IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Comparative Analysis of Improved Path Selection Using PSO

[1] Sumit; [2] Karuna Ghai

[1] *M.Tech Student,* Department of Computer Science and Engineering
Bharat Institute of Technology, Sonepat

[2]*Associate Professor (CSE),* Bharat Institute of Technology, Sonepat

Abstract - In recent years, a broad research has been done in the domain of Mobile Ad-hoc Networks(MANETs). Due to the bounded resources in MANETs, to develop a reliable and efficient routing approach is still a threat or issues. There are distinct aspects appropriate for research like synchronization, power consumption, routing, bandwidth consideration, etc. This paper concentrates on routing approach which is the major challenging concern due to the change in topology of ad-hoc networks. Under a number of network scheme, such as network topology and size, it is difficult to figure out which routing protocol may perform well. In this paper we contribute an outline of broad range of the current routing approaches, with a special focus on their functionality and characteristics. Also based on the routing information and methodologies the comparison is provided, which can be use to make decisions of routing. Performance of all the routing protocols are considered as well. Further this consideration will benefit the researcher to get an outline of the existing protocols and advice which protocols may have better performance with respect to changing network scenario.

Keywords - *MANET, PSO, TORA, Routing Protocol, Performance*

1. Introduction

A Mobile ad hoc network is a group of wireless mobile computers and it is a self-configuring network of mobile routers connected by wireless links. In which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. A MANET is an autonomous group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly and unpredictably over time, because the nodes are mobile. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves.

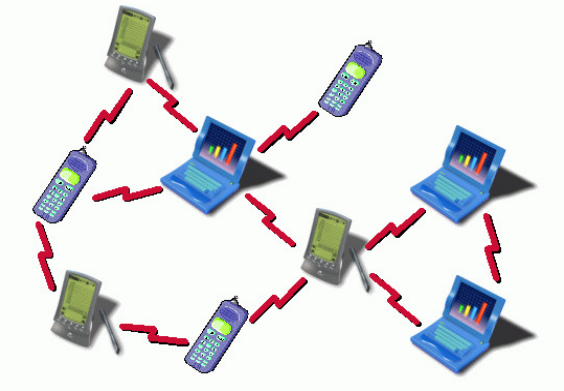

Fig 1: MANET

2. Routing Approaches in MANET

Routing approaches for MANETs can be divided into three classes on the basis of routing information update technique. Classification of routing protocols in mobile ad hoc network can be done in many ways, but most of these are done depending on routing strategy and network structure.

They could be Proactive (Table-driven), Reactive (On-demand) and Hybrid. Figure 2 shows the three classes of routing approaches in MANET. Proactive MANET protocols are also called as table-driven protocols and will actively determine the layout of the network.

In this approaches all the paths are maintained all the times so routes can be found anytime. The main properties of proactive approaches are that it uses the low latency in discovering the new path. It uses the more bandwidth to update routing knowledge. Reactive approach does not initiate for finding the paths. By flooding a query it establishes routes on demand. When finding a route it uses bandwidth only when there is a need for discovering the routes.

So, its latency is high. In this approach due to flooding there is a network overhead for query for finding the routes. Hybrid approach merges the advantages of above two approaches.

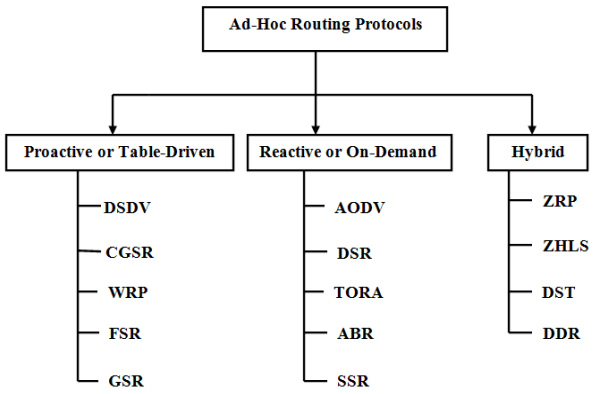

Fig 2: Classification of Routing Protocols

3. Particle Swarm Optimization

The Particle Swarm Optimization algorithm is based on certain social behaviours observed in flocks of birds, schools of fish, etc., from which certain aspects of intelligence emerge. After its development by Kennedy and Eberhart in 1995, this evolutionary paradigm has been seriously studied on and grown in the past decade. The standard PSO model consists of a swarm of particles, moving interactively through the feasible problem space to find new solutions. Each particle has a position represented by a position vector; where *i* is the index of the particle, and a velocity represented by a velocity vector.

