

# AN APPROACH FOR MESSAGE ENCRYPTION IN MULTIPATH ROUTING

**Harsimranjeet Kaur Bhattal** (Coordinator CSE Deptt., GGSCMT, Kharar)

**Navreet Kaur** (Lecturer, MCA Deptt., GGSCMT, Kharar)

**Mandeep Kaur**(Coordinator, IT Deptt., GGSCMT, Kharar)

*Abstract* - This paper outlines the experience of the design of an efficient network security algorithm for message encryption in multi-path routing. It is very difficult to develop a network method which is completely secure and the data can be efficiently transferred and in very less time. The network should not have any leakage, any congestion and speedy transfer of data on the network. Several multipath routing algorithms are developed with their own specialty. These multipath routing schemes have their own limitations. Here we try to explore the approaches and issues to enhance data confidentiality when transmitting across the network. In this work, an algorithm for route optimization and message encryption is developed using GA and AHP (not used by packet technology till date). It uses network security parameters like authentication, integrity, power consumption, & node status for route determination as a design criterion in order to ensure the integrity of network services in the event of component failures, traffic congestion and various other adverse conditions.

Also in this, a novel GA and AHP based route optimization algorithm for MANETs has been presented. Once the optimized route is obtained the message passing through the route is encrypted using cipher encryption.

**Keywords:** Multipath, AHP, MANET's, encryption, optimization, cost function, decryption, cross-over, mutation, GA.

## I. INTRODUCTION

Data security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification [6]. Common information security classification labels used by the business sector are: public, sensitive, private, confidential. Common information security classification

labels used by government are: unclassified, sensitive but unclassified, confidential, secret, top secret.

In any modern network, there is a need for security. However, the current Internet, without integrating with security mechanisms originally, has a number of security problems and lacks effective protection of confidentiality and integrity of the data transferred over the network below the application layer[1][10][9]. With the emerging of applications such as e-commerce/m-commerce, the need for network security services that can provide secure communication in public networks has been more and more significant.

The common approach of providing secure communication across unsecured channel is to apply data encryption/decryption on the information transmitted over the networks. Encryption algorithms widely used for this purpose include Data Encryption Standard (DES), which is a 64-bit block cipher and widely used to encrypt the transferred data, and RSA, a popular public-key algorithm widely used for session key exchange and distribution[11][16]. Both of the algorithms are computationally intensive while RSA is more. In addition, encryption/decryption algorithms need to work in combination with a good authentication mechanism and a good key management scheme. The confidentiality provided by pure data encryption is not absolute in the sense that with today's super computer, it is possible to break any encryption algorithm when enough encrypted information are collected[14][15]. Most routing algorithms used today favor the stable path, i.e., the session from a source node to a destination node tends to use the same path for quite a long time. If the path is breached in, a large number of messages will be intercepted, which can greatly facilitate the unauthorized decryption of the messages[3]. Till now there is no absolute security in the network.

In this paper, a novel GA and AHP based route optimization algorithm for MANETs has been presented. It uses network resilience parameters like latency, power consumption, & node status, route determination as a design criterion in order to ensure the integrity of network services in the event

of component failures, traffic congestion and various other adverse conditions. Here in this work, GA and AHP together have been used for the optimal selection of the routes as well as the node selection parameters. Once the optimized route is obtained the message passing through the route is encrypted using cipher encryption.

This paper is organized as follows. In section II, we describe the multipath routing and how it is applied to the message to be transmitted. In section III, we present a proposed algorithm for message encryption in multipath routing to find the desired multiple independent paths. The conclusions and future scope about the algorithm are reported in section IV. References are given in the last section.

## II. MULTIPATH ROUTING

In order to distribute shares to multiple paths, we need to design efficient algorithms for finding multiple paths with minimum overlaps. The routing protocols used in today's Internet are destination-based single shortest path algorithms[12]. In between a single source-destination pair, normally the same shortest path will be used. The existing Internet routing protocols provide very limited multiple paths routing capability. Only when there exist multiple paths and are of the same (or varies within certain range of) cost, the packets will be forwarded via multiple paths to the same destination, and this is mainly done for load balancing, congestion control or reliability.

