International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 5041-5047

An Optimized Secure Hybrid Routing Protocol with Intrusion Detection System

Divya Sharma

M. Tech.

Computer Science and Engineering, College of Technology & Engineering (CTAE), Udaipur, Rajasthan, India.

Maharana Pratap University of Agriculture & Technology (MPUAT), Udaipur (313001), Rajasthan, India.

Abstract

This paper presents an optimised secure hybrid routing algorithm for Mobile Ad-hoc Networks (MANETs). The proposed algorithm uses Genetic Algorithm optimization for efficient routing and distributed attack detection architecture to detect the presence of Black-Hole attack to enhance security level of proposed routing algorithm. Simulation of proposed algorithm is carried out on MATLAB (2014a) and results on the basis of device's lifetime, end-to-end delay and network throughput has been provided and compared with conventional zone based routing scheme. Simulation results validate the effectiveness of proposed algorithm in terms of efficiency and security.

Keywords: Hybrid Routing, MANET, Genetic Algorithm, Black-Hole attack detection.

INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes that make up a temporary network without centralized management. MANET networks (Mobile Ad hoc Networks) are wireless networks multi-hop self-configured and self-organized, in which the structure of the network changes dynamically due to the mobility of the nodes. The routing protocols whose objective is to find the best path between the source and the destination in a communication have been widely used in multi-hop networks. The elementary functions performed by a protocol of this type consist of the discovery of routing routes, the selection of the optimal route and the updating of the state of the route. To discover the set of possible routing routes, the routing protocol uses information gathering mechanisms that allow it to determine the intermediate points where the parcel can travel from a source node to the destination. The metrics constitute performance parameters that the routing protocol will use in the selection of the routes. These can be based on the minimization of the delay and losses, or on the maximization of throughput, among others. Finally, the maintenance process of the selected route monitors the status of the communication path and reacts in a timely manner to any eventual difficulty in it. The way in which each protocol solves the problem of routing differs by virtue of the algorithm that each protocol executes. Much of the routing protocols have been designed based on two important classes of algorithms: link state and vector-distance [1].

CLASSIFICATION OF ROUTING PROTOCOLS

The routing protocols applicable to ad hoc mobile wireless networks can be classified according to various parameters or characteristics. The most used classification is based on the way in which routes are discovered and selected. Based on this the routing protocols can be classified as [2]:

Proactive: Where periodically packages are issued to discover new nodes in the network and the route to them, assuming that at some point these routes will be necessary and used. A table is used to keep all routes updated. The fundamental advantage of proactive protocols is the fact that nodes can easily obtain routing information and establish a session easily. Among the disadvantages are the existence of a lot of information in the nodes for the maintenance of the routes and that this information is slow to update when there is a failure in some link. Proactive routing protocols are often used in small networks and in networks with a high traffic density, due to the advantage of the continuous exchange of topological information they perform. There are several proactive protocols that can be used in ad hoc mobile networks, among which are Destination Sequence Distance Vector (DSDV) [3], Cluster Head Gateway Switch Routing (CGSR) [4], Optimized Link State Routing (OLSR) [5], Scalable Routing through the HEAT protocol [6], Better Approach to Mobile Ad hoc Networking (BATMAN) [7] and Distance Routing Effect Algorithm for Mobility (DREAM) [8], among others.

Reactive: These routing protocols look for the routes when they are needed, by flooding the network of route request packages. When a node wishes to find a path to a destination node, it must initiate a route discovery process. Once the right path is found, it remains until the destination becomes inaccessible or the route is no longer required. This limits the total number of destinations for which the routing information is maintained and therefore the size of the routing tables is reduced. Reactive routing protocols are best suited to networks with low node density and static traffic patterns, and are preferred in networks with high mobility [9]. Among the main reactive protocols are Ad hoc On Demand Distance Vector Routing (AODV) [10], Dynamic Source Routing (DSR) [11], Temporally Ordered Routing Algorithm (TORA) [12], Link Quality Source Routing (LQSR) [13], among others. The disadvantages of the reactive protocols are the significant latency in the discovery process, the possibility of saturation of the network due to the flooding technique and the lower quality of the routes.

