International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Routing of Data Using Secure Data Transmission Technique in Mobile Ad-hoc Network

Anita Kumari[1], Jitender Yadav[2], S S Yadav[3]
[1]Scholar, Computer Science & Engg. Deptt.,RPSGOI, Mohendergarh
[2]Assistant Professor, Computer Science & Engg. Deptt., RPSGOI, Mohendergarh
[3]Dean PG Academics, Computer Science & Engg. Deptt., RPSGOI, Mohendergarh
[1]anita6singh@gmail.com, [2]jitendery006@gmail.com, [3]deanpg@rpsinstitutions.org

***Abstract:** In this thesis, we proposed a Secure Alternate path, called "Intruder safe path strategies using alternate path in an ad hoc network" which aims at addressing the above limitations by combining the best properties of both proactive and reactive approaches. The proposed algorithm is based on the concept of Shortest path algorithm i.e. Dijkstra algorithm to achieve the security goals. The thesis details the design of the proposed algorithm and providing security and analysis its robustness in the presence of multiple possible security attacks that involves impersonation, modification, fabrication and replay of packets caused either by an external advisory or an internal compromised node within the network. The security and performance evaluation of alternate path algorithm through simulation indicates that the proposed scheme successfully defeats all the identified threats and achieves a good security at the cost of acceptable overhead. Together with existing approaches for securing the network stack, the Secure Alternate path can provide a foundation for the secure operation of an ad hoc network.*

***Keywords:** MANET, Security, Secure alternate path, SEAD.*

I. INTRODUCTION

A mobile ad hoc network (MANET) sometimes called a *wireless ad hoc network* or a Mobile mesh network is a wireless network, comprised of mobile computing devices (Nodes) that use wireless transmission for communication, without the aid of any established infrastructure or centralized administration such as a base station or an access point . Secure routing in the field of mobile ad hoc networks is one of the most emerging areas of research. Designing a foolproof security in an ad hoc routing is a challenging task due to the unique network characteristics such as, lack of central authority, rapid node mobility, frequent topology changes, insecure operational environment, shared radio channel and limited availability of resources. Secure alternate path has been proposed in the literature for secure routing.

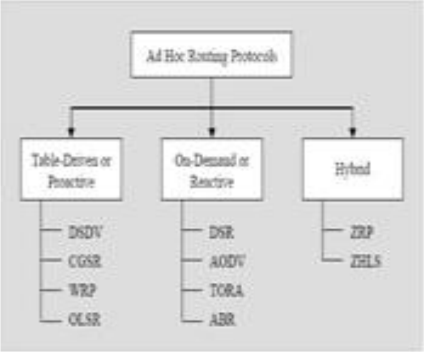
II. OBJECTIVE

Due to insecure nature of the wireless link, ad-hoc networks require a security oriented approach as any node can join or leave the network at any time. This is security breach as the joining node can be a malicious node and can have unwilling effects on the network performance. So it is very important to authenticate the joining nodes. That's why we do the following:

1. To develop an algorithm to send data from source to destination in secured manner.
2. To design a path that is safe from the intruder attack i.e. we are designing a highly efficient algorithm.
3. To find an alternative route through which the packets can be routed to control the congestion.
4. To Check that the selected path is safer than the path used in traditional routing algorithm (shortest path algorithm).
5. To detect malicious types of attacks in the ad hoc environment and then apply suitable algorithm specific for that purpose.
6. To Compute the whole activity and then operate the algorithm in the real time environment.
7. We provide a suitable platform to suit ad hoc networks must be developed in which we can implement our algorithm.

III. ROUTING PROTOCOL IN MOBILE AD-HOC NETWORK

Since the advent of Defense Advanced Research Projects Agency (DARPA) packet radio networks in the early 1970s [1], numerous routing protocols have been developed for ad hoc mobile networks [2, 5]. As shown in Fig. 1.4, these are generally categorized as

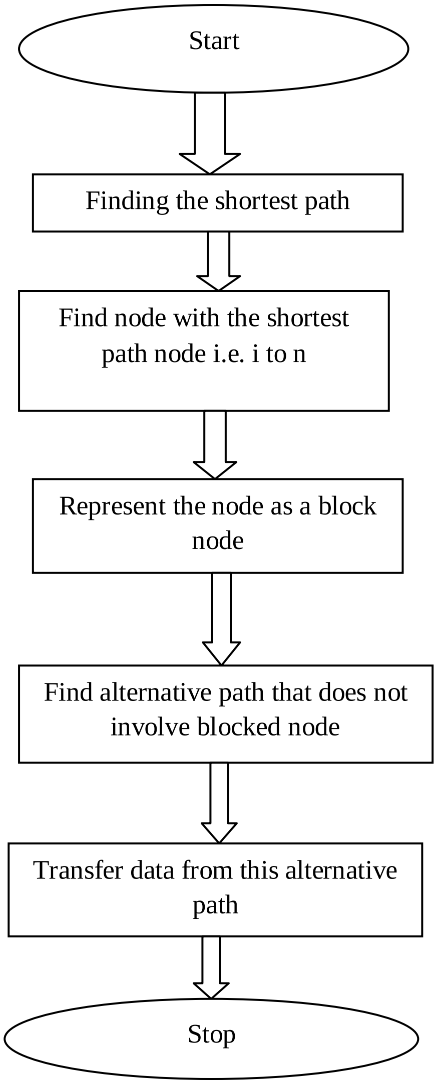


Requirements of Ad-Hoc Network are:

- Route signaling can't be spoofed.
- Fabricated routing messages can't be injected into the network.
- Routing messages can't be altered in transit.
- Routing loops can't be formed by through malicious action.
- Routes can't be redirected from the shortest path by malicious action.
- Unauthorized nodes should be excluded from route computation and discovery.