Each particle remembers its own best position so far in the vector p_{best} and the best position vector among the swarm is stored in a vector g_{best} the search for the optimal position (solution) advances as the particles' velocities and positions are updated. In every iteration, the fitness of each particle's position is calculated using a pre-defined fitness function and the velocity of each particle is updated using the *gbest* and *pbest* which were previously defined. A particle's velocity and position are updated as follows:

$$v_{id} = wv_{id} + c_1 r_1(p_{Best} - x_{id}) + c_2 r_2(g_{Best} - x_{id});$$
$$i = 1,2,....., N, \text{ and } d = 1,2,....,D$$
$$x_{id} = x_{id} + v_{id}$$

Particle Swarm Optimization optimizes an objective function by undertaking a population based search. The population consists of potential solutions, named particles, which are metaphor of birds in flocks. These particles are randomly initialized and freely fly across the multi dimensional search space. During flight, each particle updates its own velocity and position based on the best experience of its own and the entire population.

The various steps involved in Particle Swarm Optimization Algorithm are as follows:

Step 1: The velocity and position of all particles are randomly set to within pre-defined ranges.

Step 2: **Velocity updating –** At each iteration, the velocities of all particles are updated according to,

$$v_i = v_i + c_1 R_1 (p_{i,best} - p_i) + c_2 R_2 (g_{i,best} - p_i)$$

where p_i and v_i are the position and velocity of particle i, respectively; $p_{i,best}$ and $g_{i,best}$ is the position with the 'best' objective value found so far by particle i and the entire population respectively; w is a parameter controlling the dynamics of flying; R_1 and R_2 are random variables in the range [0,1]; c_1 and c_2 are factors controlling the related weighting of corresponding terms. The random variables help the PSO with the ability of stochastic searching.

Step 3: **Position updating –** The positions of all particles are updated according to,

$$p_i = p_i + v_i$$

After updating, p_i should be checked and limited to the allowed range.

Step 4: **Memory updating –** Update $p_{i,best}$ and $g_{i,best}$ when condition is met,

$$p_{i,best} = p_i \quad if\ f(p_i) > f(p_{i,best})$$
$$g_{i,best} = g_i \quad if\ f(g_i) > f(g_{i,best})$$

where f(x) is the objective function to be optimized.

Step 5: **Stopping Condition –** The algorithm repeats steps 2 to 4 until certain stopping conditions are met, such as a pre-defined number of iterations. Once stopped, the algorithm reports the values of g_{best} and $f(g_{best})$ as its solution.

PSO utilizes several searching points and the searching points gradually get close to the global optimal point using its pbest and gbest. Initial positions of pbest and gbest are different. However, using thee different direction of pbest and gbest, all agents gradually get close to the global optimum.

4. Problem Formulation

4.1 Problem Statement:

Energy and efficiency are always the main concern in wireless Mobile network. A mobile network contains huge amount of data transmission over the network. In this work we have combined the Path Selection Routing along with the concept of PSO. The initial route will be identified by the Path Selection algorithm and in case of any broken link or intrusion in the path it will look for the Alternate path using Swarm optimization.

The presented work is divided in two main stages. In first stage, the path selection algorithm will be defined over the network as the optimized path. After the path generation, some agents will be distributed over the network to monitor the network and to identify the broken link over the network. As the broken link will

be identified, the PSO will be identified to find an optimimal route from the broken link position to the destination.

The objective function is defined as follows:

$$f = min\left(\sum_{i,j\in V}^{N}(w_{i,j})\, I_{i,j}\right)$$

$$s.t. \qquad \sum_{j=1}^{N} I_{i,j} - \sum_{j=1}^{N} I_{j,i} = \begin{cases} 1, & i = 1 \\ 0, & i = 2,3,\ldots,N-1 \\ -1, & otherwise \end{cases}$$

