ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Optimized Secure Routing with Randomize and Forward Strategy in Multi-Hop Wireless Ad Hoc Networks

Dr. S. Mythili
MCA, M.Phil., Ph.D
Associate Professor and Head
Department of Information Technology
Kongunadu Arts and Science College,
Coimbatore, Tamil Nadu, India

A.Anitha
M.Sc (CT)
Research Scholar
Department of Computer Science
Kongunadu Arts and Science College
Coimbatore, Tamil Nadu, India

Abstract:A wireless ad hoc network is also known as IBSS- Independent Basic Service Set, is a computer network in which the communication links are wireless. It is an IP routing protocol optimized for MANETs and WANETs. The proactive link state protocol use hello and topology control (TC) messages to discover and then disseminate link state information throughout the WANET. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths. Hence, the main goal of this research work is to improve the secrecy performance in multi-hop wireless ad hoc network with respect to two different cases such as the colluding and non-colluding eavesdroppers with Randomize and Forward (RF) relay strategy using Optimized Link State Routing Protocol (OLSR) which is specifically designed from the viewpoint of physical layer security. The relay strategy in the wireless ad hoc networks, deals with the secure connection path between the source and destination through the intermediate relay nodes and also the intermediate relay selection. The RF strategy is an optimized version of traditional link state protocol such as the Optimized Link State Routing (OLSR) protocol helps in the relay selection with the concept of the Multipoint Relay (MPRs) nodes to efficiently disseminate link state updates across the network. The Dijkstra's algorithm (K Shortest path routing) selection is adopted for both colluding eavesdroppers case and the non-colluding eavesdroppers case in order to find the highest secure connection probability (SCP) shortest path between any given source-to-destination pair in a distributed way in order to improve the detection accuracy using the heterogeneous passion point process. The proposed research work presents a new approach to measure the secure routing in multi-hop wireless ad hoc networks in wireless networks with the steps namely the Network Model, Mobility Modeling, Secure Routing Randomize-and-Forward using Optimized Link State Routing (RFOLSR) Protocol and Secure shortest path routing detection algorithm. The RFOLSR protocol used to select the multiple shortest paths and secure protocol used to transfer a message to destination without packet drops. Through extensive simulations and verification the proposed mechanism achieves significantly better detection accuracy than conventional methods such as decode and forward (DF) strategy based detection.

Keywords: Multi-hop Routing, Randomize and Forward (RF), Optimized Link State Routing (OLSR), Colluding Eavesdroppers, Non-Colluding Eavesdroppers

I. INTRODUCTION

A. *Routing in Ad Hoc Networks*

In mobile ad hoc networks, the issue of routing packets between any pair of nodes becomes a challenging task because the nodes can move randomly within the network. A path that was considered optimal at a given point in time might not work at all a few moments later. Moreover, the stochastic properties [23] of the wireless channels add to the uncertainty of path quality.

The operating environment as such might also cause problems for indoor scenarios [19] the closing of a door might cause a path to be disrupted. Traditional routing protocols [20] are proactive in that they maintain routes to all nodes, including nodes to which no packets are being sent. They react to any change in the topology even if no traffic is affected by the change, and they require periodic control messages to maintain routes to every node in the network.

The rate at which these control messages are sent must reflect the dynamics of the network in order to maintain valid routes. Thus, scarce resources such as power [24] and link bandwidth will be used more frequently for control traffic as node mobility increases. An alternative approach involves establishing reactive routes, which dictates that routes between nodes are determined solely when they are explicitly needed to route packets. This prevents the nodes from updating every possible route in the network, and instead allows them to focus either on routes that are being used, or on routes that are in the process of being set up.

B. *Characteristics of Wireless Mobile Ad Hoc Networks*

Wireless mobile ad hoc networks have significant characteristics as follows [3]:

Dynamic Network Topology: Each node in an ad hoc network is free to move randomly. This feature makes the network topology change unpredictably. Also, an ad hoc network may be comprised of both bidirectional and unidirectional links [38]. Thus, using ad hoc networks could augment mobility and flexibility of nodes in the networks [26]. Even though the network topology varies, connectivity in the network should be maintained to allow applications and services to operate without disruption. In particular, this characteristic will affect the design of routing protocols. In addition, a user in an ad hoc network will require access to a fixed network, such as the Internet, even if nodes are mobile. This needs mobility management functions allowing network access for devices located several radio hops away from a network access point.

Bandwidth-Limited and Fluctuating Capacity Links: Wireless links will remain to have substantially lower capacity compared to their hardwired counterparts. Besides, the throughput of wireless communications in real environments is much less than a radio’s maximum transmission rate, the reason are the effects of multiple access [34], fading, noise, and interference conditions, and so on. The effects of high bit-error rates may be more severe in a multi-hop ad hoc network, because the aggregate of all link errors affects a multi-hop path. Moreover, more than one end-to-end route can use a given link if the link were to break. This could disrupt several sessions during periods of high bit-error transmission rates. Thus, this will affect the routing function. However, efficient functions for link layer protection, such as forward error correction (FEC), and automatic repeat request (ARQ), can significantly improve the link quality.

Low-Power and Resource-Limited Operation: In most cases, the network nodes in a wireless ad hoc network may depend on batteries or other exhaustible means for their energy. This feature makes the power budget tight for all the power-consuming components in a mobile device. For example, this will affect CPU processing, memory size and usage, signal processing, and transceiver output/input power [4]. For these nodes, energy conservation should be considered for the optimization as a key system design criterion [28].

Constrained Physical Security: In general, mobile wireless networks are more likely to be vulnerable to physical security threats than are fixed-cable nets [35]. For example, there is the increased possibility of eavesdropping, spoofing, and denial-of-service attack that should be carefully considered. Often current link security techniques are applied to wireless networks to diminish security threats [40].

C. *Types of Eavesdroppers*

There are two types of eavesdroppers available. They are:

Colluding Eavesdroppers: The Colluding Eavesdroppers Case occurs, when one or more eavesdroppers who attack the same path or the packet during the time of transmission of packets from the source node to the desired destination node. If there is a chance of join attack or colluding attack, the eavesdropper who does it are called as the Colluding Eavesdroppers.

Non-Colluding Eavesdroppers: The Non-Colluding Eavesdroppers Case occurs, when one eavesdropper attack the secured path at the time of transmission of packets from the source node to thedesired destination node. If there is a chance of attack and the eavesdropper who does it are called as the Non-Colluding Eavesdropper. In other words, Non–Colluding Eavesdropper are the eavesdropper who act in a independent manner and attacks the independent secured path while the communication between source node and destination node exists and secure performance is determined with the strongest received signal from the transmitter [37].

The secure connection [21] probability for colluding eavesdroppers will obtain the exact expressions of secure connection probability for the direct transmission and relay transmission by assuming the arbitrary relay, respectively [33] [36] [39]. Then the lower bound for colluding eavesdroppers is obtained, and the lower bound gives accurate approximation of the exact performance when the eavesdropper density is small. Using the lower bound, to find that the optimum relay is the nearest one to the midpoint between the source and destination, and get the lower bound expression for relay selection.

D. *Dijstra Algorithm*

Dijkstra's algorithm, conceived by Dutch computer scientist Edsger Dijkstra in 1959. The Single-Source Shortest Path Problem (SSSP) is the problem of finding shortest paths from a source vertex v to all other vertices in the graph. The Dijkstra's algorithm is a solution to the single-source shortest path problem in graph theory. This algorithm is often used in routing. For a given source vertex (node) in the graph, the algorithm finds the path with lowest cost (i.e. the shortest path) between that vertex and every other vertex.

It can also be used for finding costs of shortest paths from a single vertex to a single destination vertex by stopping the algorithm once the shortest path to the destination vertex has been determined. Dijkstra Algorithm used the method of increasing node by node to get a shortest path tree which makes the starting point as its root [41]. It works on both directed and undirected graphs. However, all edges must have non-negative weights. It is a Greedy based algorithm and the global information of the network is required. The time complexity of the algorithm is O(|E| + |V|Log|V|).Let us consider,

Input: Weighted graph G = {E, V} and source vertex v ∈ V, such that all edge weights are non-negative.

Output: Lengths of shortest paths (or the shortest paths themselves) from a given source vertex v ∈ V to all other vertices. The simplest implementation is to store vertices in an array or linked list. This will produce a running time of O(|V|^2+E|).For the sparse graphs, or graphs with very few edges and many nodes, it can be implemented more efficiently storing the graph in an adjacency list using a binary heap or priority queue. This will produce a running time of O((|E|+|V|)log |V|).

Working of Dijkstra Algorithm: As with all greedy algorithms, it is possible to make sure that it is a correct algorithm (e.g., it always returns the right solution if it is given correct input).Dijkstra’s algorithm calculates the shortest path to every vertex. To know the optimal path to some other vertex from a determined origin the Dijkstra’s algorithm is been used.

Application of Dijkstra Algorithm: Robot path planning [42], Logistics Distribution Lines [43], Link-state routing protocols [44], OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System).

E. *Optimized Link State Routing Protocol(OLSR)*

It is an IP routing protocol optimized for MANETs also used in WANET. It is a proactive link state routing protocol. The protocol receives the stability of the link state algorithm. Due to its proactive nature, it has an advantage of having the routes immediately available when needed. In a pure link state protocol, all the links with neighbor nodes are declared and are flooded in the entire network. OLSR protocol is an optimization of a pure list state protocol. Because first, it reduces the size of control packets instead of all links, it declares only a subset of links with its neighbors who are its *multipoint relay selectors.* Secondly, it minimizes flooding of this control traffic by using only the selected nodes, called multipoint relays, to diffuse its messages in the network. Only the multipoint relays of a node retransmit its broadcast messages.

This technique significantly reduces the number of retransmissions in a flooding or broadcast procedure.The OLSR protocol is intended to work in completely distributed manner and does not depend upon any central entity. The protocol does not need a dependable transmission of the control messages: each node sends its control messages from time to time, and can therefore sustain a loss of some packets periodically, which happens very frequently in the radio networks due to collisions or transmission problems. The OLSR protocol carry out hop by hop routing that is each node uses its most latest information to route a packet. Hence, when the node is moving, its packet can be effectively delivered to it, if its speed is such that its movement could be followed in its neighborhood, at least. The protocol supports a nodal mobility that can be traced via its local control messages, which depends upon the frequency of these messages.

F. *Multipoint Relay(MPR) Selection*

The important point of the optimization is the multipoint relay (MPR). The MPR is identified by each node. When is used for exchanging link-state routing information, a node contains the list which has the connections to those neighbors only and that have been selected it as MPR that is Multipoint Relay Selector Set. The protocol selects the bi-directional links for routing, hence avoiding packet transfer over the unidirectional links [45]. It is clearly represented in the fig 1.