Hybrid: These routing protocols combine proactive and reactive elements. In the hybrid routing protocols, intradomain and interdomain routing is carried out simultaneously. Proactive routing is applied for communication at the domain level and reactive routing is used for communication between different domains. Hybrid routing protocols are preferred over large networks where there are a large number of nodes. Most protocols of this type are area-based, where routing within the zone is done proactively and outside of it in a reactive manner. There are several protocols widely used among which are: Zone Based Routing Protocol (ZRP) [14], Sharp Hybrid Adaptive Routing Protocol (SHARP) [15], Zone-based Hierarchical Link State (ZHLS) [16], Scalable Location Update Routing Protocol (SLURP) [17] and Distributed Dynamic Routing (DDR) [18]. Hybrid routing algorithm eliminates the deficiencies of proactive and reactive routing algorithm.

RELATED WORK

Recent researches on hybrid routing algorithm have proposed the application of evolutionary algorithms to further improve the performance of MANET routing schemes. In this regard, CW Ahn and RS Ramakrishna have proposed Hopfield neural network based algorithm for finding optimal routes in MANET [19]. The application of Genetic algorithm to solve routing problem in MANET is proposed by R. S. Ramakrishna [20], where GA is used to find optimal route based with higher degree of convergence with varying population size. Particle Swarm optimization based optimal clustering algorithm is presented by Tillett et al [21] to find the optimal and evenly distributed clusters in Ad-hoc sensor networks. In a seminal work, the distance minimization based optimization based on polynomial-time approximation is presented by Ostrosky et al [22]. This research work is focused towards development of an optimized hybrid routing algorithm for secure routing in mobile ad-hoc networks (MANETs) based on Genetic algorithm and Watch mechanism. Rest of this paper is arranged as follows, section-II describes adopted system model, proposed optimized hybrid routing algorithm for secure routing is presented in section-III. Section-IV presents the results and discussion and section-V concludes this paper.

System Model:

Consider a network scenario where N devices are uniformly deployed over given area, let each device be represented by a set of properties given by $N_i = \{X_i, Y_i, E_i, D_i\}$, with X and Y being device's X and Y coordinate, E_i being device's available energy and D_i presents distance of device from centralised control station for the considered node. The energy consumption of device's in network depends on the size of data packet to be transmitted and distance of data transmission. Furthermore the network arrangement is considered to adopt hybrid routing scheme where the available devices are divided into different groups known as clusters and the routing between clusters takes place through inter-cluster and intra-cluster communication. The depiction of cluster based routing is given in fig-1, where source node is transmitting data to its nearest cluster-head node which is further forwarded with the help of other cluster-heads to intended destination. In this research work it is assumed that each cluster is in transmission range of other cluster-head nodes.

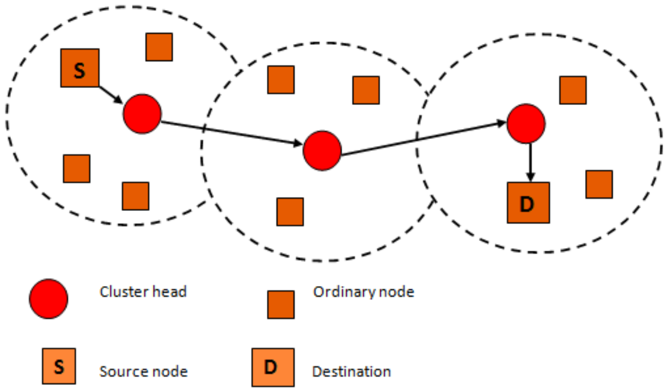

Figure 1: Data Transmission from Source to Destination via Cluster-head and intermediate nodes

Proposed Algorithm:

This paper presents MANET architecture with an optimised hybrid routing algorithm and distributed black-hole attack detection mechanism for secure hybrid routing data transmission. Proposed routing protocol is capable of monitoring the intrusions constantly irrespective of the routes connections, traffic types and mobility of nodes in the network.