How to find the multiple paths with the desired property is the key implementation issue in our approach. The solution lies on the so-called multipath routing algorithms and protocols[2]. Notice that in the current Internet implementation, a router will have at least two interfaces/connections and usually it has more. Multipath routing aims to take advantage of the connectivity redundancies of the underlying physical networks by providing multiple paths between source-destination pairs [4]. A closely related topic to multipath routing is the long studied  $k$ -shortest path problem. Generally speaking, the  $k$  shortest paths problem is to list the  $k$  paths connecting a given source-destination pair in the digraph with minimum total cost [2][16].

However, the paths found by the  $k$  shortest path algorithms tend to share many links. The lack of independence limits the effectiveness of providing the security for the message shares in our proposed scheme. Algorithms that overcome the problem of path independence are ones that find disjoint paths between nodes[4]. Ogier, et al, proposed a distributed algorithm for finding two disjoint paths of minimum total cost

from each node to a destination. Sidhu, et al, proposed a distributed algorithm that finds multiple disjoint paths to a destination. In our case, the message is divided into various packets and then the information is passed through the various paths so that it becomes more secure in comparison to single path network. Path quantity is the number of available paths between nodes. The higher the number better are the chances for load distribution[8]. Uniform path sets are preferable over high variance path sets i.e. a path set with every node having 5 paths is preferred than one with nodes having 1 path for some path sets and 9 paths for other path sets. The second characteristic of path sets is path independence, which is illustrated with Fig. 1. Consider a path set with 2 paths (a, b, c, d) and (a, f, c, d) and other path set with 2 paths as (a, b, c, and d) and (a, f, e, d). The second set is independent when compared to the first set.

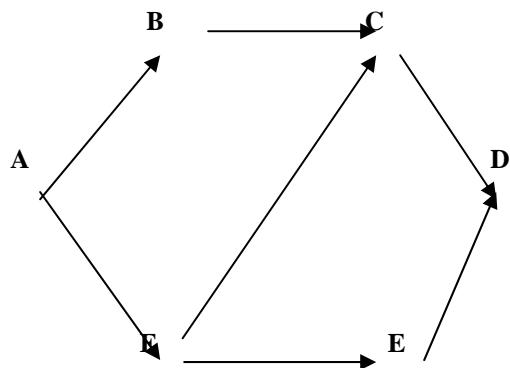


Fig.: Illustration of multipath routing scheme

So the second set would lead to better usage of resources and is less likely to be congested because at least one link in each path should be congested, whereas in the first set congestion at link (c, d) is reflected in both the path sets. Multipath sets with these attributes facilitate for higher performance.

The number of paths was predicted taking some considerations that would successfully deliver a message among the multiple disjoint paths obtained from the route discovery process. Furthermore, approximation is taken to predict the successful delivery. The increase of the probability for this successful delivery comes at the trade-off of added redundancy. Of course, one can send the whole message along each of the available paths, but the overhead induced by this will be too high. The entire data package to be sent from the source to the destination over the available  $k$  disjoint paths will be split up into smaller sub packets of equal size with added redundancy. The number of created sub packets corresponds to the number of available paths. Only a smaller number of these sub packets will then be needed at the destination to reconstruct the original message. There exist several fast and simple (i.e. linear) forward error correcting

codes (or erasure codes) that allow the reconstruction of an original message that has been split up, with added redundancy, and of which not all parts arrive at the destination.

In the following, we will focus on approximating a value  $Ek$  that gives, with high probability, the number of successful paths. This value will then be used to determine the amount of redundancy to be added for the split message transmission. The total number of sub packets as well as the added redundancy is a function dependent on the multipath degree and on the failing probabilities of the available paths. As these values change according to the positions of the source and the destination in the network, each source must be able to decide on the parameters for the error correcting codes before the transmission of the actual data sub packets.