In wireless ad hoc networks, the medium are usually shared when a packet is flooded; the same packet is sent many times to the same receiver. It is not only the waste of bandwidth but also the load of broadcast packets is increased in the network, it may increase the collision rate and the actual packet delivery may then be decreased. The multipoint relay technique is used to reduce the overhead induced by transmitting of broadcast packets. The concept of multipoint relay optimization is the core optimization of OLSR [2] [17] [18].

The main idea of the multipoint relay optimization is that only a subset of neighbors has to relay a flooded packet that has been flooded. It can be easily understood that if a conveniently chosen subset of one's neighbor nodes can relay a flooded packet to all one's 2-hop neighbors; then the relay of these nodes will be sufficient to ensure the proper delivery of the packet to the node m's 2-hop neighbors, which is shown in the fig. 2.

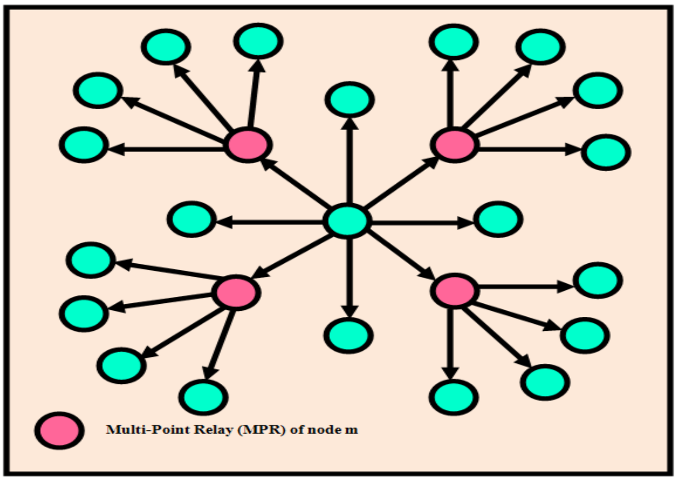


Fig. 1 Multipoint Relay Nodes in Multi-Hop Wireless Networks

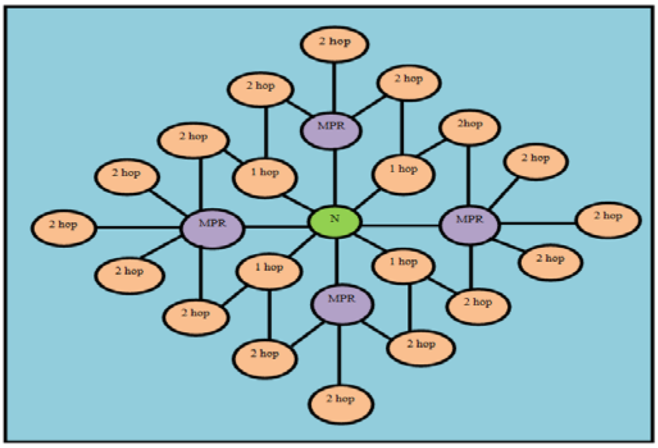


Fig. 2 MultipointRelays of Node N

Multipoint relay optimization must be repeated recursively when the packet is flooded. At each hop a flooded packet is relayed by the next hop multipoint relay set. Hence, already transmitted packet will not be retransmitted twice and it is carried out with the help by a duplicate table. The interesting point is that the notion of multipoint relay is deeply embedded in the OLSR protocol. To maintain the knowledge of the network topology OLSR uses two kinds of control. The first kind of packet called *"Hello"* and it is used to build the neighborhood. The second kind of packet called *"Topology Control"* which is used by each node to broadcast the neighborhood within the network.

II. RELATED WORK

***I. Csiszar and J. Korner*[1]**has proposed the two discrete memory less channels (DMC's) with a common input, it is desired to transmit private messages to receive 1 at R1, and common messages to both receivers at rate R0, while keeping receiver 2 as ignorant of the private messages as possible. Measuring ignorance by equivocation, a single-letter characterization is given by the achievable triples (Ri, Re, R0) where Re is the equivocation rate. Based on this channel ding result, the related source-channel matching problem is also settled. There was a model for simultaneously broadcasting both messages for common use and confidential messages. And the model has been characterized by the achievable rates in terms of information quantities, so that the rate region is, in principle, computable. That is the commonly accepted criterion of a "solution" in multi-user Shannon theory. The actual computation might be very difficult. The possible approach is to look at the tangent planes to the rate region but in some simple cases, the numerical results are readily obtained.

***J. Mo, M. Tao, Y. Liu, and R. Wang* [5]** made a studied on the secure beam forming design in a multiple-antenna [22] three-node system where two source nodes exchange messages with the help of an untrusted relay node.

The relay acts as both an essential signal forwarder and a potential eavesdropper. Both two-phase and three-phase two-way relay strategies are considered. The study has focused on to jointly optimize the source and relay beam formers for maximizing the secrecy sum rate of the two-way communications [29]. Hence, first derive the optimal relay beam former structures. Then, iterative algorithms are proposed to find source and relay beam formers jointly based on alternating optimization.Furthermore, the behavior asymptotic analysis on the maximum secrecy sum-rate which has showed that when all transmit powers approach are infinity, then the two-phase two-way relay scheme achieves the maximum secrecy sum rate if the source beam formers are designed such that the received signals at the relay align in the same direction which reveals an important advantage of signal alignment technique in against eavesdropping.If the source powers approach zero, then the three-phase scheme performs the best while the two-phase scheme is even worse than direct transmission [31]. Simulation results have verified the efficiency of the proposed secure beam forming algorithms as well as the analytical findings [30].The study concludes that the conventional two-way direct transmission is preferred when the relay power goes to zero. When the relay power approaches infinity and source powers approach zero, the three-phase two-way relay scheme performs best. Moreover, when all powers go to infinity, the two-phase two-way relay scheme has the best performance if signal alignment techniques are used, which also lowers the requirement of numbers of antennas at the source nodes for security.

***Y. Zou, X. Wang, and W. Shen* [6]**has explored the physical-layer security in cooperative wireless networks with multiple relays where both amplify and forward (AF) and decode and forward (DF) protocols has been considered. The AF and DF based optimal relay selection (i.e., AFbORS and DFbORS) schemes to improve the wireless security against eavesdropping attack. For the purpose of comparison, this research work examines the traditional AFbORS and DFbORS schemes, which was denoted by T-AFbORS and TDFbORS, respectively. And also investigate a so-called multiple relay combining (MRC) framework and presented the traditional AF and DF based MRC schemes, called T-AFbMRC and TDFbMRC, where multiple relays were participated in forwarding the source signal to destination which then combines its received signals from the multiple relays.

The work derived closed-form intercept probability expressions of the proposed AFbORS and DFbORS (i.e., P-AFbORS and P-DFbORS) as well as the T-AFbORS, TDFbORS, T-AFbMRC and T-DFbMRC schemes in the presence of eavesdropping attack. Further an asymptotic intercept probability analysis to evaluate the diversity order performance of relay selection schemes and showed that no matter which relaying protocol is considered (i.e., AF and DF), both the traditional and proposed optimal relay selection approaches achieved the diversity order M (where M represents the number of relays).

***D. Goeckel, et.al*[7]** was discussed about the secure transmission of information in wireless networks without the knowledge of eavesdropper channels or locations [27].The discussion involves in two key mechanisms. The first mechanism was the artificial noise generation from system nodes other than the transmitter and receiver. And the second was a form of multi-user diversity that allows message reception in the presence of the artificial noise. To determine the maximum number of independently-operating and uniformly distributed eavesdroppers presence while the desired secrecy is achieved with high probability in the limit of a large number of system nodes. While the main motivation is considering the eavesdroppers of unknown location, first consider the case where the path-loss is identical between all pairs of nodes. In this case, a number of eavesdroppers that is exponential in the number of systems nodes can be tolerated. In the case of uniformly distributed eavesdroppers of unknown location, any number of eavesdroppers whose growth is sub-linear in the number of system nodes can be tolerated.

The discussion of secure transmission information suggests a number of avenues for future research and it is critical to the applicability of the results are an understanding of the rate at which the outage probabilities of the desired receivers and eavesdroppers converge to their asymptotic limits. The information-theoretic secrecy scenario leads a way for the consideration of the colluding eavesdroppers. Finally, the techniques require an exponential tail of the probability density function of the random power gain caused by the fading.

***A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel*[8]** has proposed the effectiveness and straightforward implementation of physical layer jammers made them an essential security threat for wireless networks. This work also discussed about the reliable communication in a wireless multi-hop network in the presence of multiple malicious jammers which is taken into consideration. Since energy consumption was an important issue in wireless ad hoc networks, minimum energy routing with and without security constraints [25] has received significant attention in the literature; however, energy-aware routing in the presence of active adversary (jammers) has not been considered.

With respect to that an efficient algorithm has been proposed for minimum energy routing between a source and a destination in the presence of both static and dynamic malicious jammers such that an end-to-end probability of outage is guaranteed. The percentage of energy saved by the proposed method with respect to a shortest path routing benchmark is evaluated. It was shown that the amount of energy saved, especially in terrestrial wireless networks with path-loss exponents greater than two, is substantial. Meanwhile the study concludes by considering the more sophisticated dynamic jammers with or without eavesdropping capabilities is an important topic for further research.

***Z. Ding, K. Leung, D. Goeckel, and D. Towsley* [9]** were discussed the information theoretic security which has recently emerged as an effective physical layer approach to provide secure communications. The outage performance of such a secrecy communication system was taken into consideration, since it is an important criterion to measure whether users' predefined quality of service can be met. Provided that the legitimate receiver and eavesdropper have the same noise power, many existing secure schemes cannot achieve the outage probability approaching zero, regardless of the transmission power. Hence, introduced the cooperative transmission into secrecy communication systems, it has shown here that outage probability approaching zero can be achieved. In particular, scenarios with single-antenna nodes and multiple-antenna nodes will both be addressed, and the optimal design of beam forming or precoding was investigated. Explicit expression of the achievable outage probability and diversity-multiplexing tradeoff was developed to demonstrate the performance of the proposed cooperative secure transmission schemes, and numerical results were presented. And focused on the secrecy communication scenario where all nodes were equipped with a single antenna. The outage performance of three schemes: the best relay scheme, the cooperative scheme using all qualified relays, and the MISO lower bound. The curves for the scheme using all qualified relays have the same slope as the ones for the MISO bound, which confirmed that this cooperative scheme can achieve the diversity gain.