$$I_{j,i} \in \{0,1\}, \quad \forall\,(i,j)$$

Fig 3: Schematic Diagram Showing Iteration for PSO

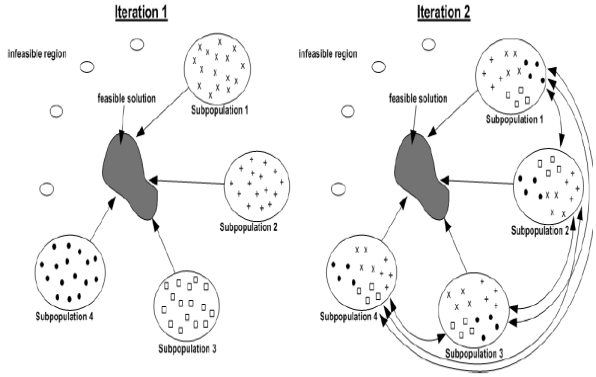

Fig 4: to illustrate the population interaction for the search model

4.2 Objectives

The proposed research work is about to achieve the following research objectives:

- Study and analyze existing shortest path techniques in MANET
- Define a Mobile Network along with specific energy based parameters.
- Detection of Broken link or intrusion over the network
- Design an Improved Path Selection Algorithm that is inspired from PSO
- Implementation of proposed algorithm in Matlab Environment.
- Analysis of Results

5. Proposed Work and implementation

5.1 Formulation of Hypothesis

A Wireless Mobile network is a dynamic network with large no. of nodes. As the traffic increases over the network such type of network suffers from the problems like congestion and packet loss. A Mobile network is always open for all nodes over the network. If the network is wireless in such case there are more chances of inclusion of some external node in the network. The complete solution is defined in terms of two stages. In first stage we have to find the node that is responsible for packet loss over the network. Another stage is the development of algorithm or approach that will eliminate the node dynamically and get the reliable data transmission over the network.

5.2 Research Methodology

Our proposed algorithm is based on **two basic** approaches:

1. Right Path Selection Algorithm
2. Swarm Optimization Algorithm

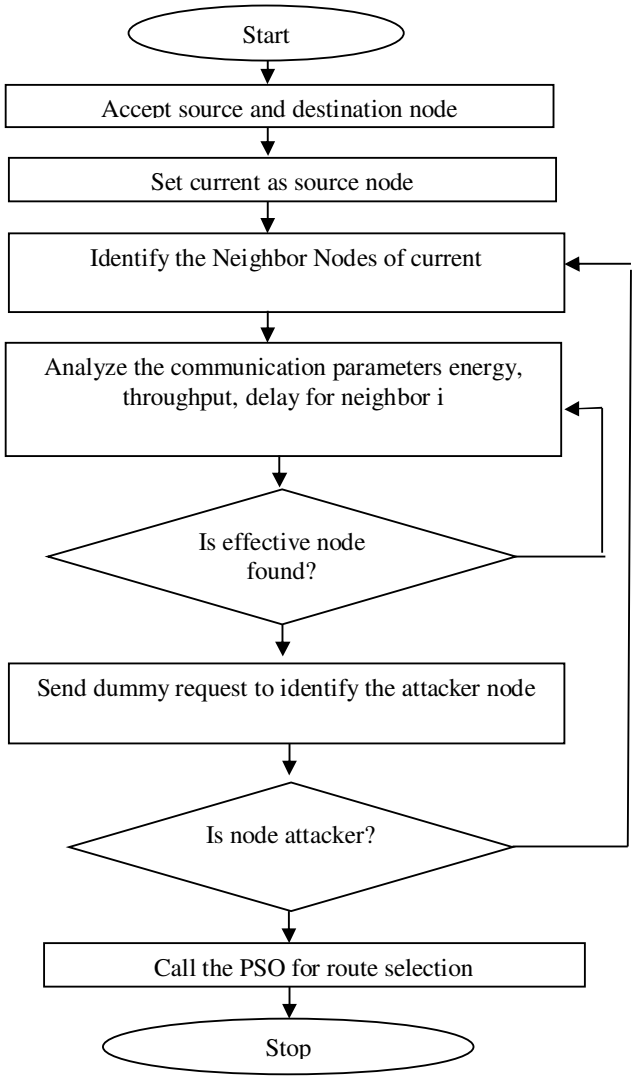

Fig 5: Algorithmic approach of the work

5.2.1 Right Path Selection

In an adhoc network, distance is the major factor respective to which routing algorithm is used. The parameters included in this work are

(i) Distance
(ii) Energy
(iii) Effective Throughput
(iv) Load Analysis

Now to perform the effective communication between the source and the destination the effective parameters are required to identify for each neighbor node of current node.

