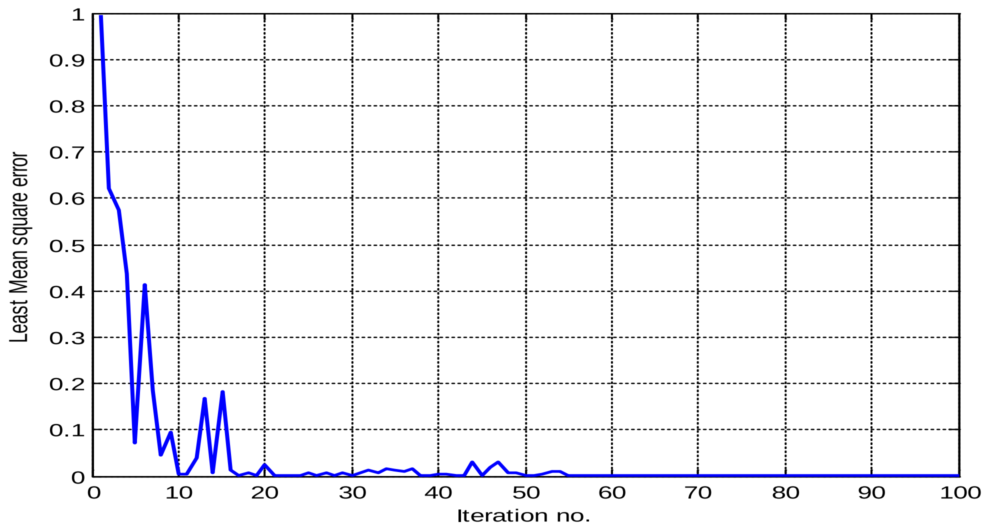


Figure 4.10:Magnitude of Array weight vs Iteration Number

By arranging the array weight, the error of the array output and desired signal is adjusted. This array weight vs iteration number below shows that after a number iteration the array weight becomes constant.



(a)



(b)

Figure 4.11: (a) Tracking of desired signal (b) LMSE error

The quality of information transmission improves after a number of iterations .as shown in figure above the array output fit the desired signal after 55 iteration is carried out.

Table 4.9: Comparision of desired and array output signal

Iteration number	Desired signal out put	Array out put	Error signal
5	1	0	1
10	0.8	0.6	.2
20	0.2	0.25	.05
30	-.04	-.45	.05
40	-.08	-.06	.02
50	-1	-1	0
60	-.8	-.8	0
70	-.04	-.04	0

The table 4.7 above shows that after a certain number of iterations the array put becomes similar to the desired signal output signal in which error is minimized. So that the quality of transmitted signal is improved or SNR maximized.

CHAPTER FIVE

5. CONCLUSION AND RECOMMENDATION

5.1 Conclusion

The frequent link failure due to the dynamic nature of VANET topology requires suitable routing. The developed combined shortest path of Bellman and Dijkstra algorithm result showed better energy efficiency. The vulnerability of information to eavesdropper in the transmission path from source to next node or destination is improved using the antenna beamforming technique. The beam steering technique is employed to scan the angle of arrival of the available signal around the source node and the direction of an incoming eavesdropper. As seen from the result the min norm algorithm beam former simulation shows the main beam directed to the intended node direction while null is put in the direction of an incoming eavesdropper. So that the secrecy rate is analyzed using a specified number of the array antenna. Finally, the LMS algorithm result indicated maximum SNR the high quality of transmitted information. Also, the analytical model compared with the simulation result shows greater secrecy improvement.

5.2 Recommendation

In this thesis single active eavesdropper with hybrid routing is considered. The Vehicular ad hoc network security and route plan can be extended to simulate other algorithms to measure their performance under specific road conditions and large road network topology. The actual specific city scenario can be implemented physically.

REFERENCES

[1] Eman S. Alwadiyeh, Ala' F A Aburumman, "Interference-Aware Multipath routing protocols for Mobile Ad hoc Networks," in *13th Annual IEEE Workshop on Wireless Local Networks*, Australia, 2013.

[2] LIAO WENXING, WU MUQING, ZHAO MIN, AND LI PEIZHE, "The Impacts of Weak Links on Routing Process in Large Scale Multi-Hop Networks," vol. 5, July 17, 2017.

[3] Tayal, S. & Triphathi, M. R., "Vanet challenges in selection of vehicular mobility model," in *Second international conference on advanced computing commuication*, 2012.

[4] Giannis Savva, Konstantinos Manousakis, and Georgios Ellinas, "Eavesdropping-aware Routing and Spectrum Allocation in EONs using Spread Spectrum Techniques," in *KIOS CoE and Department of Electrical and Computer Engineering*, 2018.