***X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes* [10]** studied the throughput of large-scale decentralized wireless networks with physical layer security constraints. In particular, there is a inquisitiveness of how much throughput needs to be sacrificed for achieving a certain level of security. Hence, considered the random networks where the legitimate nodes and the eavesdroppers are distributed according to the independent two-dimensional Poisson Point Processes (PPP). The transmission capacity framework was used to characterize the area spectral efficiency of secure transmissions with constraints on both the quality of service (QoS) and the level of security. The framework illustrates the dependence of the network throughput on key system parameters, such as the densities of legitimate nodes and eavesdroppers, as well as the quality of service (QoS) and security constraints. One important finding was that the throughput cost of achieving a moderate level of security is quite low, while throughput must be significantly sacrificed to realize a highly secured network. The study also included the use of a secrecy guard zone, which was shown to give a significant improvement on the throughput of networks with high security requirements. The model of secrecy transmission capacity can be extended to analyze and design networks with other transmission techniques, medium access control protocols, and eavesdropping strategies in the future work. Similar to other transmission capacity formulations, the main limitation of this model is that it only considers single-hop transmissions, while the communication between an arbitrary source-destination pair usually requires multiple hops. End-to-end throughput analysis of wireless networks with physical layer security requirements was still an open problem. Another limitation of the current model was the Homogeneous Poisson distribution of nodes. The impact of eavesdropper distribution on secrecy throughput was an curious problem to investigate.

***M. Saad* [11]** has suggested a multi-hop wireless network and a source destination pair of nodes which addressed the problem of jointly selecting a communication route and allocating transmit power levels, so that the end-to-end spectral efficiency of the route exceeds a desired threshold. The transmit power level, however, has been assumed to be known, and route selection was considered in isolation. The work has been presented by the first rigorously proven optimal, polynomial-time algorithms for two versions of the joint spectral-efficient routing and power allocation problem they are sum-power minimization and maximum power minimization. The algorithms relied on the Divide-and-Conquer principle and the Bellman-Ford algorithm for shortest (or widest) path computation.

***C. Wang, H.M. Wang, and X.-G. Xia* [12]**studied the cooperative transmission for securing a Decode and Forward (DF) two-hop network where multiple cooperative nodes coexist with a potential eavesdropper. Further down the more practical assumption that only the Channel Distribution Information (CDI) of the eavesdropper is known, and proposed an opportunistic relaying with artificial jamming secrecy scheme, where a “best” cooperative node is chosen among a collection of N possible candidates to forward the confidential signal and the others send jamming signals in order to confuse the eavesdroppers. At first investigated the Ergodic Secrecy Rate (ESR) maximization problem by optimizing the power allocation between the confidential signals and jamming signals. In particular, to exploit the limiting distribution technique of extreme order statistics to build an asymptotic closed-form expression of the achievable ESR and the power allocation was optimized to maximize the ESR lower bound. Although the optimization problems are non-convex, proposed a Sequential Parametric Convex Approximation (SPCA) algorithm to locate the Karush- Kuhn-Tucker (KKT) solutions. Also, the time variance of the legitimate links Channel State Information (CSI) are taken into consideration, and addressed the impacts of the outdated CSIs to the proposed secrecy scheme, and derived an asymptotic ESR. Finally, generalized the analyzed scenario with multiple eavesdroppers, and given the asymptotic analytical results of the achievable ESR.

***J. Li, A. Petropulu, and S. Weber* [13]** considered a cooperative wireless network in the presence of one or more eavesdroppers, and exploit node co-operation for achieving physical (PHY) layer based security. Two different co-operation schemes were considered. The first scheme, cooperating nodes retransmit a weighted version of the source signal in a Decode and Forward (DF) relay. And the second scheme, referred to as cooperative jamming (CJ), while the source is transmitting, cooperating nodes transmit weighted noise to confound the eavesdropper.

The investigation was made on two objectives: i) maximization of the achievable secrecy rate subject to a total power constraint and ii) minimization of the total power transmit power under a secrecy rate constraint. For the first design objective, need to obtain the exact solution for the DF scheme for the case of a single or multiple eavesdroppers, while for the CJ scheme with a single eavesdropper have reduced the multivariate problem to a problem of one variable. For the second design objective, work introduced additional constraints in order to reduce the degree of difficulty, thus resulting in suboptimal solutions. This work raised those constraints, and obtained either an analytical solution for the DF scheme with a single eavesdropper, or reduces the multivariate problem to a problem of one variable for the CJ scheme with a single eavesdropper.

***C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang* [14]** considered the Device-to-device (D2D) communication underlying cellular networks which were a promising technology to improve network resource utilization. In D2D-enabled cellular networks, interference generated by D2D communications was usually viewed as an obstacle to cellular communications. However, a new perspective was presented on the role of D2D interference by taking security issues into consideration. While concerning with a large-scale D2D-enabled cellular network with eavesdroppers overhearing cellular communications. By the usage of stochastic geometry model such a network and analyzed the Signal-to-Interference plus Noise Ratio (SINR) distributions, connection probabilities and secrecy probabilities of both the cellular and D2D links. There are two proposed criteria for guaranteeing the performances of secure cellular communications, namely the strong performance guarantee criteria and weak performance guarantee criteria. Based on the analytical results of link characteristics and the design of optimal D2D link scheduling schemes are the two criteria respectively. Both analytical and numerical results are shown that the interference from D2D communications enhanced the physical layer security of cellular communications and at the same time created extra transmission opportunities for D2D users.

***H. Wang, X. Zhou, and M. Reed* [15]** studied the information-theoretic secrecy performance in large-scale cellular networks based on a stochastic geometric framework. The locations of both base stations and the mobile users were modeled as independent two-dimensional Poisson Point Processes (PPP). The study contains two important features of cellular networks, namely, information exchange between base stations and cell association, to characterize their impact on the achievable secrecy rate of an arbitrary downlink transmission with a certain portion of the mobile users acting as potential eavesdroppers. In particular, tractable results are presented under diverse assumptions on the availability of eavesdropper's location information at the serving base station, which captured the benefit from the exchange of the location information between base stations.

***C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang* [16]** discussed about the relay transmission which can enhance coverage and throughput, while it can be vulnerable to eavesdropping attacks due to the additional transmission of the source message at the relay. Thus, whether or not one should use relay transmission for secure communication is an interesting and important problem. Meanwhile the transmission of a confidential message is taken into consideration from a source to a destination in a decentralized wireless network in the presence of randomly distributed eavesdroppers. The source-destination pair can be potentially assisted by randomly distributed relays. The arbitrary relay was used to derive exact expressions of secure connection probability for both colluding and non-colluding eavesdroppers. Then the obtained lower bound expression on the secure connection probability, are accurate when the eavesdropper density is small. By means of utilizing these lower bound expressions, a relay selection strategy was proposed to improve the secure connection probability. Through analytically comparing the secure connection probability for direct transmission and relay transmission, were addressed the important problem of whether or not relay transmission for secure communication and discussed about the conditions for relay transmission in terms of the relay density and source-destination distance.

III. METHODOLOGY

The proposed architecture accepts the simulation parameters as input which contains the NS2.34 simulation for the Dijkstra's algorithm is applied to the multi-hop wireless ad hoc network with randomize and forward strategy with OLSR. This overall proposed architecture in the fig. 3 follows a routine procedure form start to end state.

A. *Proposed System*

The proposed system presents a modification in the secure routing protocol with Randomizeand Forward (RF) strategy using the Optimized Link State Protocol (OLSR) with the Multi-Point Relay (MPR) and implementing it using the Dijkstra's algorithm for the secure connection probability (SCP) for the network lifetime without losses of performance (in terms of throughput, end-to-end delay or overhead). Additionally, proposed system proves that the exclusion of the energy consumption due to the overhearing can extend the lifetime of the nodes without compromising the routing functioning at all. The following algorithm describes the implementation of finding the shortest path for the secure connection.

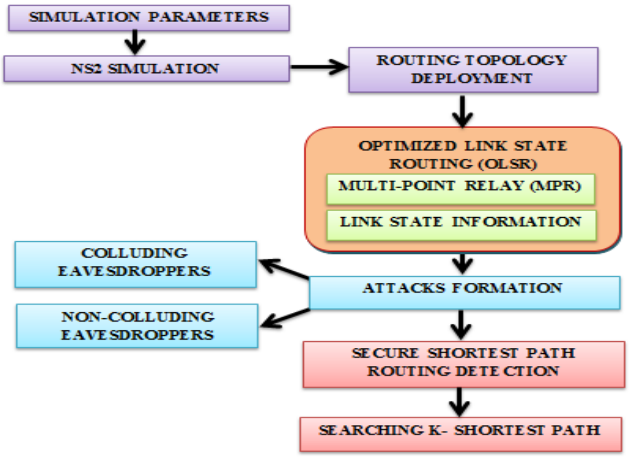

SIMULATION PARAMETERS
NS2 SIMULATION
ROUTING TOPOLOGY DEPLOYMENT
OPTIMIZED LINK STATE ROUTING (OLSR)
MULTI-POINT RELAY (MPR)
LINK STATE INFORMATION
COLLUDING EAVESDROPPERS
ATTACKS FORMATION
NON-COLLUDING EAVESDROPPERS
SECURE SHORTEST PATH ROUTING DETECTION
SEARCHING K- SHORTEST PATH

Fig. 3 Architecture of Proposed System

B. *Secure Shortest Path Routing Detection Algorithm*

Step 1: A source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes.

Step 2: While receiving the RREQ packet each node update their routing table

Step 3: Compare both Neighbor List (NL) and calculate the number of common neighbor nodes (common_node) present between sources to destination

```
        For i=0;i<number_of_source_neighbors;i++
For j=0;j<number_of_destination_neighbors;j++
      If (NLS(i) =NLD(J))
Common _node++;
```

Step 4: Initialize one hop neighbors can reach target node with maximum of 3 hops and minimum of 1 hop. If maximum target_hop_count exceeds 3 then target node and their previous hop may be the attacker node.

Step 5: If target_node_count>node_count_thresh then declare the target node and their previous hop nodes are attacker nodes.

Step 6: Send attacker announcement message to all nodes.

Step 7: Any node receives attacks announcement message it removes attacker node id from its Neighbor Table and Routing Table.