1. Optimised Hybrid Routing Scheme

The first step in proposed system is optimised hybrid routing scheme for which the whole network is divided into small group of nodes known as cluster to facilitate efficient routing, low processing and intrusion detection. The main advantage of cluster based architecture is that it reduces number of hopes required for data transmission which in turn is reduces the end-to-end delay. The proposed scheme uses Genetic algorithm [24] for optimising the performance of hybrid routing scheme in MANET [25]. In proposed routing scheme each cluster region elects its head node; known as cluster-head, which is responsible for monitoring the data traffic exchanged between its associate nodes. Furthermore cluster-head node is also responsible for communicating with other clusters for data transmission and cooperative detection of malicious nodes and maintains information of every member node and neighbour clusters, which is useful for network-wide communication. The cluster management responsibility is rotated among the capable members of the cluster for load balancing and fault tolerance which is achieved by conducting regular elections. The optimised cluster based routing scheme requires balanced cluster formation to maximise lifetime of devices in MANET, which in turn is dependent on number of number of clusters formed, distance between devices and size of cluster formed. In this research work Genetic algorithm is used find the optimal cluster-head election probability (p) as a function of total remaining energy of devices in MANET, which is used for election of optimal cluster-head devices around which the cluster will form. Therefore the impact of Genetic Algorithm on proposed system will be to find optimal number of cluster so as the remaining energy of devices will be maximum. This relationship is also described in form of fitness function pseudo code.

The major steps involved are given as follows:

Problem Representation:

Finding optimal number of clusters is critically important to limit the energy consumption of network. For this purpose, each device in network is presented by a binary digit i.e. 0/1, where ‘1’ corresponds to cluster-head and ‘0’ corresponds to normal nodes. In first step of Genetic algorithm initial population is randomly chosen to represent a number of devices.

Genetic Algorithm Operators:

Crossover: This research work uses single-point crossover scheme, where crossover is done between two consecutive nodes with the predefined probability specified by crossover rate. These two devices exchange portions which are separated by crossover point. The process of crossover is also given in example below:

Individual-1: 1 1 1 0 1 1 0 0

Individual-2: 1 1 0 1 | 1 0 1 1

Cross Over Point

Based on the result of crossover operation, two offspring are created as shown below:

Child-1: 1 1 1 0 1 0 1 1

Child-2: 1 1 0 1 1 1 0 0

At the end of crossover operation, if a normal node is elected to be cluster-head, all of the other normal nodes present in the field must check if they are nearer to this node. If they are nearer, they must join this node and as their head node and must be detached from their respective cluster-head node. If a cluster-head node becomes normal node, all of its members must join other cluster-head nodes. There are only two states of nodes is possible in the network either cluster-head or cluster-member.

Mutation: In mutation operator, each ‘0’ bit of the individual is mutated into bit ‘1’ and each ‘1’ bit is mutated into bit ‘0’. Mutation operator is applied with the predefined probability value known as mutation rate. The mutation operation is given in example below:

Individual: 1 1 1 1 1 1 1 0

↓ ↓

Individual: 1 1 1 0 1 1 1 1

Selection: After mutation process, selection process chooses the individual candidates based on their value of fitness function. This research work uses proportional selection where each individual candidate is assigned a slot, the size of this slot is proportional to the fitness value of the individual.

Fitness Evaluation:

Based on the requirements of MANET the objective function to optimise the performance of routing scheme can be given as:

$$Objective = \begin{cases} minimise\ (Number\ of\ Cluster) \\ maximise(Life\ of\ devices) \\ minimise\ (Distance\ between\ CH\ and\ Control\ Centre) \end{cases} \tag{1}$$

The number of clusters formed is function of cluster-head election probability (ρ) and number of devices present in network (N) given by:

$$N_{cluster} = \rho * N \tag{2}$$

Network lifetime is number of devices with energy level greater than the zero at the end of simulation and given by:

$$Life\ of\ devices = \frac{E_0}{e_i}, 1 < i < N \tag{3}$$

Where E_0 is initial energy of devices and e_i represents the energy consumption of devices in MANET.