[5] S. Mumtaz, K.M.S. Huq, M.I. Ashraf, J. Rodriguez, V. Monteiro, C., "Cognitive vehicular communication for 5G," *IEEE Commun*, pp. 109-117, 2015.

[6] L. C. Godara, "Application of antenna arrays to wireless communication: beamforming and direction of arrival considerations," vol. 85, pp. 1195-1245, 1997.

[7] Zivin Park, Jenshan Lin, "A Beam-steering Microstrip Antenna for Non-Contact Vital Sign Detection," vol. 10, pp. 235-238, 2011.

[8] X.Lan, W.Si and M.Dong, "New algorithm for DoA Estimation with Low SNR," in *Internationa Conferance on Innovation management and Idustrial Engineering*, 2011.

[9] R. S. e. D. S. M. Peden, "World report on road traffic injury prevention," *World Health Organiztion,* April15,2016.

[10] G. Yan, and D. B. Rawat, "Vehicles-to-vehicle connectivity analysis for vehicular ad-hoc networks,," *Ad-hoc Networks,* vol. 58, pp. 25-38, 2017.

[11] S. B. Mer, "Smart Vehicle to-Vehicle Communication with 5G Technology," vol. 53, no. 7, pp. 109-117, 2015.

[12] N. Lu,N.Cheng,N. Zhang,X. Shen, andJ.W.Mark, "Connected vehicles: solutions and challenges," *IEEE Internet of thiings,* vol. 1, no. 4, p. 289–299, 2014.

[13] Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A. Hassan, "Vehicular ad hoc networks (VANETs): Status,result and challenges," *telecommun.system,* pp. 217-241, 2012.

[14] H. N. a. M. Valkama, "Impact of VANET-based V2X communication using IEEE 802.11p on reducing vehicles traveling time in realistic large scale urban area," in *2013 International Conference on Connected Vehicles and Expo (ICCVE),* Las Vegas,, 2013.

[15] Miao Wang, Hangguan Shan, Rongxing Lu, Ran, "Real-Time Path Planning Based on Hybrid-," *IEEE Transactions on Vehicular Technology,* 2015.

[16] P. Golmohammadi, P. Mokhtarian, F. Safaei, and R. Raad, "An analytical model of network connectivity in vehicular ad hoc networks using spatial point processes," p. 1–6, June 2014.

[17] H. Zhang, "A Survey of Ant Colony Optimization Based Routing Protocols for Mobile Ad Hoc Networks," vol. 5, pp. 24139-24161, 2017.

[18] Charalampopoulos G, Dagiuklas T, Chrysikos T, "V2I applications in highways how RSU dimensioning can improve service delivery," *international conference on telecommunications (ICT),* pp. 1-6, 2016.

[19] Gosman, C., Dobre, C., & Cristea, V., "A security protocol for vehicular distributed systems, in: 12th," *12th International Symposium on Symbolic and Numeric Algorithims for Scientific Computing,* pp. 321-327, 2010.

[20] K. Singh, P. Rawat, and J. Bonnin, "Cognitive radio for vehicular ad hoc networks (CR-VANETs): approaches and challenges," *EURASIP J.Wirel. Commun. and Netw,* no. 49, pp. 1-22, Mar. 2014.

[21] Andr´e Egners, Patrick Herrmann, Tobias Jarmuzek, and Ulrike Meyer, "Experiences From Security Research Using a Wireless Mesh Network Testbed," in *38th Annual IEEE Confrance on local Computer Networks*, 2013.

[22] Chammem, M. H. , Hamdi, M., & Boudriga, N, "Notice of Violation of IEEE Publication Principles Cooperative Security in Vehicular Communication Systems In Advanced Information NetworkinR and Applications (AlNA)," *2011 iEEE international Conference on,* pp. 495-500, March 2011.

[23] X. Ma, J. Zhang, X. Yin, K.S. Trivedi, "Design and analysis of a robust broadcast scheme for VANET safety-related services," *IEEE Trans,* pp. 46-61, 2012.

[24] B. A. Forouzan, Cryptograph & Network Security, India, New Delhi: McGrow-Hill Company, 2007.

[25] Thomas HCormen,Charles.ELeasorson,Ronald L.Rivest,Clifford Stain, Introduction to Algorithm, Third Edition ed., London,England: Massachutes Institute of Technology, 2009.

[26] B. Hamid, and E. E. Mokhtar, "Performance analysis of the vehicular ad-hoc networks (VANET) routing protocols, AODV,DSDV and OLSR," pp. 1-6, 2017.