The secure shortest path routing detection algorithm predicts the distributed attacks (Colluding and Non-Colluding) in the wireless ad hoc network. In the detection scheme, every node in the network monitors the behavior of its neighbors and upon detecting any abnormal action by any of its neighbors invokes a distributed algorithm to ascertain whether the node behaving abnormally is indeed malicious. The protocol works through co-operation of some security components that are present in each node in the networks.The components are as follows:

Discovery: Each node passively listens to the communication to and from each of its neighbors. For detecting packet drops and modifications by the neighboring nodes, the monitor module of a node randomly copies the incoming packets to its neighbors and checks whether the neighbors really forward the packets with contents unchanged, or drop them, or modify the contents before forwarding them. The collected data is audited by the monitor. The deviation from normal behavior of a neighbor is used as an indicator for the unbiased degree of maliciousness, because this is independent of the past behavior of the neighbor node. If this unbiased deviation exceeds a preset threshold, the trust collector module of the node is invoked.

Trust Collector: A node invokes a majority consensus algorithm among the neighbors of a node that has been suspected to be malicious. On being activated by its discovery module, the (accuser) node that has suspected some malicious activity by one of its neighbors challenges the suspicious node to verify its behavior as observed by all of its neighbors. The accused (suspected) node on receiving the challenge responds by acknowledging the message and sending a verify behavior message to all of its neighbors. The neighbors respond by sending the observed value of the degree of maliciousness of the accused node. The accused node calculates the group's trust in its behavior using the received values and broadcasts the computed group-trust along with the received responses to all the neighbors. The messages are also time-stamped so as to prevent replay attacks. For computing group trust value from the received responses, any consensus-based scheme can be used. In the proposed scheme, the difference of the absolute trust values and the average degree of maliciousness of the majority of the respondents (neighbors) has been taken as the final group-trust value of the node. Majority among the neighbors has been taken as the larger of the two subsets of nodes obtained by partitioning the nodes on the basis of a preset threshold value of trust.

Trust Manager: Each node in the network maintains a global trust state containing the suspected nodes and their trust values. A routing table is also maintained that contains a list of nodes that has been determined to be malicious and thus should not be allowed any access to the network resources. The trust manager of a node is responsible for verifying the correctness of the group trust certificate received, caching them, and updating the global trust state (table) of the node for which it has received a new group certificate (from the neighbors of a suspected node). While verifying the correctness, the trust manager must check whether the response from every neighbor node has been correctly considered in computing the group- trust by the suspected node, and the messages have not been tampered with.The host maintains the routing table, the routing table entries have following information: destination address, next address, number of hops to the destination and local interface address. Next address indicates the next hop host. The information is got from the topological set (from that messages) and from the local link information base (from the Hello messages). So if any changes occur in these sets, then the routing table is recalculated. Because this is proactive protocol then the routing table must have routes for all available hosts in the network. The information about broken links or partially known links is not stored in the routing table.The routing table is changed if the changes occur in the following cases: neighbor link appear or disappear, two hops neighbor is created or removed, topological link is appeared or lost or when the multiple interface association information changes. But the update of this information does not lead to the sending of the messages into the network. For finding the routes for the routing table entry the shortest path algorithm is used.

C. Steps Involved In Proposed System

The following are the steps involved in the proposed system.

Network Model: The network model is concerned with the Distributed Path Vector (DPV) protocol with respect to the Optimized Link State Routing (OLSR) protocol. It is a proactive routing protocol, so the routes are can be easily determined based on the necessity. DPV is an optimization version of a pure link state protocol. So 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 uses *Multipoint Relays (MPR).* The idea of MPR is to reduce flooding of broadcasts by reducing the same broadcast in some regions in the network. And it also used to provide the shortest path which reduces the time interval for the control message transmission that can bring more reactivity. The DPV uses two kinds of the control messages: *Hello and Topology Control (TC).*Hello messages are used for finding the information about the link status and the host's neighbors. With the Hello message the Multipoint Relay (MPR) Selector set is constructed which describes the information about all the neighbor nodes with the help of this MPR Selector Set the host will calculate its own MPR set. The Hello messages are sent only one hop away but the TC messages are broadcasted throughout the entire network. The TC messages are used for broadcasting information about own advertised neighbors which includes the MPR Selector list. The TC messages are broadcasted periodically and only the MPR hosts can forward the TC messages.

Mobility Modeling: The Random Waypoint Model (RWP) is one of the most widely used mobility models in performance analysis of ad hoc networks. The research work analyzes the stationary spatial distribution of a node moving according to the RWP model in a given convex area. For this it gives an explicit expression, which is in the form of a one-dimensional integral giving the density up to a normalization constant [32]. This result is also generalized to the case where the waypoints have a non-uniform distribution. Additionally, the modified RWP model, describes where the waypoints are on the path boundary. The analytical results are illustrated through numerical examples. Moreover, the analytical results are applied to study certain performance measures in ad hoc networks, namely connectivity and traffic load distribution.

In the Network Simulator (NS-2) distribution, the implementation of this mobility model contains with the start of the simulation, each mobile node randomly selects one location in the simulation field as the destination. It then travels towards the destination with constant velocity chosen uniformly and randomly from $[0,V]$, where the parameter V is the maximum allowable velocity for every mobile node. The velocity and direction of a node are chosen independently of other nodes. Upon reaching the destination, the node stops for a duration defined by the 'pause time' parameter. If T=0, this leads to continuous mobility. After this duration, it again chooses another random destination in the simulation field and moves towards it. The whole process is repeated again and again until the simulation ends.

In the Random Waypoint model, V_{max} and T_{pause} are the two key parameters that determine the mobility behavior of nodes. If the V_{max} is small and the pause time T_{pause} is long, the topology of ad hoc network becomes relatively stable. On the other hand, if the node moves fast (i.e.,V_{max} is large) and the pause time T_{pause} is small, the topology is expected to be highly dynamic. Varying these two parameters, especially the V_{max} parameter, the Random Waypoint model can generate various mobility scenarios with different levels of nodal speed.The proposed the Mobility Metric to capture and quantify this nodal speed notation. The measure of Relative Speed between node*i* and *j* at time *t* is given in the equation 1.

$$RS(i,j,t) = \left| V_i(t) - \frac{V_j(t)}{M} \right| \qquad (1)$$

Then, the Mobility Metric is calculated as the measure of relative speed averaged over all node pairs and over all time. The formal definition is as follows,

$$M = \frac{1}{|i,j|} \sum_{i=1}^{N} \sum_{j=i+1}^{N} \frac{1}{T} \int_0^T RS(i,j,t)dt \qquad (2)$$

According to the formula given in the equation 1, |*i*, *j*| is the number of distinct node pair (*i*, *j*), *n* is the total number of nodes in the simulation field (i.e.) ad hoc network, and *T* is the simulation time. Using this Mobility Model is used to roughly measure the level of nodal speed and also differentiates between the different mobility scenarios based on the level of mobility. The Relative Speed (RS) linearly and monotonically increases with the maximum allowable velocity.

Secure Routing Randomize And Forward (RF) Using Optimized Link State Routing (OLSR) Protocol: The secure routing of *RF* uses two kinds of the control messages: Hello and Topology Control (TC). Hello messages are used for finding the information about the link status and the host's neighbors. With the Hello message of OLSR protocol Multipoint Relay (MPR) Selector set is constructed which describes the information about all the neighbor nodes with the help of this MPR Selector Set the host will calculate its own MPRs set. The Hello messages are sent only one hop away but the TC messages are broadcasted throughout the entire network. TC messages are used for broadcasting information about own advertised neighbors which includes at least the MPR Selector list. The TC messages are broadcasted periodically and only the MPR hosts can forward the TC messages. The path in the mobile ad hoc network can be either unidirectional or bidirectional so the host must know this information about the neighbors. The control messages are broadcasted periodically for the neighbor sensing. The control messages are only broadcasted one hop away so that they are not forwarded further. When the first host sends the Hello message to the second host, at that time it makes an entry about the second host status to asymmetric in its routing table. Again when the first host sends control message which includes the link state information such as the link to the second host as asymmetric, the second host makes an entry in its routing table that the first host status to symmetric. Finally, when second host response back with the control message, where the status of the link for the first host is indicated as symmetric, then first host changes the status in its routing table entry of the second host from asymmetric to symmetric. At the end, both hosts know that their neighbor is alive and the corresponding link is bidirectional. The Control Messages (CM) is used for getting the information about local links and neighbors. The control messages are periodic broadcasting is used for link sensing, neighbor's detection and MPR selection process.

Control message contains the information of how frequently the host sends control messages, readiness of host to act as a Multipoint Relay, and information about its neighbor. Information about the neighbors contains the interface address, link type and neighbor type. The link type indicates that the link is symmetric, asymmetric or simply lost. The neighbor type is just symmetric, MPR or not a neighbor. The MPR type indicates that the link to the neighbor is symmetric and that this host has chosen it as Multipoint Relay.

IV. IMPLEMENTATION

The following are the process involved in the implementation.

Neighbor Node Discovery Using Multipoint Relay (MPR) Nodes: After the deployment of the nodes in the simulation area, each and every node in model will perform neighbor node discovery process. During this process all the links with neighbor nodes are declared and are flooded in the entire network. OLSR protocol is an optimization of a pure list state protocol. Because it reduces the size of control packets instead of all links, it declares only a subset of links with its neighbors who are its multipoint relay selectors. It also minimizes flooding of this control traffic by using only the selected nodes, called multipoint relays, to diffuse its messages in the network. Only the multipoint relays of a node retransmit its broadcast messages. This technique significantly reduces the number of retransmissions in a flooding or broadcast procedure. It is carried out with the help of the topology control (TC) packets which provides the assurance of the neighbor node's information. Hence with the help of the MPR nodes it is easy to discover the neighbor node's information. Subsequently all the nodes will maintain neighbor table in order to maintain the information of frequently changing node and node trust value. Node trust value is evaluated using neighbor's collective opinion. The *Node Trust Value (NTV)* of a *node i* will be calculated by the following formula:

$$NTV=[NNT(1)+NNT(2)+NNT(3)+\ldots\ldots+NNT(n)]/n \qquad (3)$$

where*NNT* is the *Neighbor Node Trust* value about the *node i* and *n* is the number of neighbors in the neighbor list.

Route Discovery: According to the assumption the source node and destination node are been emphasized among the other nodes. During route discovery, node has packets to send it broadcasts RREQ packets. When all RREQ reaches to the destination, it sends RREP packets. After receiving the RREP packets, source node selects three RREP packets that have high route trust value. Then the source node generates the TREQ packets and sends it to all neighbors' in the neighbor list of that RREP packet. After receiving the TREQ packet, all neighbors replies with TREP packet to the source node. Then the source node calculates the node trust of the nodes. Next, the source node arrange the RREP packets in the ascending order based on node trust value and selects the first RREP packet and hence that path is selected for communication.

Route Trust Calculation: Every node calculates route trust for each route in the routing table at some regular interval. Destination node in each entry in the routing table generates R_ACK packet and send back in reverse path. The nodes that receive R_ACK calculate the route trust value using the value in the no_of_packets_received_by_destination field of R_ACK packet and the value of no_of_packets_sent _by_source field in the routing table. Route trust value is calculated by the equation 4.

