

A Review on Enhancing the Security of the Link State Protocol in MANET Using Cryptography

Richa Kumari, Charu Kathuria

M. Tech (Pursuing), Dept. of Computer Science, BSAITM, Faridabad, Haryana, India

Assistant Professor, Dept. of Computer Science at BSAITM, Faridabad, Haryana, India

ABSTRACT: MANETs is a collection of wireless mobile nodes forming flexible networks, thus they do not require any existing infrastructure and centralized access points. With the expansion of the existing wireless networks and the emergence of new applications that require a real time communication with low cost, higher efficiency and less complexity; routing protocols become one of the most important decisions in the design of these networks. More recently, an increasing emphasis has been on the potential of infrastructure less wireless mobile networks that are easy, fast and in-expensive to set up, with the view that such technologies will enable numerous new applications in a wide range of areas. Such networks are commonly referred to as MANET. In MANET data is transferred from source to destination by the link state protocol and the security is provided by the cryptography technique. This paper concentrates on the security of the routing protocol, for security the cryptography technique is used where the data is encrypted and then it is decrypted by the receiver as soon as it is received.

I. INTRODUCTION

MANET: Mobile Ad Hoc Network (MANET) is formed by nodes having no infrastructure. In MANET the nodes involved act as router. Routing in such an ad hoc network is challenging due to the lack of central control and the high dynamics of the network. Nodes are free to move in any direction and organize themselves arbitrarily[1]. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently.

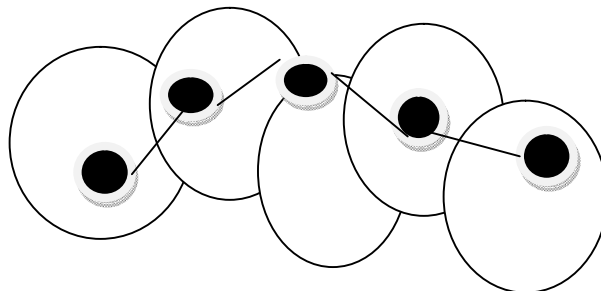


Figure 1 Mobile Ad Hoc Network

Categories of MANET: Mobile Ad-hoc routing protocols can broadly be classified into three categories as:

- i. Proactive Routing Protocol
- ii. Reactive Routing Protocol
- iii. Hybrid Routing Protocol

Proactive Routing Protocol: Proactive approach is also known as Table-Driven approach. It involves attempting to maintain routes between nodes in the network at all times, plus when the routes are not currently being used[4]. The advantage of this approach is that there is little or no latency involved when a node wishes to begin communicating

International Journal of Innovative Research in Computer and Communication Engineering

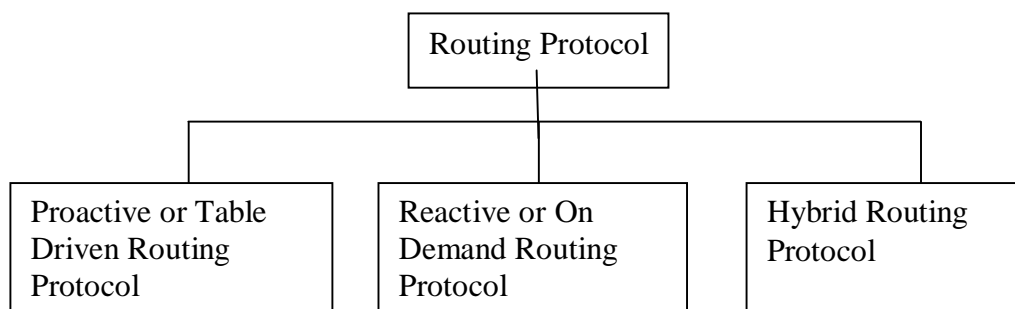
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

with an arbitrary node that it has not yet been in communication with and the disadvantage of the approach is that the control message overhead of maintaining all routes within the network can rapidly overwhelm the capacity of the network in very large networks, or situations of high mobility. The examples which fall under the proactive are Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing.