One way of assuring that a data packet reaches the destination in a sensor network is by using multipath routing algorithms[7]. The method developed has the disadvantage of increasing the overall traffic substantially. New idea is introduced by splitting the original data packet in sub packets and sending each one of them through one of the multiple paths. Even if some of them are lost, the original message can be reconstructed. Because of the failures that might appear (mainly due to mobility of the nodes and to the wireless transmissions) a path rater mechanism needs to be used. After the rating process, it will be decided on the amount of redundancy to be added in order to use the available resources efficiently.

### III. PROPOSED ALGORITHM

We have proposed an algorithm for route optimization and message encryption by using GA and AHP (not used by packet technology till date). The main objective is to select an optimized route among the three zones and each zone having three nodes. Once the optimized route is selected with its respective cost function (high throughput route), the message is sent through the route using cipher encryption.

In this case the message is divided into various packets (letters) and then it is (encrypted message) transmitted through the selected route. On the receiver side each letter is decrypted according to the agent code and the original message is retrieved.

In this, we have taken up a MANET between two places on a map and have divided the region into various zones consisting in each region, so as to standardize input data for normalization[7]. After that we have taken up the shortest path as the backbone and assigned it the highest priority. The

attributes like latency, power consumption, and network congestion have been considered. The cost function is given by equation (1) below, in which various local static constants  $B_1$ ,  $B_2$  and  $B_3$  are assumed. These depend upon the priority and various attribute indices, which are basically the attributes or local static constants on a scale of 0-1. The various weights related to these local static constants are calculated by applying the AHP model[8][13]. The cost function is optimized using GA, so as to choose the best possible routing path for easy data flow without jamming, and minimum power consumption.

$$\text{High throughput route selection function } F_n = B_1\lambda_1 + B_2\lambda_2 + B_3\lambda_3 \dots \dots \dots (1)$$

Here,  $\lambda_1, \lambda_2, \lambda_3$  are the weights.

A sample value for  $\lambda$  is calculated using comparison matrix. Their values depend upon present and initial condition pertaining to node condition. Similarly, other attribute indices are obtained under various operating conditions. The values of  $\lambda^s$  form the basis for node selection for optimal route in MANET. These values of  $\lambda$  as obtained by AHP are basically taken at different time slots in a particular region.

Genetic algorithm is used to perform two functions viz., firstly to obtain two (02) best values of  $\lambda$ s (taken as parent chromosomes participating in crossover), and secondly to generate offspring value of  $\lambda$ , which is optimal in comparison to other attribute indices in the initial population. Binary encoding is used in this work. The developed GA is equipped with a clause conditionally prohibiting the selection of the shortest path, every time. Also the developed algorithm sends the message by dividing the whole message into small packets. These packets in the form of individual are then sent through the optimized route. This helps in preventing network congestion and improper utilization of all the available resources.

A particular source and destination is being selected and the whole area is being divided into three zones  $Z_1, Z_2, Z_3$ . These three zones are assumed to have each three nodes  $N_1, N_2, N_3$ . This results into 27 paths in these 3 zones through the specified nodes. Each of these 9 nodes is being characterized by attributes like latency, power consumption, congestion etc. In this case three attributes have been taken which have their respective attribute indices. The weights of the respective nodes in the three regions are calculated using analytical hierarchy process. After obtaining the cost functions genetic algorithm is applied to it, which includes crossover and mutation. Once the desired no of crossovers & mutation have been done the fittest values of cost functions are obtained.

These cost functions are the performance indices of various nodes in the three zones specified giving the best-optimized route for the transmission of the data in these three zones. Once the route is decided, there will be a source node, an intermediate node, and a destination with the respective values of their cost functions. The message is encrypted and transmitted along this optimized path.

#### IV. CONCLUSIONS AND FUTURE SCOPE

It is concluded that the use of adaptive techniques in combination with the mathematical tools such as AHP, brings a pronounced throughput improvement in ad-hoc networks. By using GA and AHP for routing, the MANET throughput has shown an improvement in comparison to the existing routing algorithms.