Route Trust= (no_of_ packets_ send by source – no_ of_ packets_ received_ by_destination) *(4)*

The route with route trust value 0 is the perfect one. If the route trust value is equal to the number of packets sent then the route will be rejected.

Finding Misbehaving Nodes: The trust manager handles *ALARM messages*. When any misbehaving node is found *ALARM messages* are sent to all other nodes to inform about that node. The trust manager maintain *alarm table* and *trust table* for checking the trustworthiness of alarm. The rating function assigns greater weights for own experience and smaller for other nodes opinion about that detected node. The rating of a node is updated when sufficient proof of the nodes maliciousness is found. If the rating falls below threshold value path manager module will be invoked.

Energy Saving Calculation: Nodes involved in the delivery process of packets losses some energy after each transmit and receive. Let *TP* be the *Transmit Power* for one packet, *TT* be the *Transmit Time* of one packet, and *ET* is the *amount of Energy consumed during Transmission* of one packet is given in the equation 5. Hence, *Remaining EnergyEnew* of node is given in the equation 6. Similarly, let *RP* be the *Receiving Power* for one packet, *RT* be the *Receiving Time* of one packet, and *ER* is the *amount of Energy consumed during Receiving* of one packet is given in the equation 7.

Hence, Remaining Energy Enew of node is given in the equation 8.

$$E_T = T_P \times T_T \qquad (5)$$

$$E_{new} = E_{curr} - E_T \qquad (6)$$

$$E_R = R_P \times R_T \qquad (7)$$

$$E_{new} = E_{curr} - E_R \qquad (8)$$

With the above mentioned equations calculations the energy of the node at any interval of time can be easily calculated.

Bandwidth Efficiency Aggregations: The trust based dynamic routing mechanisms based on channel sensing and the Secure distributed Map detection Algorithm. To begin with a discussion of our assumptions is stated as follows:

Single Transceiver: The nodes in the network are equipped with a transceiver that can operate in one of two modes; they are transmission mode or reception mode. Nodes cannot simultaneously transmit and receive.

Channel Sensing: The receiver node is able to detect the presence of a carrier signal and measure its power even for messages that cannot be decoded into a valid packet.

Collisions: In the case of simultaneous transmissions in the system, neither of the packets can be received unless one of the transmissions captures the receiver. The receiver can be captured if the power level of one of the transmissions is significantly larger than the power level of all other simultaneous transmissions. Such a capturing mechanism is the driving factor of the advantages gained through channel reuse.

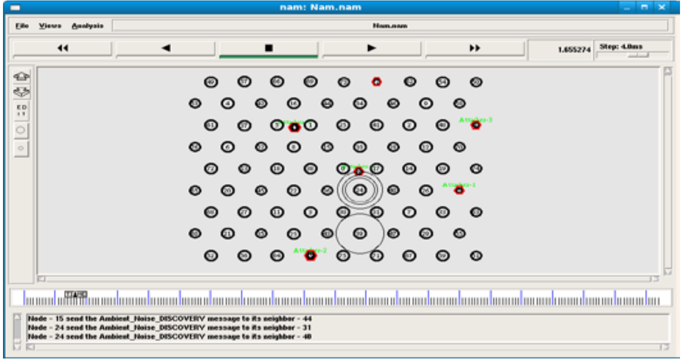
Channel Coordinators: The channel resources are managed and distributed by channel coordinators. These coordinators can be ordinary nodes that are selected to perform the duty, or they can be specialized nodes. The channel is provided to the nodes in the network for their transmission needs by these channel coordinators. The system is also assumed to be a closed system where all the nodes comply with the channel access rules.

V. EXPERIMENTAL RESULTS

In the proposed experimental network model nearly 83 nodes are taken for simulation process for both the colluding eavesdroppers case and non-colluding eavesdroppers case.

A. *Colluding Eavesdroppers Network Model*

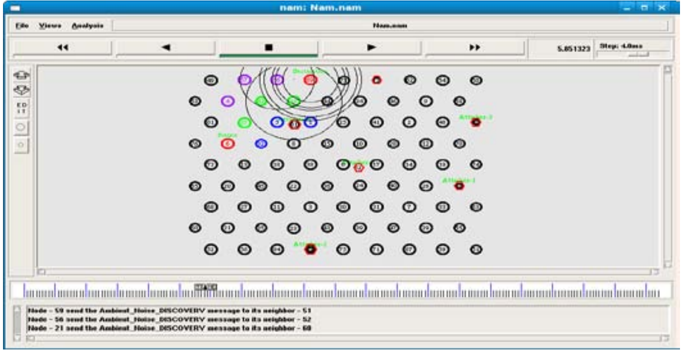
In this experimental network model contains totally 83 nodes are been created for handling the colluding eavesdroppers case. In that 78 nodes are taken for sending message and the starting node is numbered as 0 and the ending node is numbered as 77. The remaining 5 nodes are termed as Attacker 1, Attacker 2, Attacker 3, Attacker 4 and Attacker 5 are conisdered as the attacker nodes and it is called as the nodes deployment process with colluding eavesdroppers.The model broadcast a message to every node in the network and it stores route information in the routing table, such as the location of the nodes, distance and the number of neighbors based on the Multi-Point Relays (MPR) and it shown in the fig. 4.



Node - 15 send the Ambient_Noise_DISCOVERY message to its neighbor - 44
Node - 24 send the Ambient_Noise_DISCOVERY message to its neighbor - 31
Node - 24 send the Ambient_Noise_DISCOVERY message to its neighbor - 40

Fig. 4 Discovery of each Node's Neighbor Routing Information

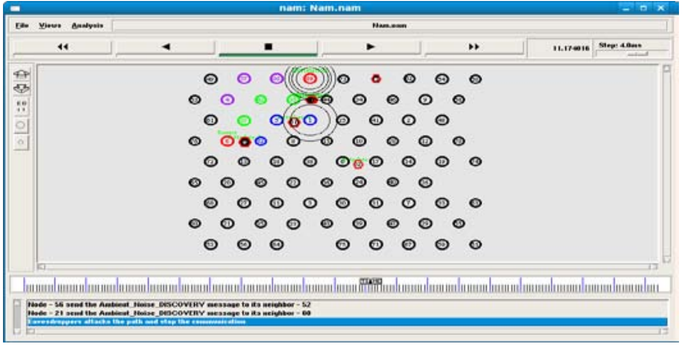
Let us assume the source node and the destination node and also chooses the available shortest paths between the source node and the destination node to send packets. This network model chooses the three different shortest paths between the source node and the destination node to send the packets. The three different shortest paths are listed as follows: Node 6→ Node 4→ Node 57→Node 67→ Node 69, Node 6→ Node 37→ Node 42→ Node 16→ Node 69 and Node 6→ Node 32→ Node 5→ Node 1→ Node 69. And the model discovers the shortest path using the Optimized Link State Routing Protocol (OLSR) with the help of the Multi-Point Relay (MPR). After selecting the shortest path the source node will initiate the packet transmission via all the three selected shortest paths to the destination node and it is illustrated in the fig. 5.



Node - 59 send the Ambient_Noise_DISCOVERY message to its neighbor - 51
Node - 56 send the Ambient_Noise_DISCOVERY message to its neighbor - 52
Node - 21 send the Ambient_Noise_DISCOVERY message to its neighbor - 60

Fig. 5 Sending Packets from Source Node to Destination Node

While sending the packets from source node to the destination node, the packet should be securely transmitted. For this reason the eavesdropper are always monitored in this network model. When an eavesdropper is detected at that point it is initiated to the source node for making the routing decision randomly. But at the same time in the colluding eavesdroppers case, it waits for more than one eavesdropper or colluding eavesdropper to make a routing decision for changing and truncating the existing route where the colluding eavesdroppers are detected.

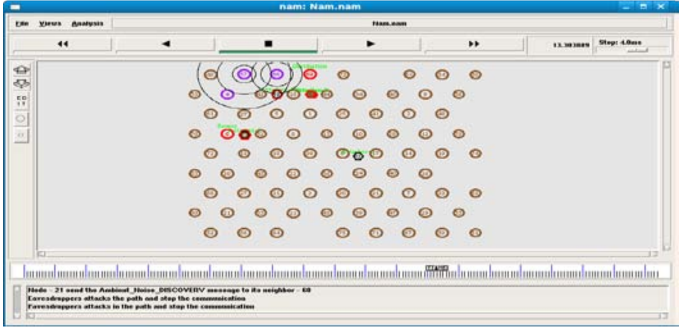


Node - 56 send the Ambient_Noise_DISCOVERY message to its neighbor - 52
Node - 21 send the Ambient_Noise_DISCOVERY message to its neighbor - 60
Eavesdroppers attacks the path and stop the communication

Fig. 6 Detection of Colluding Eavesdropper

When one of the Attacker nodes makes a move which may get onto the third secure path in order to monitor the packet transmission from the source to destination. At the same time another eavesdropper is been detected on the same path in the network model. Hence, the movements of the eavesdroppers are in a colluding manner. That is more than one eavesdropper are attempting to monitor the secured transmission of the same region. Again another eavesdropper is detected on the same shortest path. Hence, now it results in the condition of the colluding eavesdroppers which leads to the cancellation of those paths or links and it shown in the fig. 6. This means that the communication between the source node and the destination node via the above paths will be cancelled and those relay nodes will react as normal nodes and that will not be used further for the purpose of packet transmission between the source node and the destination node.

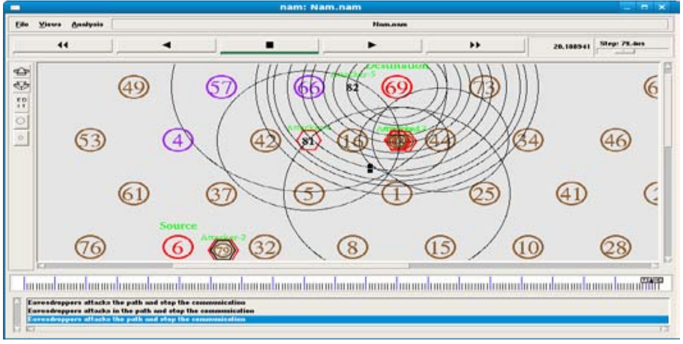
Now the experimental network model searches for the alternate shortest path to continue the packet transmission and it will do the shortest path selection between the source node and the destination node which does not contain the colluding eavesdroppers is chosen. When the movement of another set of eavesdroppers in a colluding manner to monitor the secured transmission of the same region. Again the process of sending packets from the source node to the destination node with the alternate selected shortest secured path begins as shown in the fig. 7.