Reactive Routing Protocol: Reactive routing protocol is also known as on-demand approach. It involves searching for routes to other nodes only as they are needed. A route discovery process is invoked when a node wishes to communicate with another node for which it has no route table entry. Reactive protocols have the advantage of being more scalable as compared to table-driven protocols and the other advantage is that they require less control traffic to maintain routes. The disadvantage of these methods is that an additional latency is incurred in order to discover a route to a node for which there is no entry in the route table [2]. The examples which fall under this are Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector Routing (AODV) and etc.

Hybrid Routing Protocol: Such as the Zone Routing Protocol (ZRP), which employs a combination of proactive and reactive methods. The Zone Routing Protocols maintains groups of nodes in which routing between members within a zone is via proactive methods, and routing between different groups of nodes is via reactive methods.



Characteristics of Manet

- I. It basically works on the dynamic topology.
- II. Manet can move in any direction independently.
- III. Communication via wireless, no need to take the burden of wires.
- IV. More prone to physical security threats than fixed cable networks.
- V. Network can be extended to that places which cannot be wired.

Application of MANET

- I. **Tele-medicine:** Conference assistance from a surgeon for an emergency intervention.
- II. **Personal area network and Bluetooth :** A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.
- III. **Collaborative work:** For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

II. LITERATURE REVIEW

2.1 Kaur Sharndeeep, Gupta Anuj [2] introduced MANETs is a collection of wireless mobile nodes forming flexible networks, thus they do not require any existing infrastructure and centralized access points. With increase in the use of Mobile Ad hoc Networks security became a fundamental requirement due to its dynamic topology, limited processing capability, bandwidth constraints, lack of central control and high bit error rate. In this paper we attempt to give a review on various secure routing protocols, security analysis of available secure protocols by identifying their advantages and disadvantages as well as comparing their relative metrics and requirements. We have examined that different authentication mechanisms and secure routing protocols till yet defend against these attacks to a certain level, no one is perfect since most of these solutions are having drawbacks such as more time delay, much network routing overhead because of newly introduced packets, exposes network configuration, wastage of bandwidth etc. To provide



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

more security and immovability in MANETs there is need to develop efficient security mechanism and secure routing protocols.

2.2 Kanata Pasrija, Ashok Kajal and Seema[3] introduced that over the past decade or so, there has been rapid growth in wireless and mobile applications technologies. More recently, an increasing emphasis has been on the potential of infrastructure less wireless mobile networks that are easy, fast and in-expensive to set up, with the view that such technologies will enable numerous new applications in a wide range of areas. Such networks are commonly referred to as mobile ad hoc networks. Each protocol has its own criteria to find the path from source to destination. Some of researchers explored the concept of shortest path routing over ad hoc network. In this paper, we will discuss the solution given by them.

2.3 Sumitha J[4] introduced Network is defined as a group of two or more computer systems which are linked with each other. It allows computers to exchange data from each other along the data connections. Routing is a process of selecting path in a network along which the packets are sending over the network traffic. In this paper, an analysis is made over the routing algorithms such as between the adoptive routing algorithms and the non adoptive routing algorithms. The results are favored to the adoptive routing algorithms in which the researchers can easily find the best routing path in a traffic over the network since it adjusts to network when compared with non adoptive routing algorithms. The redundancy is reduced in the dynamic or adoptive routing algorithm when compared with non adoptive routing algorithms. For non adoptive routing algorithms, most probably, dijkstra's algorithm is used for finding shortest path. It does not give redundancy as such that in the adoptive or dynamic routing

2.4 Shubhi, Prashant Shukla[1] introduced With the expansion of the existing wireless networks and the emergence of new applications that require a real time communication with low cost, higher efficiency and less complexity; routing protocols become one of the most important decisions in the design of these networks. In this paper distance vector protocol and Link state protocol are presented based on Bellman-Ford algorithm and Dijkstra's algorithm respectively. This paper compares the advantages and disadvantages of DVF and OSPF on the basis of their performance. Our study shows that result of the shortest path routing also depends upon the selected parameters and as well as on the selected protocol used for routing. Each author worked on a specific parameter but no one has considered all the parameters in a particular solution, discussed in this paper.