The proposed model is relatively simple (using GA and AHP), but is parameterisable in a way that allows different scenarios to be modeled both at the level of social organization and topographical translation.

In this paper, we have not considered the additional burden in coordinating access to the wireless channel, and the additional burden caused by mobility and link failures and the consequent need to route traffic in a distributed and adaptive way. These can only further throttle capacity. It would be useful to quantify these additional burdens. Another issue to be studied is delay. This will arise when the traffic is bursts or when nodes are mobile. These two sources of delay are markedly different. When node locations and demands are known and do not have to be figured out purely from ternary feedback, transmissions can be advantageously scheduled so that collisions are avoided, and the throughput can consequently be increased.

However, this is a challenging proposition since transmissions from nodes will have to be carefully orchestrated. Such schemes may pose some technological challenges though for low cost networks. Also, in the present work we have considered three attributes and also each zone consists of three nodes. In a more generic case more nodes as well as parameters can be considered and its effect on the selection of optimized route can be analyzed in terms of speed and complexity of execution of the algorithm.

#### REFERENCES

1. E. Gafni and D. Bertsekas. Distributed Algorithms for Generating Loop-free Routes in Networks with Frequently Changing Topology. *IEEE Transactions on Communications*, pages 11-18, January 1981.

2. De Jong, K. A. and Spears, W. M., "Using Adaptive multipath algorithms to solve networking Problems", *Proceedings of the Third International Conference on Genetic Algorithms*, pp. 124-132, June, 1989,
3. M. Singhal. A Dynamic Information-Structure Mutual Exclusion Algorithm for Distributed Systems. *IEEE Transactions on Parallel and Distributed Systems*, pp 121-125, January 1992.
4. Abuali, F. N., Schoenefeld, D. A. and Wainwright, R. L. "The Design of a Multipoint Line Topology for a Communication Network", appeared in *proceedings of the Seventh Oklahoma Conference on Artificial Intelligence*, pp 125-157, November, 1993.
5. C.E. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *Proceedings of ACM SIGCOMM Conference on Communication Architectures, Protocols and Applications*, pages 234-244, August 1994.
6. IEEE. P802.11, IEEE Draft Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, D2.0, pp 546- 560, July 1995.
7. D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad-Hoc Wireless Networks. In T. Imielinski and H. Korth, editors, *Mo- bile Computing*. Kluwer Academic Publishers, pp 256- 289, 1996.
8. M. Marengoni, B.A. Draper, A. Hanson, and R.A. Sitarman, "System to Place Observers on a Polyhedral Terrain in Polynomial Time", *Image and Vision Computing*, vol.18, pp. 773-80, Dec. 1996.
9. B. Das, R. Sivakumar, and V. Bharghavan. Routing in Ad-Hoc Networks Using a Spine. In *Proceedings of IEEE IC3N*, pp 1132- 1143, 1997.
10. T.V. Lakshman, U. Madhow, and B. Suter. Window-based error recovery and flow control with a slow acknowledgment channel: a study of TCP/IP performance. In *Proceedings of IN- FOCOM*. IEEE, pp 15-30, 1997.
11. C Don and R Phillip, "A Software-Optimized Encryption Algorithm," 17th Sept., 1997.
12. A. Molina, G.E. Athanasiadou, A.R. Nix, "The Automatic Location of Base-Stations for Optimized Cellular Coverage: A

New Combinatorial Approach,” IEEE 49th Vehicular Technology Conference, vol.1, pp. 606-10, May 1999.

13. C.W. Kang, M.W. Golay, “An Integrated Method for Comprehensive Sensor Network Development in Complex Power Plant Systems,” Reliability Engineering & System Safety, vol.67, pp. 17-27, Jan. 2000.

14. B John, K Tadayoshi and P Adriana, “Building secure cryptographic transforms, or how to encrypt and MAC,” Aug.28,2003.

15. B William C.,“ Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher,” May 2004.

16. Paterson Kenneth G. and Yau Arnold K.L.,“Cryptography in Theory and Practice: The Case of Encryption in IPsec,” November 18<sup>th</sup>, 2005.