The distance between Cluster-head node and control centre is given as:

$$D_i = \sqrt{(X_i - X_{cr})^2 + (Y_i - Y_{cr})^2} \tag{4}$$

Where X_i, Y_i is location of i^{th} cluster-head node and X_{cr}, Y_{cr} is location of control centre.

The objective function for Genetic algorithm is developed and evaluated for optimal performance of routing scheme. The fitness function is developed so as to find the optimized cluster-head election probability to maximise the life of devices given by eq. (3).

Fitness function $f(x)$ can be given as:

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 5041-5047

function TE = Fitness-Function(p)

Find P in range of [LB, UB] % LB=0, UB=0.1;

% To Maximize Total Residual Energy of nodes at end of simulation

{

TE=0; % TE- Total Energy

{ for i=1: No of devices

TE= TE+ Residual Energy(i)

end }

end

Attack Detection Architecture for enhanced security

The second phase of this research work is towards the security enhancement of optimised hybrid routing scheme this purpose the distributed Black-hole attack detection mechanism is presented. Once the network setup phase is completed and cluster-head election is done, the chosen cluster-head nodes will start to monitor the network for the presence of malicious nodes which can perform Black-hole attack. For this purpose, Watchdog mechanism proposed by AA Bhosle et al [26] is adopted. In their seminal work authors have proposed the application of Watchdog mechanism on AODV routing algorithm, while this research work adopts it for monitoring over optimised Hybrid routing scheme. As stated in [26], in Watchdog mechanism each node is responsible for creating and maintaining two extra tables namely pending packet table and node rating table. The architecture of these tables is shown below:

Table 1: Pending packet table

Packet ID	**Next Hop**	**Expiry Time**	**Packet Destination**

Where ***Packet ID*** represents identification of packet sent, address of next hop node is represented by ***Next Hop***, ***Expiry Time*** is lifetime of the packet and ***Packet destination*** is address of destination node for the current packet. Similarly the architecture of node rating table is provided in table-2.

Table 2: Node rating table

Current Node Address	**Packet Drops**	**Packet Forwards**	**Misbehave**

Where ***Node address*** is next hop node address**,** ***Packet Drops*** is the counter for calculating the number of dropped packets. ***Packet forwards*** is the counter for number of packets forwarded and ***Misbehave*** is the indicator for the misbehaving nodes. It has two values 0 or 1. Where 0 indicates well behaving node while 1 indicates misbehaving node.

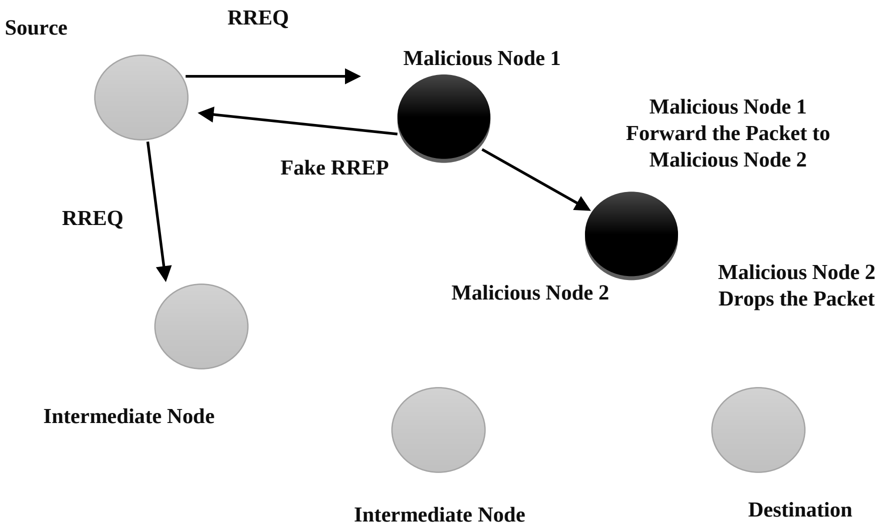

Figure 2: Illustration of cooperative Black-Hole attack

The attack detection mechanism is presented in form of pseudo code below.