[27] M. Ren, L. Khoukhi, H. Labiod, J. Zhang, and V. Veque,”, "A mobilitybased based scheme for dynamic clustering in vehicular ad-hoc networks (VANETs)," *Vehicular Communications,* vol. 9, p. 233–241, 2017.

[28] S. Benkirane, S. Mostafa, M. L. Hasnaoui, and A. Beni-Hassane, "A new comparative study of Ad-hoc routing protocol AODVand DSR in VANET environment using simulation tools," *2015 15th International conference on intelligent system designs and applications,* p. 458 –461, 2015..

[29] K. Collins and G. M. Muntean, "n Adaptive Vehicle Route Management Solution Enabled by Wireless Vehicular Networks," in *2008 IEEE 68th Vehicular Technology Conference*, Calgary, 2013.

[30] Cooper, C.; Franklin, D.; Ros, M.; Safaei, F.; Abolhasan, M, "A Comparative Survey of VANET Clustering Techniques," *IEEE Commun. Surv. Tutor*, no. 19, pp. 657-487, 2017.

[31] J. a. J. Tornow, "The DARPA packet radio network protocols," 211.

[32] H. Kanoh, "Dynamic route planning for car navigation systems using virus genetic algorithm," *international Jornal of Knowledge based and Intelligent Engineering Systems,* vol. 11, pp. 65-78, 2007.

[33] Tantan Zhao, Guobing Li, Guomei Zhang, and Chun-Xia Zhang‡, "Security-Enhanced User Pairing for MISO-NOMA Downlink Transmission," China, 2018.

[34] M. Rivas, S. Xie and D. Su, "A review of adaptive beamforming technique for wide band smart antennas," in *6th Intl. Conference on Wireless Communications, Networking and Mobile Computing (WiCOM),* Cchingdu,China, 2010.

[35] T. Rappaport, S. Sun, R.Mayzus et al., "Millimeter wave mobile communication for 5G mobile communication for 5G," *IEEE Access,* vol. 1, pp. 335-349, 2013.

[36] Ahmed Attia, Ahmad A. El Moslimany, Amr El-Keyi, Tamer El Batt,Fan Bai, and Cem Saraydar, "MIMO Vehicular Networks: Research Challenges and Opportunities," *Journal Of Communications,* vol. 7, no. 7, pp. 500-513, June 2012.

[37] S.Timilsina, D. Kudathanthirige and G. Amarasuriya, "Physical Layer Security in Cell-Free Massive MIMO," USA, 2018.

[38] S. M. et.al, "An Approach for the Integration of Smart Antennas in the Design and Simulation of Vehicular Ad-Hoc Networks," in *International Conference on Future Generation Communication Technology (FGCT'12),* December 2012.

[39] H.V.Poor and R>F.Schaefer, "Wireless physical layer security," *Proceeding of the National Academy of Sciences,* vol. 114, no. 1, pp. 19-26, 2017.

[40] A. H. Khosroshahi, P. Keshavarzi, Z. D. KoozehKanani and J. Sobhi, "Acquiring real time traffic information using VANET and dynamic route guidance," in *2011 IEEE 2nd International Conference on Computing, Control and Industrial Engineering,* Wuhan, 2011.

[41] K. Pandey and S. Raina, "Hop Count Analysis of Location Aided multihop

routing protocols for VANET," 2015.

[42] Y.Vasudeva Reddy, M.Nagendra and G.Vijaya Kumar, "Current Research Work on Routing Protocols for MANET: A Literature Survey," vol. 2, no. 3, pp. 706-713, 2010.

[43] A. Kurien and A. Diana, "Survey on various position based routing protocol in Vehicular ad hoc Network," vol. 2, 12 December 2013.

[44] Gavilanes G, Reineri M and Brevi D, "Comparative characterization of four antennas for Vanets by on-field measurements. In: International conference on microwaves," *communications, antennas and electronics systems (COMCAS) IEEE*, pp. 1-5, 2013.

[45] a. H. B. I. Basaran, "Performance Comparison of non Delay Tolerant Vanet Routing Protocols," *International workshop on urban mobility & intelligent transportation systems*, pp. 1-6, 2016.