Node - 21 send the Ambient_Noise_DISCOVERY message to its neighbor - 68
Eavesdroppers attacks the path and stop the communication
Eavesdroppers attacks in the path and stop the communication

Fig. 7 Sending Packets in the Alternate Secure Path

When the colluding eavesdroppers again attack the last available secured shortest path then automatically the packets get dropped.The reason is the secured shortest paths between the source node and the destination node are affected by colluding eavesdroppers. Hence, the packets are dropped to maintain the secure information transfer and it does not assure for successfully packet transmission as in the fig. 8. This creates a greater issue in this model.

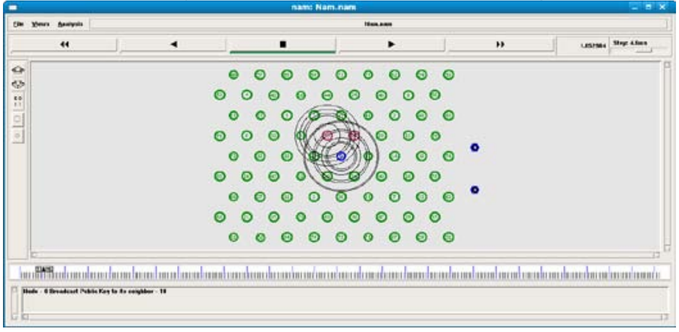


Eavesdroppers attacks the path and stop the communication
Eavesdroppers attacks in the path and stop the communication
Eavesdroppers attacks the path and stop the communication

Fig. 8 Packets are Dropped due to the Presence of Many Colluding Eavesdroppers

B. *Non-Colluding Eavesdroppers Network Model*

The Non-Colluding Eavesdroppers Case take place when one eavesdropper attack the secured path at the time of transmission of packets from the source node to the desired destination node. If there is a chance of attack and the eavesdropper who does it are called as the non-colluding eavesdropper. In other words, Non–Colluding Eavesdroppers are the eavesdropper who act in a independent manner while the communication between the source node and destination node exists. In the non-colluding eavesdropper experimental network model contains totally 83 nodes are been created for handling the non-colluding eavesdroppers case. In that 80 nodes are taken for sending message and the starting node is numbered as 0 and the ending node is numbered as 80. The remaining 2 nodes are termed as Attacker 1, and Attacker 2 are considered as the attacker nodes. The model broadcast a message to every node in the network and it stores route information in the routing table, such as the location of the nodes, distance and the number of neighbors based on the Multi-Point Relay (MPR) and it is shown in the fig. 9.

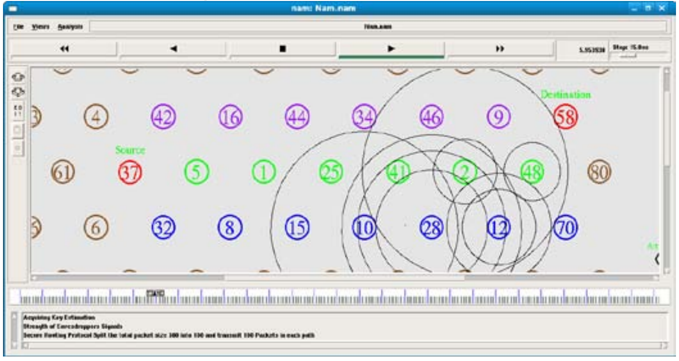


Node - 6 Broadcast Public Key to its neighbor - 18

Fig. 9 Discovery of each Node's Neighbor Routing Information

Let us assume the source node and the destination node and also chooses the available shortest paths between the source node and the destination node to send packets.This network model chooses the three different shortest paths between the source node and the destination node to send the packets. And the model discovers the shortest path using the Optimized Link State Routing Protocol (OLSR) with the help of the Multi-Point Relay (MPR). The selected three shortest paths are as follows: Node 37→Node 42→Node 16→Node 44→Node 34→ Node 46→ Node 9→Node 58, Node 37→ Node 5→Node 1→ Node 25→Node→ Node41→Node 2→Node 48→Node 58 and Node 37→ Node 32→Node 8→ Node 15→Node 10→Node 28→ Node 12→Node 70→ Node

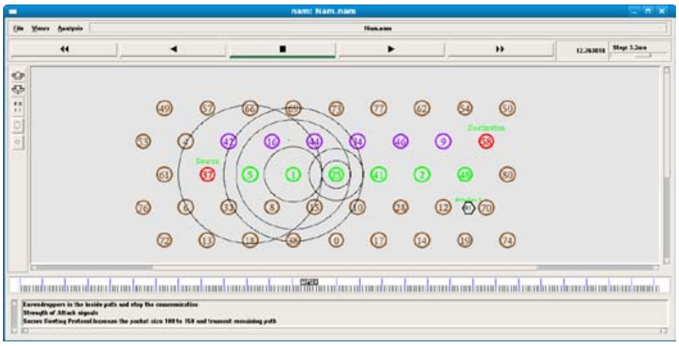
58.After selecting the shortest path the original packet size 300 is been equally segregated among three selected path (i.e.) each path will transmit the packet of size 100. This transmission of packet will occur between the source node and the destination node. After selecting the shortest path the source node will initiate the packet transmission via all the three selected shortest paths to the destination node and it is illustrated in the fig.10.



Acquiring Key Estimation
Strength of Eavesdroppers Signals
Secure Routing Protocol Split the total packet size 300 into 100 and transmit 100 Packets in each path

Fig. 10 Sending Packets from Source Node to Destination Node

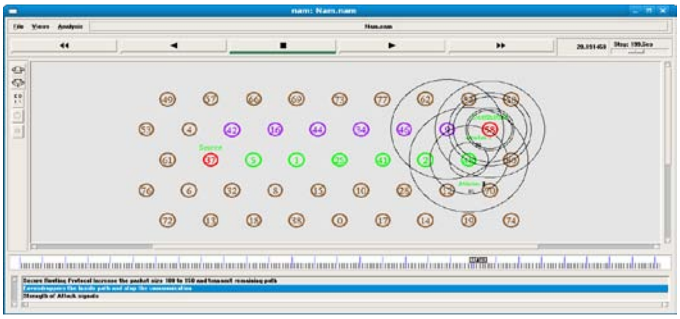
While sending the packets from source node to the destination node, the packet should be securely transmitted. For this reason the eavesdropper are always monitored in this network model. When an eavesdropper is detected then it is initiated to the source node for making the routing decision randomly. The Attacker 1 moves into one of the three secured shortest paths and considered that path as the third shortest path.An eavesdropper is detected on the secured shortest path. Hence, it results in the presence of non-colluding eavesdropper which leads to the cancellation of that path or link. This means that the communication between the source node and the destination node via the above path will be cancelled and those nodes will react as normal nodes and that will not be used further for the purpose of packet transmission between the source node and the destination node.



Eavesdroppers in the inside path and stop the communication
Strength of Attack signals
Secure Routing Protocol Increase the packet size 100 to 150 and transmit remaining path

Fig. 11 Sending Packets in the Rest of the Two Secured Paths

In the non-colluding eavesdroppers case, when an eavesdropper is found on the selected secure shortest path then the path or the link will get terminated also the nodes on that path will become as normal nodes and further it will not be used for sending packets from the source node to the destination node. And that respective packet of size 100 will be equally divided among the rest of available two paths that is now the source node will send the packets via the first and second secured shortest path in order to continue the communication with the destination node. Hence, now the packet of size 150 are transmitted through the paths or links from the source node to the destination node which help in proper secure connection and it is shown in the fig. 11.

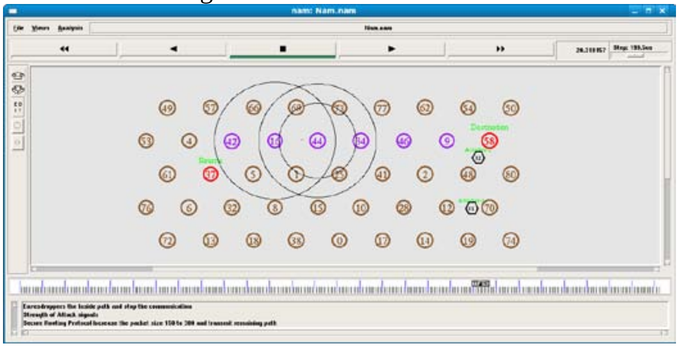


Secure Routing Protocol increase the packet size 100 to 150 and transmit remaining path
Eavesdroppers the inside path and stop the communication
Strength of Attack signals

Fig. 12 Detection of Eavesdropper in the Second Path hence it got Cancelled

The Attacker 2 which moves into one of the second secured shortest paths and considers that path as the second shortest path.An eavesdropper is detected on the secured shortest path. Hence, it results in the presence of non-colluding a eavesdropper which leads to the cancellation of that path or link. This means that the communication between the source node and the destination node through the above path will be cancelled and those nodes will react as normal nodes and that will not be used further for the purpose of packet transmission between the source node and the destination node and it is shown in the fig. 12.

In the non-colluding eavesdroppers case, when an eavesdropper is found on the selected secure shortest path then the path or the link will get terminated also the nodes on that path will become as normal nodes and further it will not be used for sending packets from the source node to the destination node. And that respective packet of size 150 will be assigned to the first secure connection path that is now the source node will send the packets via the first and second secured shortest path in order to continue the communication with the destination node. Hence, now packets are transferred only through a single path or link from the source node to the destination node which helps in proper secure connection is illustrated in the fig. 13.



Eavesdroppers the inside path and stop the communication
Strength of Attack signals
Secure Routing Protocol Increase the packet size 150 to 300 and transmit remaining path

Fig. 13 All the Remaining Packets are transferred with the First Secured Path

VI. PERFORMANCE EVALUATION

A. *Packet Delivery Ratio (PDR)*

It is defined as the ratio of the data packets delivered to the destinations to those generated by the Constant Bit Rate (CBR) sources. The EPDR shows how successful a protocol performs delivering packets from source to destination. The higher for the value give use the better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness.PDRis the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%) as given by the equation 9. This parameter is also called "success rate of the protocols", and is described as follows:

$$PDR = \left(\frac{\boldsymbol{SendPacketno}}{\boldsymbol{Receivepacketno}}\right) \times \mathbf{100} \qquad (\mathbf{9})$$

In the *colluding eavesdroppers case*, the delay during packet transmission is clearly represented in the fig. 14 wherein the *X-axis* represents the *time duration* for sending the packets from the source node to the destination node and the *Y-axis* represents the *delay duration* of the packet transmission. The delay is indicated by the yellow curve.