1. Data packet forwarded or sent.

2. Copy and keep the data packet in pending packet table until it is expired or forwarded

3. If (data packet forwarded)

{

Increment the corresponding forwarded packet in the node-rating table and remove the data packet from pending packet table.

Update the current Node number which routes the data, and also update the previous routing node number from which the current node receives the packet.

}

4. If (data packet expires in the pending packet table)

{

Increment the corresponding dropped packet in the node-rating table and removes the data packet from pending packet table.

If (dropped packet > threshold (th1)) then

{

If ((dropped packet / forwarded packet) > threshold (thl))

{

Node is misbehaving, update the misbehaving node counter.

Promiscuous node locally tells all the node of its wireless range from node rating table that particular node (misbehaving node 2) and the previous node (misbehaving node 1) which route the data packets to that particular node are misbehaving node.

Discard RREP message coming from the misbehaving node 1

}

}

}

Figure 3: Attack detection Mechanism [26]

RESULTS AND DISCUSSION:

This research work is focused towards the development of a novel hybrid routing algorithm and Black-hole attack detection mechanism. For this purpose, MATLAB based simulation model has been developed and simulated. To compare the performance of proposed scheme lifetime of devices in MANET, network throughput and end-to-end delay has been considered as reference parameters.

The simulation scenario consists of a network with field area equals 100x100 square meters where 100 mobile devices are randomly deployed with initial energy of each device equals 0.5 Joules. The cluster-head election probability is set to be in range of 0-0.2 (corresponds to minimum Zero and Maximum 20 Clusters in the field), which is elected by Genetic algorithm. Developed network scenario is simulated for 6000 rounds where each round represents time taken by algorithm to complete a single iteration. The simulation parameters for the proposed system are also given in table-3 below.

Table 3. Network Parameters

Field area	100×100 meter squares
Number of nodes in the field	100
Cluster-head Election Probability	0-0.2
Initial Energy of nodes	0.5 J
Maximum number of rounds	6000

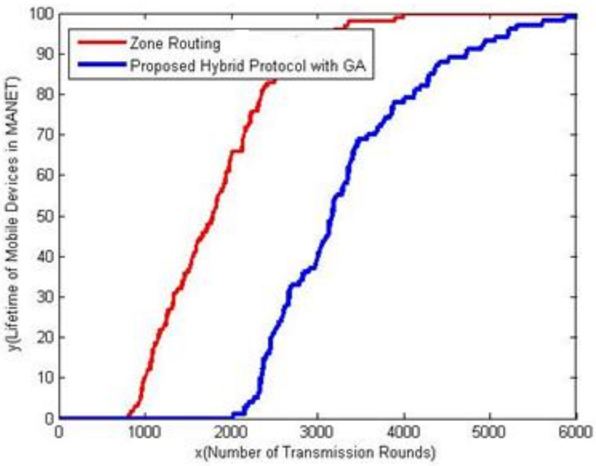

Figure 4: Comparison of Lifetime of Mobile devices for Zone Routing and Proposed Hybrid Routing algorithm with GA

The performance comparison of lifetime of mobile devices for Zone routing and proposed Hybrid routing with GA is presented in Fig-4. It can be observed from the figure, that in case of Zone routing the energy of first device depletes around 1000 round and for last device around 4000 round, causing the lifetime to be 4000 rounds. Whereas, for proposed algorithm, the energy of first device gets depleted around 2000 round and last device's energy gets depleted around 6000 round, causing the lifetime to be 6000 rounds. Based on aforementioned observation, it can be concluded that the proposed algorithm provides better lifetime of devices as compared to Zone Routing scheme.