5.2.2 Swarm Optimization Algorithm

In this work, the parametric analysis is performed on each node to identify the best neighbor. The parameters considered here are the throughput analysis, energy, delay analysis on each node. As the parameters are identify for all the neighbors, best neighbour is selected from the list. Now it will check the node for valid node. Set this node as the best neighbour and the communication will be performed over that node. If reply is not accurate, the attacker node is identified.

Hence we achieved efficiency in terms of energy by applying path selection whereas Swarm Optimization Algorithm gives the required reliability.

6. Discussions and Results

6.1 Simulation Tool

1) MATLAB Editor is used for writing the code to implement our algorithm.
2) The result will be shown in the command window of MATLAB.

An Overview of Matlab Environment

MATLAB is a high-level language and interactive environment that enables you to perform computationally intensive tasks faster than with traditional programming languages such as C, C++, and Fortran.

6.2 Network Design

The proposed work is about to find the optimal solution of any broken link or data loss in a high speed Wireless LAN. The proposed work is about the generation of such an approach that will dynamically compensate the problem of link failure and provide the optimize solution without any data loss.
The proposed system will give the benefit in terms of Efficiency and accuracy. The network is designed with some defined parameters given as

6.2.1 Scenario 1

Parameter	Value
• Number of Nodes	10
• Topography Dimension	100m x 100m
• Traffic Type	CBR
• Topology	Random
• Initial Node	1
• Destination Node	10

The proposed work is about to introduce a compromising path to transfer data from some safe route if there are some chances of occurring of any intrusion or the congestion in the route of the basic routing algorithm.
The results obtained from the work are shown here:

6.2.2 Results

The network is defined with 10 number of nodes from 1 to 10. Blue nodes are showing source and destination node. Other nodes are the intermediate nodes. We have first implemented the shortest path algorithm used by DSDV protocol.