APPENDIX

These are MATLAB code used for simulation

Min-Norm AOA Estimation

```
clc;
clear all;
close all;
L=16;
D = 3; % number of signals
sig2=.1;
th1=-10*pi/180;
th2=5*pi/180;
th3=25*pi/180;
a1=[1];
a2=[1];
a3=[1];
a=[1];
F=[1;1];
temp=eye(L);
%temp=zeros(1,L-1);
%u1=[1 temp];
u1=temp(:,1);
u3=temp(:,3);
for i=2:L
```

```
    a1=[a1 exp(-1j*i*pi*sin(th1))];
    a2=[a2 exp(-1j*i*pi*sin(th2))];
    a3=[a3 exp(-1j*i*pi*sin(th3))];
end
A=[a1.' a2.' a3.'];     % transpose without conjugating
Rss=[1 0 0;0 1 0;0 0 1];
Rrr=A*Rss*A'+sig2*eye(L);
%Rrr=(A*F+sig2*diag(eye(L)))*(A*F+sig2*diag(eye(L)))';
[V,Dia]=eig(Rrr);
[Y,Index]=sort(diag(Dia));   % sorts the eigenvalues from least to greatest
 EN=V(:,Index(1:L-D));      % calculate the noise subspace matrix of eigenvectors
                            % using the sorting done in the previous line
for k=1:360;
   th(k)=-pi/6+pi*k/(3*360);
   clear a
a=[1];
   for jj=2:L
      a = [a exp(-1j*jj*pi*sin(th(k)))];
   end
P(k)=1./abs(conj(a)*EN*EN'*u1).^2;
%P(k)=1./abs(conj(a)*EN*EN'*u3).^2;
P2(k)=1./abs(sum(conj(a)*EN)).^2;
end
figure;
```

```
plot(th*180/pi,10*log10(P/max(P)),'b','linewidth',1.5)

grid on

xlabel('Angle')

ylabel('|P(\theta)|')

axis([-40 40 -30 10])

%num2str(A,2)
```

Analytical secrecy routing model code

```
clc;

close all;

clear all;

Ps=0:0.1:10;

sig2=0.1;

M=500;

I=32;

w=ones(1,I);

% w=diag(fliplr(pascal(N)))';

% w=kaiser(N,50)';

ksr=ones(1,I)';

Ksr=ksr*ksr';

diag_Ksr=diag(Ksr);

E=10;

kre=zeros(1,I)' + E;

Kre=kre*kre';

diag_Kre=diag(Kre)
```

```
D=0.1;

krd=ones(1,I)' + D;

Krd=krd*krd';

diag_Krd=diag(Krd);

gamma_re=Ps.*(w*diag_Ksr*(kre')*kre*(diag_Ksr')*w')./((sig2.*w*(diag_Kre)*(diag_Kre')*w')+sig2);

gamma_rd=Ps.*(w*diag_Ksr*(krd')*krd*(diag_Ksr')*w')./((sig2.*w*(diag_Krd)*(diag_Krd')*w')+sig2);

Re=0.5*log10(1+gamma_re)/log10(2)

Rd=0.5*log10(1+gamma_rd)/log10(2);

Rs=Rd-Re;

figure(1);

plot(Ps,Rs,'r--','linewidth',1.5);

xlabel('Tx. Power (mW)');

ylabel('secracy rate (bps/Hz)');

title(['Antennas = ',num2str(I), '    SNR (dB) = ',num2str(10*log10(E/D))]);

grid on;
```