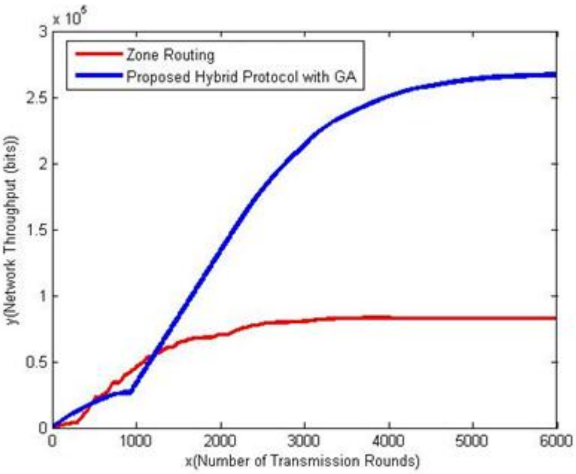

Figure 5: Comparison of Network throughput for Zone Routing and Proposed Hybrid Routing algorithm with GA

The Network throughput comparison for Zone routing and proposed Hybrid routing with GA is presented in Fig-5. It can be observed from the figure, that in case of Zone routing the total number of message transmitted are approx. 80000 (0.8×10^5), while in case of proposed routing, the total number of messages transmitted are approx. 260000(2.6×10^5). Based on aforementioned observation, it can be concluded that the proposed algorithm provides better throughput performance as well when compared to Zone Routing scheme.

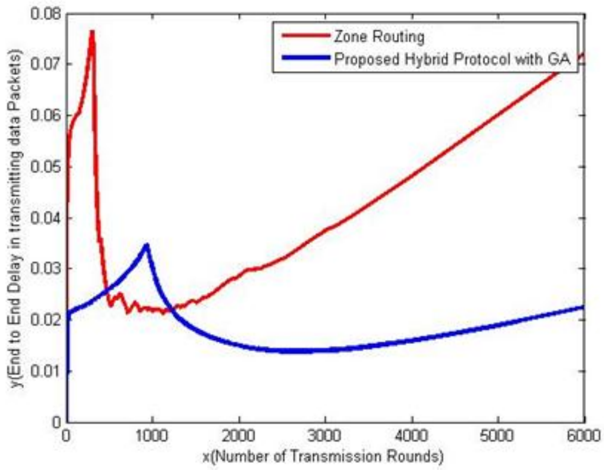

Figure 6: Comparison of End-to-end delay for Zone Routing and Proposed Hybrid Routing algorithm with GA

Comparison of End-to-end delay (i.e. the time taken by a packet to route through network from a source to destination) for Zone routing and proposed hybrid routing with GA is presented in Fig-6 above. It can be observed from the figure, that in case of Zone routing the estimated maximum delay is approx. 0.08 seconds while in case of proposed hybrid routing with GA, the maximum observed delay is around 0.035 seconds which is quite less as compared to Zone routing. Therefore it can be concluded that the proposed hybrid routing with GA outperforms Zone routing in case of delay comparison too.

CONCLUSION

Mobile Ad-hoc network is a popular networking technology these days. With distributed networking characteristics of MANET there are some severe security threats present. This paper presents the impact of Black-hole attack on MANET with hybrid routing scheme and presents watch mechanism based tabular approach for the detection of the same. Furthermore, to enhance the system performance hybrid routing scheme with cluster based architecture and intelligent cluster-head selection is also presented. Simulation results show that the performance of MANET can be remarkably enhanced with the application of proposed scheme.

REFERENCES

[1] Akkaya, Kemal, and Mohamed Younis. "A survey on routing protocols for wireless sensor networks." *Ad hoc networks* 3, no. 3 (2005): 325-349.

[2] Wu, Jun, Ning Xie, and Hui Wang. "Routing Protocols in Wireless Mesh Networks." In *International Conference on Future Computer and Communication, 3rd (ICFCC 2011)*. ASME Press, 2011.

[3] Perkins, Charles E., and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." In *ACM SIGCOMM computer communication review*, vol. 24, no. 4, pp. 234-244. ACM, 1994.

[4] Chiang, Ching-Chuan, Hsiao-Kuang Wu, Winston Liu, and Mario Gerla. "Routing in clustered multihop, mobile wireless networks with fading channel." In *proceedings of IEEE SICON*, vol. 97, no. 1997, pp. 197-211. 1997.