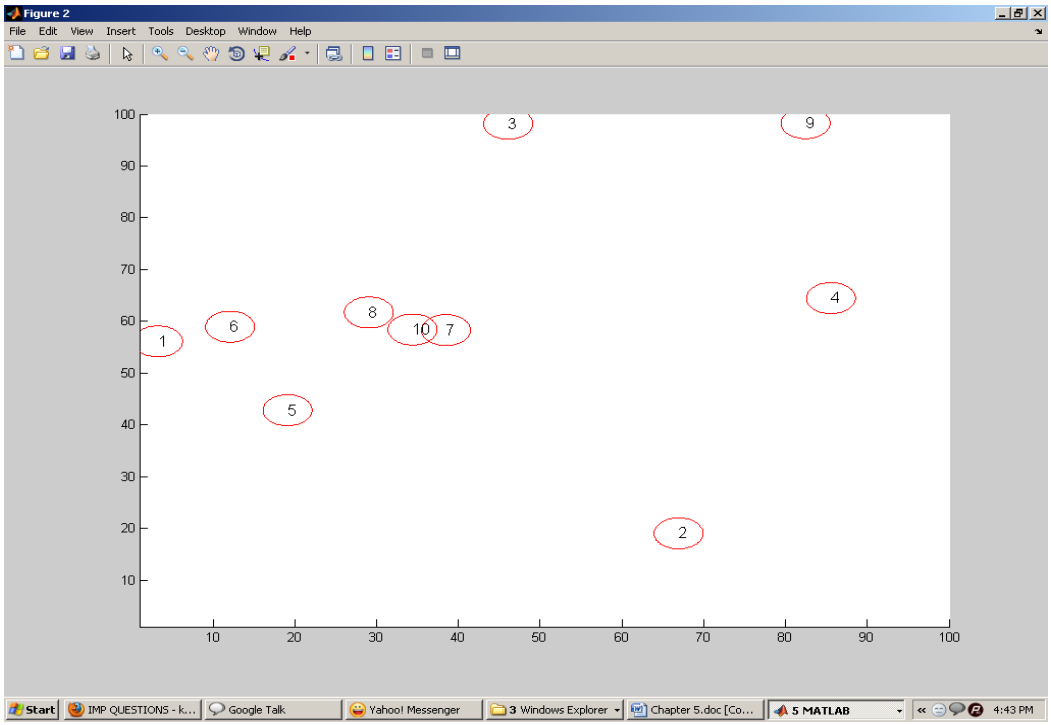

Fig6 : Network Architecture

The path obtained from the network is

1 => 5 => 7 => 10

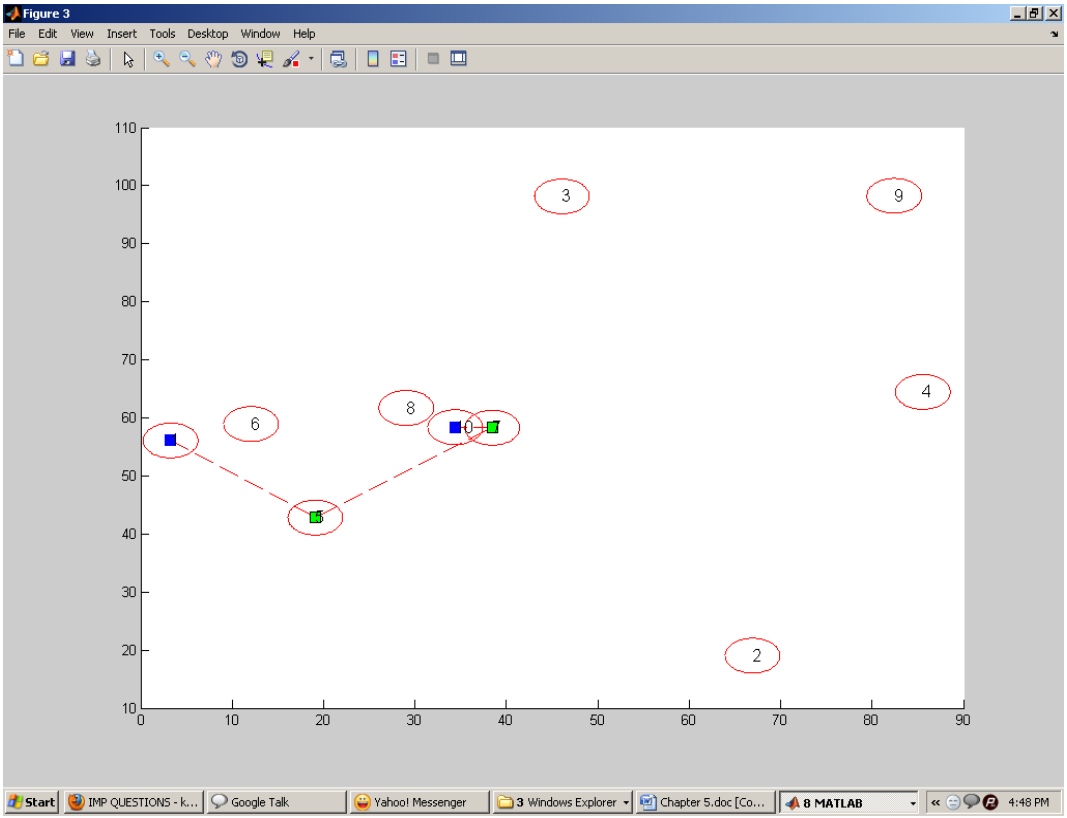

Fig7 : Generated Path (Existing Approach)

Such kind of path is always the first choice of intruder. The proposed PSO Improved algorithm has defined an intruder safe compromising path that will not cover any node of shortest path and will return a safer path to the user.