MVDR algorithm mat lab code

```
clc;

close all;

clear all;

d=.5;

ant=8:1:32;

for kk=1:length(ant)
```

```
 N= ant(kk);
var=0.001:0.1:3;        % noise variance
for k=1:length(var)
sig2=var(k);
theta=-pi/2:.01:pi/2;
ang=theta*180/pi;
th0=5*pi/180;      % receive angle
 th1=-20*pi/180;
s=1;                %signal amplitude
a=[];
n1=[];
n2=[];
n=-(N-1)/2:(N-1)/2;
a=exp(1j*2*pi*n*d*sin(th0));  % array steering vector
n1=exp(1j*2*pi*n*d*sin(th1));  % array steering vector
 a=a.';
n1=n1.';
Rss=a*a.';              % signal correlation matrix
 Rii=n1*n1';            % interferer 1 correlation matrix
Rnn=sig2*eye(N);        % noise correlation matrix
Ruu=Rii+Rnn;            % total undesired signal correlation matrix
w=inv(Ruu)*a./(a'*inv(Ruu)*a);          % calculated weight vector
th1;
for j=1:length(theta)
```

```
th=theta(j);
aa=[exp(1j*2*pi*n*d*sin(th))];
aa=aa.';
y(j)=w'*aa;
if (th < -0.34 && th > -0.36)
AFI=y(j);
 end
end
 AFI_abs(k)=abs(AFI)/max(abs(y));
SNR(k)=s^2/(sig2+AFI_abs(k)^2);
Secy_rate(k)=log10(1+SNR(k))/log10(2);
if(k ==1)
y1=y;
end
if(k==length(var))
y2=y;
end
end
SNR_1=10*log10(SNR(1));
SNR_2=10*log10(SNR(length(var)));
 Secy_rate_N(kk)=Secy_rate(1);
SNR_N(kk)=SNR_1;
if(kk ==1)
Secy_rate_1=Secy_rate;
```

```
snr_1=SNR;
end
if(kk==length(ant))
Secy_rate_2=Secy_rate;
snr_2=SNR;
end
end
figure(1);
plot(ang,abs(y1)/max(abs(y1)),'r','linewidth',1.5)
axis([-90 90 0 1])
xlabel('\theta')
ylabel('|AF(\theta)|')
title(['SNR = ',num2str(SNR_1),' dB']);
grid
figure(2);
plot(ang,abs(y2)/max(abs(y2)),'r','linewidth',1.5)
axis([-90 90 0 1])
xlabel('\theta')
ylabel('|AF(\theta)|')
title(['SNR = ',num2str(SNR_2),' dB']);
grid
figure(3);
plot(10*log10(snr_1),Secy_rate_1,'linewidth',1.5)
xlabel('SNR (dB)')
```

```
ylabel('Secrecy Rate (bps/Hz)')

title(['Number of Antennas in Array = ',num2str(ant(1))]);

grid

figure(4);

plot(10*log10(snr_2),Secy_rate_2,'linewidth',1.5)

xlabel('SNR (dB)')

ylabel('Secrecy Rate (bps/Hz)')

title(['Number of Antennas in Array = ',num2str(ant(end))]);

grid

figure(5);

plot(ant,Secy_rate_N,'linewidth',1.5)

xlabel('Number of Antennas in Array')

ylabel('Secrecy Rate (bps/Hz)')

grid

figure(6);

plot(ant,SNR_N,'linewidth',1.5)

xlabel('Number of Antennas in Array')

ylabel('SNR (dB)')

grid

% num2str(a,2)
```

LMS Algorithm

```
clc;

close all;
```

```
clear all;
d = .5;  % element spacing
K=16;
thetaS =25;
thetaI =15;
T=1E-3;
t=(1:100)*T/100;
it=1:100;
S=cos(2*pi*t/T);
thetaS = thetaS*pi/180;                    % desired user AOA
I = randn(1,100);
thetaI = thetaI*pi/180;                    % interferer AOA
vS = []; vI = [];
i=1:K;
vS=exp(1j*(i-1)*2*pi*d*sin(thetaS)).';
vI=exp(1j*(i-1)*2*pi*d*sin(thetaI)).';
w = zeros(K,1);     snr = 10;  % signal to noise ratio
 X=(vS+vI);
Rx=X*X';
mu=1/(4*real(trace(Rx)))
%mu = input('What is step size?')
wi=zeros(K,max(it));
for n = 1:length(S)
    x = S(n)*vS + I(n)*vI;
```

```
    %y = w*x.';
    y=w'*x;
    e = conj(S(n)) - y;      esave(n) = abs(e)^2;
%    w = w +mu*e*conj(x);
    w=w+mu*conj(e)*x;
    wi(:,n)=w;
    yy(n)=y;
end
w = (w./w(1));    % normalize results to first weight
theta = -pi/2:.01:pi/2;
AF = zeros(1,length(theta));
% Determine the array factor for linear array
for i = 1:K
    AF = AF + w(i)'.*exp(1j*(i-1)*2*pi*d*sin(theta));
end
figure;
plot(theta*180/pi,abs(AF)/max(abs(AF)),'b','LINEWIDTH',1.5)
xlabel('AOA (deg)')
ylabel('|AF_n|')
axis([-90 90 0 1.1])
set(gca,'xtick',[-90 -60 -30 0 30 60 90])
grid on
figure;
plot(it,S,'b',it,yy,'r--','linewidth',1.5)
```

```
xlabel('No. of Iterations')

ylabel('Signals')

legend('Desired signal','Array output')

grid;

disp('%-------------------------------------------------%')

disp(' ')

disp(['   The weights for the K = ',num2str(K),' ULA are:'])

disp(' ')

for m = 1:length(w)

    disp(['   w',num2str(m),' = ',num2str(w(m))])

end

disp(' ')

figure;

plot(it,abs(wi(1,:)),'bx',it,abs(wi(2,:)),'ro',it,abs(wi(3,:)),'ks',it,abs(wi(4,:)),'b+',it,abs(wi(5,:)
),'bd','markersize',2,'linewidth',1.5)

xlabel('Iteration no.')

ylabel('|weights|')

grid;

figure;

plot (it, esave,'b','linewidth',1.5)

xlabel('Iteration no.')

ylabel('Least mean square error')

grid;
```