[5] Clausen, Thomas, and Philippe Jacquet. *Optimized link state routing protocol (OLSR)*. No. RFC 3626. 2003.

[6] Baumann, Rainer, Simon Heimlicher, Vincent Lenders, and Martin May. "HEAT: Scalable routing in wireless mesh networks using temperature fields." In *World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a*, pp. 1-9. IEEE, 2007.

[7] Neumann, Axel, et al. "Better approach to mobile ad-hoc networking (BATMAN)." *IETF draft* (2008): 1-24.

[8] Basagni, Stefano, et al. "A distance routing effect algorithm for mobility (DREAM)." *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, 1998.

[9] Mohan, S. Venkat, and N. Kasiviswanath. "Routing protocols for wireless mesh networks." *International Journal of Scientific & Engineering Research* 2.8 (2011).

[10] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003.

[11] Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." *Mobile computing*. Springer, Boston, MA, 1996. 153-181.

[12] Park, Vincent D., and M. Scott Corson. "A performance comparison of the temporally-ordered routing algorithm and ideal link-state routing." *Computers and Communications, 1998. ISCC'98. Proceedings. Third IEEE Symposium on*. IEEE, 1998.

[13] Draves Jr, Richard Powell, Brian D. Zill, and Jitendra D. Padhye. "System and method for link quality source routing." U.S. Patent No. 7,376,122. 20 May 2008.

[14] Joa-Ng, Mario, and I-Tai Lu. "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks." *IEEE Journal on selected areas in communications* 17.8 (1999): 1415-1425.

[15] Ramasubramanian, Venugopalan, Zygmunt J. Haas, and Emin Gün Sirer. "SHARP: A hybrid adaptive routing protocol for mobile ad hoc networks." *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2003.

[16] Joa-Ng, Mario, and I-Tai Lu. "A GPS-based peer-to-peer hierarchical link state routing for mobile ad hoc networks." *Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st*. Vol. 3. IEEE, 2000.

[17] Li, Jinyang, et al. "A scalable location service for geographic ad hoc routing." *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000.

[18] Seppänen, Kari. "Distributed dynamic routing." U.S. Patent No. 7,529,239. 5 May 2009.

[19] C. W. Ahn, R. S. Ramakrishna, C. G. Kang, and I. C. Choi, “Shortest path routing algorithm using Hopfield neural network,” Electron. Lett., vol. 37, no. 19, pp. 1176–1178, Sep. 2001.

[20] R. S. Ramakrishna, “A genetic algorithm for shortest path routing problem and the sizing of populations,” IEEE Trans. Evol. Comput., vol. 6, no. 6, pp. 566–579, Dec. 2002.

[21] J. Tillett, R. Rao, F. Sahin, and T.M. Rao. “Clusterhead Identification in Ad hoc Sensor Networks Using Particle Swarm Optimization. In Proceedings of the IEEE International Conference on Personal Wireless Communication, 2002.

[22] R. Ostrosky and Y. Rabani. “Polynomial-Time Approxiamation Schemes for Geometric Min-Sum Median Clustering”. Journal of the ACM, Vol. 49, No. 2, 2002, pp 139-156.

[23] Waharte, Sonia, Raouf Boutaba, Youssef Iraqi, and Brent Ishibashi. "Routing protocols in wireless mesh networks: challenges and design considerations." *Multimedia tools and Applications* 29, no. 3 (2006): 285-303.

[24] Schmitt, Lothar M. "Theory of genetic algorithms." *Theoretical Computer Science* 259, no. 1-2 (2001): 1-61.

[25] Yen, Yun-Sheng, Han-Chieh Chao, Ruay-Shiung Chang, and Athanasios Vasilakos. "Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs." *Mathematical and Computer Modelling* 53, no. 11-12 (2011): 2238-2250.

[26] Bhosle, Amol A., Tushar P. Thosar, and Snehal Mehatre. "Black-hole and wormhole attack in routing protocol AODV in MANET." International Journal of Computer Science, Engineering and Applications 2.1 (2012): 45.