The results driven from the Compromising path Algorithm

1 => 6 => 10

The connectivity is shown in fig 8

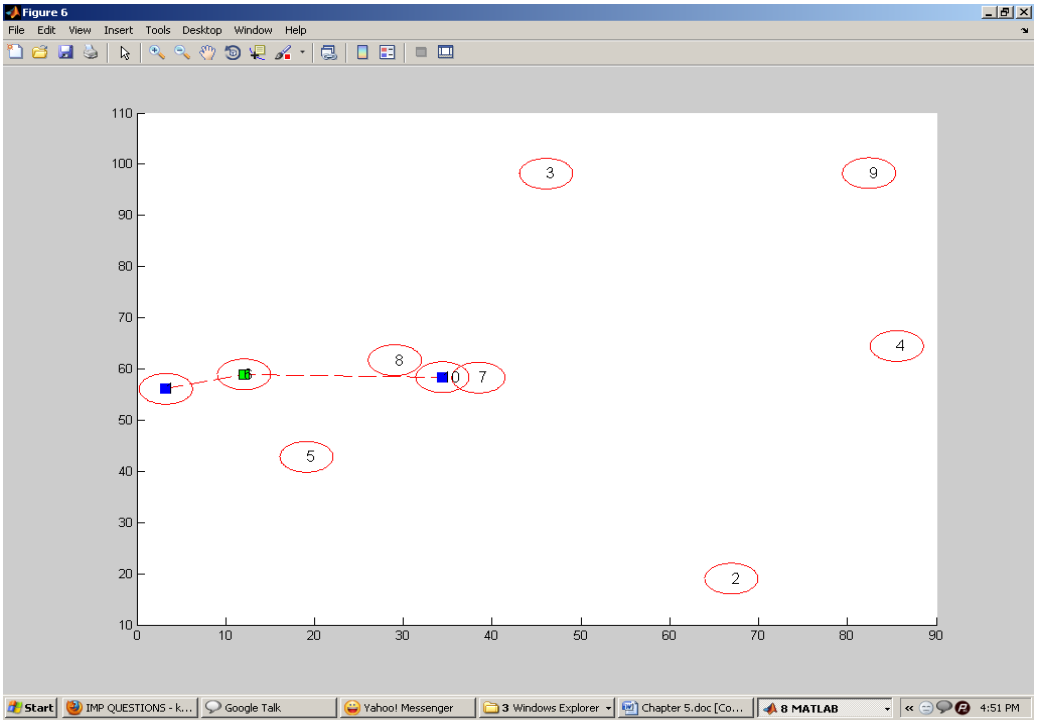

Fig8 : Generated Path (Proposed Work)

The comparison of distance covered between Existing and Proposed work is:

Parameters	Values (Existing) (DSDV)	Values (Proposed) (PSO)
Distance	49.54	40.15
Energy Consumed	6.5119e+003	5.2569e+3
Network Delay	1.4845e+005 ms	4.8787e+003 ms

Table 6.1 comparison of distance covered between Existing and Proposed work

The comparative analysis is shown in the form of graphs given as under

(i) Distance Analysis

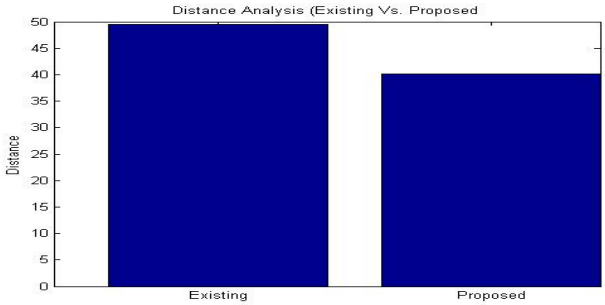

Fig9 : Distance Analysis (Existing Vs. Proposed)

The proposed work has reduce the total distance covered while generating the intruder safe and congestion free path over the network.

(ii) Energy based Analysis

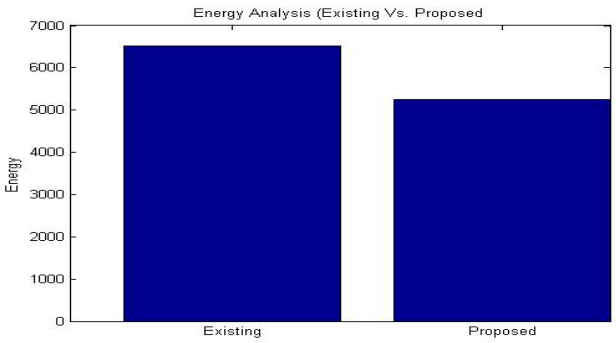

Fig10 : Energy Analysis (Existing Vs. Proposed)

As the data is transferred from a congestion free path, the overall energy consumed while performing the transmission is reduced as compared to the existing approach.

(iii) Network Delay Analysis

As the data is transferred from a congestion free path, the delay for performing the transmission is reduced as compared to the existing approach.