IV. Design And Implementation

In the routing mechanism used the route taken to receiving node is shortest path and malicious resides in the route . The scheme is as that each node must find alternate path to the destination node which is not the shortest path .


Start
Finding the shortest path
Find node with the shortest path node i.e. i to n
Represent the node as a block node
Find alternative path that does not involve blocked node
Transfer data from this alternative path
Stop

1. Finding the shortest route to the destination.
2. Finding the alternative that does not involve any of the nodes that lies on the way to the shortest path. After that getting the acknowledgement from that path about the ongoing communication.

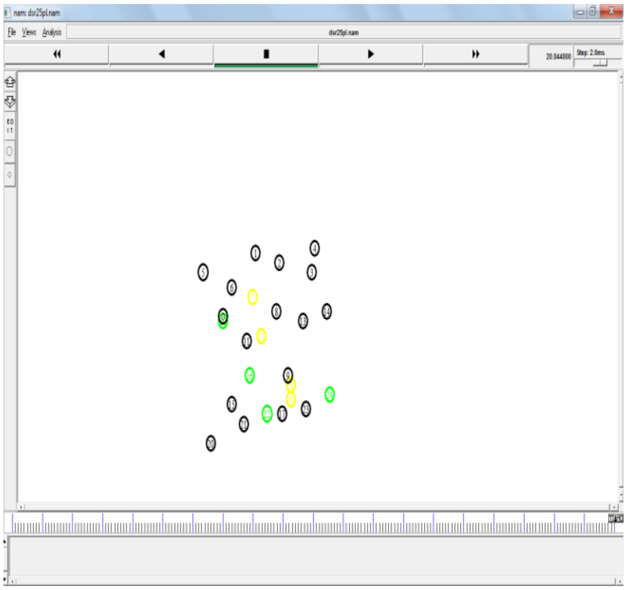
V. Percentage Of Packets Dropped That Passed Through Malicious Nodes

This Metric indicates the percentage of total packets dropped that traverse malicious Nodes when using each routing protocol, in the presence of different percentages of malicious nodes. Assuming that all the packets that pass through a malicious or Compromised node were altered, this metric can be calculated as follows:

$$\begin{array}{l}\textit{\% of Packets}\\ \textit{Dropped that}\\ \textit{passed through}\\ \textit{Malicious Nodes}\end{array} = \left(\frac{\begin{array}{c}\textit{No. of packets dropped by the benign nodes}\\ \textit{that are previously generated by or passed}\\ \textit{through any malicious node in the network}\end{array}}{\textit{Total number of packets communicated}} \right) \text{X } 100$$

VI. Experimental Results

Secure alternate path algorithm gives the utmost advantage to the users that it provides the maximum security and prevent the hosts from the malicious nodes injecting the harmful packets .Now after going this yellow color nodes tells for packet loss for previous path and green color tells for alternate path.



VII. CONCLUSIONS

In this thesis, we have considered the routing approaches in mobile ad hoc networks from the security 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 MANET cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, MANET 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.

We are providing the solution for the problems where we can save the ad hoc network from the active attack of Intruders that are on the basis of algorithmic implementations. Generally the path selected for data transfer in ad hoc network is the shortest path because of this intruder attack is also in same area. We have generated such a path in which no node from the shortest path will be included. It will give a secure and efficient approach of data transmission in ad hoc network in unicast routing.

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

VIII. FUTURE ENHANCEMENT

The proposed algorithm presented in this thesis considers the defend of Man in Middle Attack which is possible in the network , by using different routing algorithm and mainly we have mentioned Routing of Data Secure alternate path algorithm .So the future work can also be done to lessen the possibility of attack by using Intrusion detection of the network ,it means that firstly we will trace all the nodes present in the network one by one and wherever we can find the malicious node going to attack on that particular node ,we will detect that node and then stopped the functioning of that particular node and not allow that node to transfer data .It means we will give the enhancement of intrusion detection and virus detection.

IX. REFERENCES

[1] Behrouz A. Forouzan, “Data communication and Networking,” 2nd edition, Tata McHill publication, 2001[7] S. Murthy and J. J. Garcia-Luna-Aceves, “An Efficient Routing Protocol for Wireless Networks,” ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183–97.

[2] Laouiti, A.Qayyum, and L.Viennot, “Multipoint Relaying; An Efficient Technique for Flooding in Mobile Wireless Networks,” in Proceedings of the 35th Annual Hawaii International Conference on System Science (HICSS’ 2002), Waikoloa, HI, January 2002.

[3] D.B. Johnson, D.A. Maltz, V. D. Park and M. S. Corson, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks,” Proc. INFOCOM ’97, Apr. 1997.

[4] Behrouz A. Forouzan, “Cryptography and Network Security”, Special Indian Edition, Tata McHill publication, 2007

[5] C. Siva Ram Murthy and B. S Manoj, “Ad Hoc Wireless Networks, Architecture and Protocols”, Prentice Hall PTR, 2004.

[6] Stefano Basagni, Macro Conti, Silvia Giordano and Ivan Stojmenovic, “Mobile Ad Hoc Networks”, IEEE press, A john Wily & Sons, INC. publication, 2003

[7] George Aggelou, “Mobile Ad Hoc Networks”, 2nd edition, Mc GRAW Hill professional engineering, 2004.

[8] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, “Mobile Ad Hoc Networking: Imperatives and Challenges”, Elsevier Network Magazine, vol. 13, pages 13-64,2003

[9] E.M. Belding-Royer and C. K. Toh, “A review of current routing protocols for Ad-hoc Mobile wireless networks”, IEEE Personal Communications Magazine, pages 46–55, April 1999.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, Proc. of the 3rd Intl. Symp. on Information Processing in Sensor Networks, 2004.