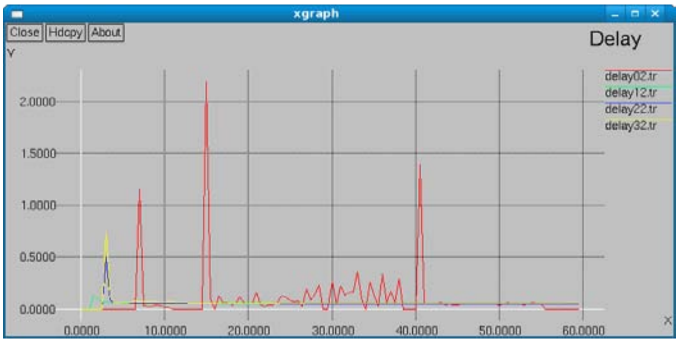


Fig. 14Delays during Packet Sending in Colluding Eavesdroppers Case

In the *non-colluding eavesdroppers case*, the *X-axis* represents the *time duration* for sending the packets from the source node to the destination node and the *Y-axis* represents the *packet delivery ratio percentage* and it is been depicted in the fig.15. And in the graph *red color* indicates the proposed research work of the non-colluding eavesdropper case and the *green color* indicates the existing research work of the non-colluding eavesdropper case and it is clear from the graph that the proposed work has optimized the secure routing and the packet delivery ratio is being maintained consistently.

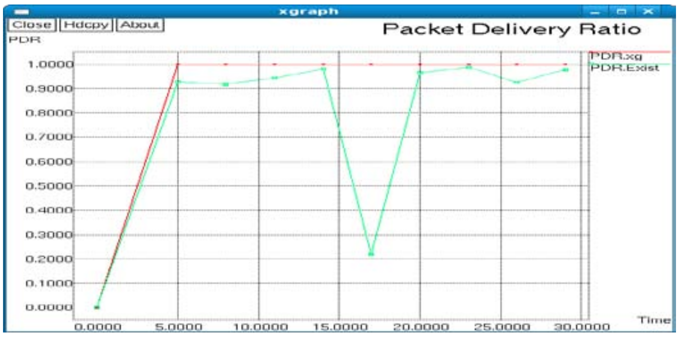


Fig. 15 Packet Delivery Ratios in Non-Colluding Eavesdroppers Case

B. *Throughput*

It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet is referred to as throughput. It is expressed in bits per second or packets per second. Factors that affect throughput include frequent topology changes, unreliable communication, limited bandwidth and limited energy. A high throughput network is desirable. It is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node.

$$\boldsymbol{X} = \frac{\boldsymbol{C}}{\boldsymbol{T}} \qquad (\mathbf{10})$$

where X is the throughput, C is the number of requests that are accomplished by the system, and T denotes the total time of system observation.

The *throughput* for the *colluding eavesdroppers case* is been depicted in the fig. 17 where the *X-axis* represents the *time taken* in seconds for the delivery of packets and *Y-axis* represents the *throughput ratio* that is accuracy of the packets delivery from the source node to the destination node which is also meant as the error rate ratio. Hence, it is clear from the graph that in this case the accuracy has strong variations in the throughput which may leads to the loss of packet or packet drop.

The *throughput* for *non-colluding eavesdroppers case* is been depicted in the fig. 18 where the *X-axis* represents the *time taken* in seconds for the delivery of packets and *Y-axis* represents the *throughput ratio* that is accuracy of the packets delivery from the source node to the destination node. In the graph the *red color* indicates the *proposed work* and the *green color* indicates the *existing work.* Hence, from the graph it is obvious that this case works better than the colluding eavesdroppers case because the throughput ratio is in an increasing manner.

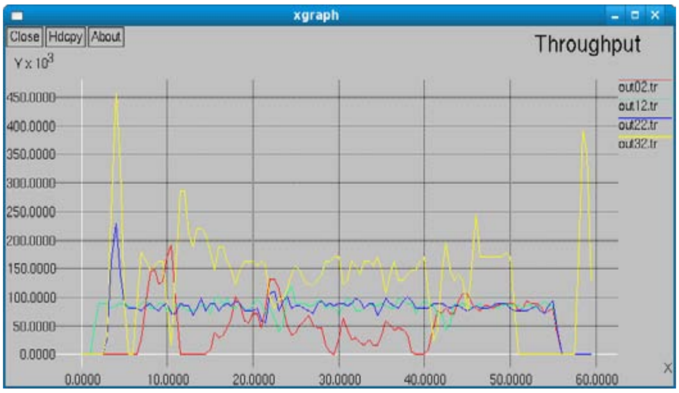


Fig.17 Throughput for Colluding Eavesdroppers Case

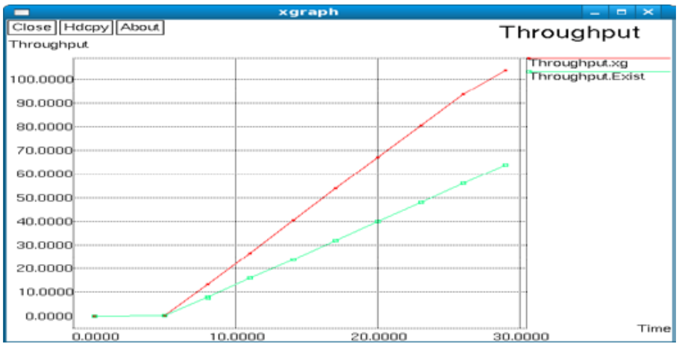


Fig.18 Throughput for Non-Colluding Eavesdroppers Case

C. *Packet Drop*

Data Packet Drop is also termed as Packet loss where the mobility-related packet loss may occur at both the network layer and the MAC layer. Here the packet loss concentrates for network layer. When a packet arrives at the network layer, the routing protocol forwards the packet if a valid route to the destination is known. Otherwise, the packet is buffered until a route is available. A packet is dropped in two cases: the buffer is full when the packet needs to be buffered and the time that the packet has been buffered exceeds the limit. The Constant Bit Rate (CBR) is taken into consideration in both the cases. In that for 1 second around 10 packets can be transmitted and each packet is 8 bits size.

The packet drop for the *colluding eavesdroppers case* is been depicted in the fig.19 where the *X-axis* represents the *time taken* and the *Y-axis* represents the *packet loss ratio*. This case results in severe packet loss and has variations in packet loss at different time intervals.

The packet drop *for non-colluding eavesdroppers case* is been depicted in the fig. 20 where the *X-axis* represents the *time taken* and the *Y-axis* represents the *packet loss ratio*. This case results in low packet loss ratio when compared with the colluding eavesdroppers case.

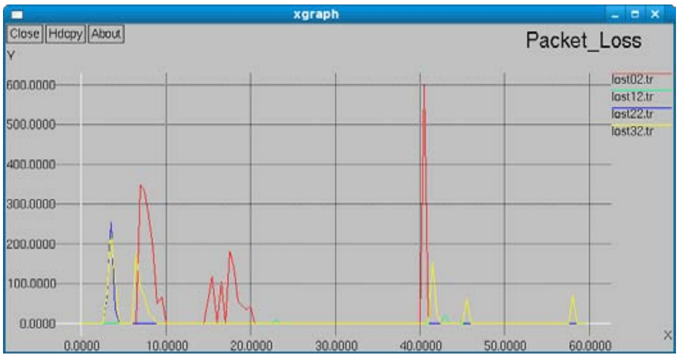


Fig. 19 Packet Drop in Colluding Eavesdroppers Case

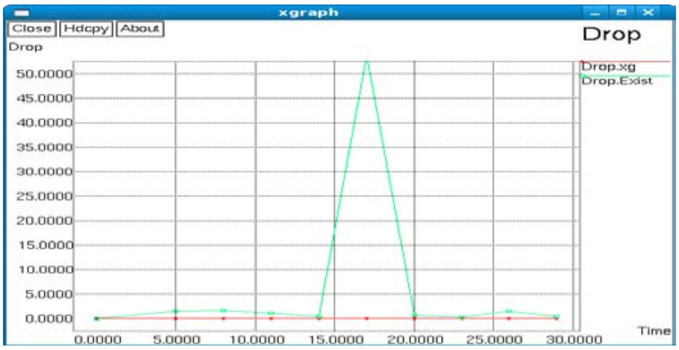


Fig.20 Packet Drop in Non-Colluding Eavesdroppers Case

VII. CONCLUSION AND FUTURE ENHANCEMENT

According the performance evaluation the packet delivery ratio, throughput and packet loss for both the colluding and non-colluding eavesdroppers network model are taken in consideration. From the resultant graphs both the cases the optimization of secure routing is been successfully implemented. Even then handling the non-colluding eavesdropper case is better than the colluding eavesdropper case. This research presents a new approach which combines the techniques from various fields and adapts to optimize the problem of secure routing, shortest path selection and packet delivery accuracy. The result generated using the above techniques are extremely relevant. It has been observed that as the packet delivery ratio and throughput prevents the quality of proposed system.

The goal of this research is designed, implemented and evaluated in a multi-hop wireless ad hoc network using Secure Routing Optimized Link State Routing (OLSR) and NS 2.34 Framework. Each secure routing path communicates wirelessly with another using the IEEE 802.11b technology without any aid of infrastructure. The main strategy implemented in this application was the *Randomize and Forward Strategy* using the *Optimized Link State Routing Protocol (RFOLSR)* consists of two important mechanisms. The mechanisms are the *Multipoint Relay (MPR)* and *Dijkstra's algorithm (K Shortest Path Routing).* Since the strategy operates exclusively based on source routing and on demand process, it has been selected as the routing protocol to be implemented and tested for multi-hop wireless ad hoc network. The mobility behavior of nodes in the application is modeled by the Random Waypoint (RWP) model through which random locations are generated, and the associated speed and pause time are specified to control the frequency at which the network topology is changed.The secure routing problem has been optimized in the multi-hop wireless ad hoc networks with two different experimental network models for both colluding eavesdroppers case and non-colluding eavesdroppers case. The proposed secure routing protocol finds the optimal path in a distributed way for both the cases.

In future the proposed work can be extended to use the other routing protocols, such as AODV, DSDV, DSR, geographical forwarding, and to compare against the RFOLSR protocol. In order to optimize the use of constrained resources in an ad hoc network, mobility prediction and battery power conservation techniques can be developed and experimented to test the effect of these ad hoc routing protocols on a real application.

VIII. REFERENCES

[1] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," IEEE Trans. Inf. Theory, Vol. 24, No. 3, pp. 339–348, May 1978.