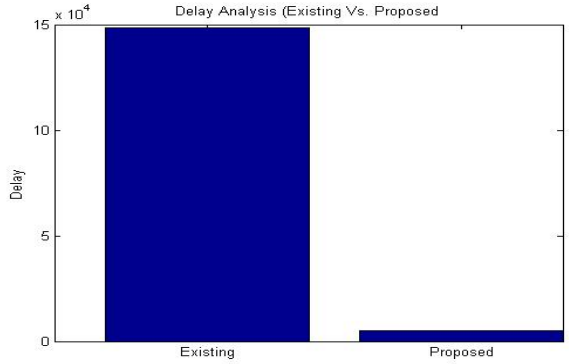

Fig11 : Delay Analysis (Existing Vs. Proposed)

7. Conclusion

In this thesis, we have considered the routing approaches in mobile ad hoc networks from the security and congestion viewpoint. We have analyzed the threats against ad hoc routing and presented the requirements that need to be addressed for secure routing. Existing secure routing algorithm for mobile ad hoc networks are not much secure. And importance of Mobile networks cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, mobile networks pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities.

In this present work, we have defined an PSO improved safe routing approach to transfer data from congestion free and attack safe path. Generally, the shortest path is the most favourite area for the attackers to perform the intrusion, but the presented approach will not cover any node that is having the higher probability of the attack or the congestion. As the communication will be performed over a congestion free path, the energy and the delay over the network will be reduced. The presented approach is effective in terms of energy and the time as well as provide a reliable route over the network. The obtained results shows that the presented approach has improve the network reliability and the energy.

The proposed algorithm intends to provide security. The Secure Compromising path Algorithm provides a foundation for governing a secure communication system for mobile ad hoc networks.

Future Work

The proposed algorithm presented in this thesis considers the defend of Man in Middle Attack as well as provide the safe communication in case of congested networks. In this work, a preventive approach is defined to perform the communication over the safe path. The path safety can be performed from the attacked nodes as well as from the congested nodes. The improvement over the work can be performed in different ways.

- In this present work, PSO is used as the optimization and safe route generation algorithm. In future, some other optimization functions can be used for the path generation such as, genetics, ABC etc.
- The presented work is the generic model respective to the attack. In future the work can be performed respective to the particular attack type over the network.

References

[1] C. K Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems 1st Edition", *Prentice Hall PTR*, 2002.

[2] Jhaveri, H. Rutvij, Patel, M. Narendra, "Mobile Ad-hoc Networking with AODV: A Review", *International Journal of Next-Generation Computing*, pp. *1*65–191, 2015.

[3] C. W. Ahn, R. S. Ramakrishna, "A genetic algorithm for shortest path routing problem the sizing of populations", *IEEE Transactions on Evolutionary Computation*, vol. no. 6, pp. 566-579, 2002.

[4] J. Branke, "Memory enhanced evolutionary algorithms for changing optimization problems", *Proceedings of the IEEE Congress on Evolutionary Computation*, pp. 1875-1882, 1999.

[5] C. S. R. Murthy, B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", *Englewood Cliffs:Prentice-Hall*, 2004.

[6] J. Branke, T. Kauler, C. Schmidt, H. Schmeck, "A multi-population approach to dynamic optimization problems", *Proceedings of the 4th International Conference of Adaptive Computing in Design and Manufacturing*, pp. 299-308, 2000.

[7] C. K. Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems", *Englewood Cliffs:Prentice-Hall*, 2002.

[8] S. K. Sarkar, T. Basavaraju, and C. Puttamadappa, "Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications," *Auerbach Publications*, MA, USA, 2007.

[9] K. V. Arya, S. S. Rajput, "Securing AODV Routing Protocol in MANET using NMAC with HBKS technique," *in Proceedings of the IEEE International Conference on SPIN*, pp. 281–285, 2014.

[10] S. S. Rajput et al., "Performance comparison of AODV and AODVDOR routing protocol in MANET," *International Journal of Computer Applications (IJCA)*, vol 63, no 22, pp. 19–24, 2013.

First Author Sumit has received B. Tech. degree in Computer Science and Engineering from Shri Balwant Institute of Technology, Sonepat, Haryana, India in 2015 and she is now a master student in Bharat Institute of Technology Sonepat, Haryana, India. Her research interest includes the routing approaches in mobile ad hoc networks from the security and congestion viewpoint.

Second Author Ms. Karuna Ghai obtained the B. Tech. degree in Computer Science and Engineering from Bhagwan Mahaveer Institute of Engineering and Technology, Sonepat, Haryana, India in 2012 and she is now a master student in Hindu College of Engineering, Sonepat, Haryana, India. Her research interest includes Bioinformatics and Data mining in Microarray data. She is presently working as an Assistant Professor in Department of Computer Science and Engineering at Bharat Institute of Technology Sonepat with 2 years' experience of academic and administrative affairs.