[2] Shiann-TsongSheu, Tobias Chen, Jenhui Chen, and Fun Ye, "The Impact of RTS Threshold on IEEE 802.11 MAC Protocol," Proceedings of the Ninth International Conference on Parallel and Distributed Systems, 2002.

[3] R. Hekmat, "Fundamental Properties of Wireless Mobile Ad hoc Networks," KiVITelecommunicatieprijs, Netherlands, March 2004.

[4] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure Beam Forming for MIMO Two-Way Communications with an Untrusted Relay," IEEE Trans. Signal Process., Vol. 62, No. 9, pp. 2185–2199, May 2014.

[5] Y. Zou, X. Wang, and W. Shen, "Optimal Relay Selection for Physicallayer Security in Cooperative Wireless Networks," IEEE J. Sel. Areas Commun., Vol. 31, No. 10, pp. 2099–2111, Oct. 2013.

[6] Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial Noise Generation from Cooperative Relays for Everlasting Secrecy in Two-Hop Wireless Networks," IEEE J. Sel. Areas Commun., Vol. 29, No. 10, pp. 2067–2076, Dec. 2011.

[7] A.Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Jamming-Aware Minimum Energy Routing in Wireless Networks," in Proc. IEEE Int. Conf. Commun. (ICC), June 2014, pp. 2313–2318.

[8] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "On the Application of Cooperative Transmission to Secrecy Communications," IEEE J. Sel. Areas Commun., Vol. 30, No. 2, pp. 359–368, Feb. 2012.

[9] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "On the Throughput Cost of Physical Layer Security in Decentralized Wireless Networks," IEEE Trans. Wireless Commun., Vol. 10, No. 8, pp. 2764–2775, Aug. 2011.

[10] M. Saad, “Joint Optimal Routing and Power Allocation for Spectral Efficiency in Multi-Hop Wireless Networks,” IEEE Trans. Wireless Commun., Vol. 13, No. 5, pp. 2530–2539, May 2014.

[11] Wang, H.M. Wang, and X.G. Xia, “Hybrid Opportunistic Relaying and Jamming with Power Allocation for Secure Cooperative Networks,” IEEE Trans. Wireless Commun., Vol. 14, No. 2, pp. 589–605, Feb 2015.

[12] J. Li, A. Petropulu, and S. Weber, “On Cooperative Relaying Schemes for Wireless Physical Layer Security,” IEEE Trans. Signal Process, Vol. 59, No. 10, pp. 4985–4997, Oct. 2011.

[13] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, “Interference Exploitation in D2D-Enabled Cellular Networks: A Secrecy Perspective,” IEEE Trans. Commun., Vol. 63, No. 1, pp. 229–242, Jan. 2015.

[14] H. Wang, X. Zhou, and M. Reed, “Physical Layer Security in Cellular Networks: A Stochastic Geometry Approach,” IEEE Trans. Wireless Commun., Vol. 12, No. 6, pp. 2776–2787, May 2013.

[15] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, “When Does Relay Transmission give a More Secure Connection in Wireless Ad Hoc Networks?” IEEE Trans. Inf. Foren. Sec., Vol. 9, No. 4, pp. 624–632, Apr. 2014.

[16] Kulla, M. Hiyama, M. Ikeda, L. Barolli, V. Kolici, R. Miho, “MANET Performance for Source and Destination Moving Scenarios Considering OLSR and AODV Protocols”, Mobile Information Systems, Vol. 6, No. 4, 2010, pp. 325–339.

[17] Spaho, L. Barolli, G. Mino, F. Xhafa, V. Kolici, R. Miho, “Implementation of CAVENET and its Usage for Performance Evaluation of AODV, OLSR and DYMO Protocols in Vehicular Networks”, Mobile Information Systems, Vol. 6, No. 3, 2010, pp. 213–237.

[18] E. Kulla, M. Hiyama, M. Ikeda, L. Barolli, V. Kolici, R. Miho, “MANET Performance for Source and Destination Moving scenarios considering OLSR and AODV Protocols”, Mobile Information Systems, Vol. 6, No. 4, 2010, pp. 325–339.

[19] MegatZuhairi, HaseebZafar, David Harle, “The Impact of Mobility Models on the Performance of Mobile Ad Hoc Network Routing Protocol,” IETE Journal of Research, Vol.29, Issue 5, pages 414-20, 2012.

[20] J. Mo, M. Tao, and Y. Liu, “Relay Placement for Physical Layer Security: A Secure Connection Perspective,” IEEE Commun. Lett., Vol. 16, No. 6, pp. 878-881, June 2012

[21] X. Zhou, R. Ganti, and J. Andrews, “Secure Wireless Network Connectivity With Multi-Antenna Transmission,” IEEE Trans. Wireless Commun., Vol. 10, No. 2, pp. 425-430, Feb. 2011.

[22] P. C. Pinto, J. Barros, and M. Z. Win, “Secure Communication in Stochastic Wireless Networks - Part I: Connectivity,” IEEE Trans. Inf. Forensics Security, Vol. 7, No. 1, pp. 125-138, Feb. 2012.

[23] W. Ai, Y. Huang, and S. Zhang, “New Results on Hermitian Matrix Rank-One Decomposition,” Math. Programm., Vol. 128, No. 1-2, pp. 253–283, 2011.

[24] S. Shafiee and S. Ulukus, “Achievable Rates in Gaussian MISO Channels with Secrecy Constraints,” in Proc. IEEE Int. Symp. Inf. Theory, Jun. 2007, pp. 2466–2470.

[25] A. De Maio, Y. Huang, D. Palomar, S. Zhang, and A. Farina, “Fractional QCQP with Applications in ML Steering Direction Estimation for Radar Detection,” IEEE Trans. Signal Process., Vol. 59, No. 1, pp. 172–185, 2011.

[26] A. Khisti and G.Wornell, “Secure Transmission with Multiple Antennas I: The MISOME Wiretap Channel,” IEEE Trans. Inf. Theory, Vol. 56, No. 7, pp. 3088–3104, Jul. 2010.

[27] Z.-Q. Luo, W.-K.Ma, A.-C.So, Y. Ye, and S. Zhang, “Semi-Definite Relaxation of Quadratic Optimization Problems,” IEEE Signal Process Mag., Vol. 27, No. 3, pp. 20–34, 2010.

[28] N. Lee, J.-B. Lim, and J. Chun, “Degrees of Freedom of the MIMO Y Channel: Signal Space Alignment for Network Coding,” IEEE Trans. Inf. Theory, Vol. 56, No. 7, pp. 3332–3342, Jul. 2010.

[29] L. Sun, T. Zhang, Y. Li, and H. Niu, “Performance Study of Two-Hop Amplify-and-Forward Systems with Untrustworthy Relay Nodes,” IEEE Trans. Veh. Technol., Vol. 61, No. 8, pp. 3801–3807, 2012.

[30] J. Huang, A. Mukherjee, and A. Swindlehurst, “Secure Communication Via an Untrusted Non-Regenerative Relay in Fading Channels,” IEEE Trans. Signal Process., Vol. 61, No. 10, pp. 2536–2550, 2013.

[31] S. Xu and Y. Hua, “Optimal Design of Spatial Source-and-Relay metrices for a Non-Regenerative Two-Way MIMO Relay System,” IEEE Trans. Wireless Commun., Vol. 10, No. 5, pp. 1645–1655, May 2011.

[32] R. Wang and M. Tao, “Joint Source and Relay Pre Coding Designs for MIMO Two-Way Relaying Based on MSE Criterion,” IEEE Trans. Signal Process., Vol. 60, No. 3, pp. 1352–1365, Mar. 2012.

[33] A. Jeong and I.-M. Kim, “Optimal Power Allocation for Secure Multicarrier Relay Systems,” IEEE Trans. Signal Process., Vol. 59, No. 11, pp. 5428–5442, Nov. 2011.

[34] L. Dong, Z. Han, A. Petropulu, and H. Poor, “Improving Wireless Physical Layer Security Via Cooperating Relays,” IEEE Trans. Signal Process., Vol. 58, No. 3, pp. 1875–1888, Mar. 2010.

[35] A. Ng, E. Lo, and R. Schober, “Secure Resource Allocation and Scheduling for OFDMA Decode-and-Forward Relay Networks,” IEEE Trans. Wireless Commun., Vol. 10, No. 10, pp. 3528–3540, Oct. 2011.

[36] J. Mo, M. Tao, and Y. Liu, “Relay Placement for Physical Layer Security: A Secure Connection Perspective,” IEEE Commun. Lett., Vol. 16, No. 6, pp. 878–881, Jun. 2012.

[37] Z. Ding, M. Xu, J. Lu, and F. Liu, “Improving Wireless Security for Bi-directional Communication Scenarios,” IEEE Trans. Veh. Technol., Vol. 61, No. 6, pp. 2842–2848, Jul. 2012.

[38] A. Mukherjee and A. L. Swindlehurst, "Securing Multi-Antenna Two-Way Relay Channels with Analog Network Coding Against Eavesdroppers," in Proc. IEEE 11th Int Signal Process. Adv. Wireless Commun. (SPAWC) Workshop, 2010, pp. 1–5.

[39] H.-M. W. Wang, M. Luo, Q. Yin, and X.-G.Xia, "Hybrid Cooperative Beam forming and Jamming for Physical-Layer Security of Two-Way Relay Networks," IEEE Trans. Inf. Forensics Security, Vol. 8, No. 12, pp. 2007–2020, 2013.

[40] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-Layer Secret Key Agreement in Two-Way Wireless Relaying Systems," IEEE Trans. Inf. Forensics Security, Vol. 6, No. 3, pp. 650–660, Sep. 2011.

[41] Huijuan Wang et. al , "Application of Dijkstra Algorithm in Robot Path-Planning", Second International Conference on Mechanic Automation and Control Engineering (MACE), pp. 1067 - 1069 ,2011.

[42] Liu Xiao-Yan, Chen Yan-Li, "Application of Dijkstra Algorithm in Logistics Distribution Lines", Proceedings of the Third International Symposium on Computer Science and Computational Technology (ISCSCT '10) 14-15,August 2010, pp. 048-050.

[43] Radwan S. Abujassar and Mohammed Ghanbari, "Efficient Algorithms to Enhance Recovery Schema in Link State Protocols", international journal of ubicomp (iju), Vol.2, No.3 ,july 2011 doi:10.5121/iju.2011.2304 53

[44] Dr. S. Mythili and A. Anitha, "An Overview of MANET and Unicast Routing Protocols", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6, No. 1, Jan. 2016.

[45] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L.Viennot,"Optimized Link State Routing Protocol for Ad Hoc Networks", In Multi Topic Conference, 2001, IEEE INMIC 2001, Technology for the 21st Century, Proceedings, IEEE International (pp. 62-68).