III. INTRODUCTION OF SHORTEST PATH ROUTING

Shortest path can be calculated for the graph in which the weights are provided. The shortest path problem is the problem of finding a path between two vertices (or nodes) in a graph such that the sum of the weights of its constituent edges is minimized[5]. The problem of finding the shortest path between two intersections on a road map (the graph's vertices correspond to intersections and the edges correspond to road segments, each weighted by the length of its road segment) may be modeled by a special case of the shortest path problem in graphs. Shortest path routing refers to the process of finding paths through a network that have a minimum of distance or other cost metric[7]. Routing of data packets on the Internet is an example involving millions of routers in a complex, worldwide, multilevel network. Optimum routing on the Internet has a major impact on performance and cost.

As the name suggests, shortest path algorithm find the shortest path between two nodes in a network. In the case of transportation networks, the nodes may represent points (or locations) from which traffic is produced or to which traffic is attracted. The nodes also represent intersections[3]. The links represents roads or movements. The above description of a transportation network is a very simplistic viewpoint. Interested readers may refer to books on transportation network analysis to gain an insight of how a real-world transportation facility may be represented as a network.

The most important algorithms for solving the problem of the Shortest Path First are the:

[Dijkstra's algorithm](#) solves the single-source shortest path problem.

[Bellman-Ford algorithm](#) solves the single-source problem if edge weights may be negative.

[A* search algorithm](#) solves for single pair shortest path using heuristics to try to speed up the search.

[Floyd-Warshall algorithm](#) solves all pairs shortest paths.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Here in this paper the algorithm which we have discussed for the shortest path problem is the Dijkstra's algorithm.

Dijkstra's Algorithm:

Dijkstra's algorithm is an [algorithm](#) for finding the [shortest paths](#) between [nodes](#) in a [graph](#), which may represent, for example, road networks. For a given source node in the graph, the algorithm finds the shortest path between that node and every other [6][2]. It can also be used for finding the shortest paths from a single node to a single destination node by stopping the algorithm once the shortest path to the destination node has been determined. For example, if the nodes of the graph represent cities and edge path costs represent driving distances between pairs of cities connected by a direct road, Dijkstra's algorithm can be used to find the shortest route between one city and all other cities [5]. As a result, the shortest path algorithm is widely used in network [routing protocols](#), mostly Open Shortest Path First (OSPF). In Dijkstra both directed and undirected graphs, all edges must have nonnegative weights and graph must be connected.

IV. CONCLUSION

In this paper we have discussed about the MANET, how does the MANET works and the routing protocol used in MANET. Brief about the protocol is provided which are used in the MANET, are the Proactive routing protocol which is also known as table driven approach, Reactive routing protocol which is known as on demand approach and the third approach is the Hybrid routing protocol. Then the challenges in the MANET are discussed, the techniques used for the broadcasting are discussed. Shortest path algorithm is briefed in which the steps of selecting the shortest path is discussed and the algorithm which is used for the solution of the shortest path is the Dijkstra's algorithm. Dijkstra's algorithm is an [algorithm](#) for finding the [shortest paths](#) between [nodes](#) in a [graph](#), which may represent, for example, road networks. Still the search on the security of the protocol is going on because it is still not secure.

REFERENCES

- [1] Shubhi¹, Prashant Shukla², "Comparative Analysis of Distance Vector Routing & Link State Protocols", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 10, October 2015
- [2] Kaur Sharandeep, Gupta Anuj, "a review on different secure routing protocols and security attacks in mobile ad hoc networks", international journal of advanced engineering technology e-issn 0976-3945, vol. v/issue iv/oct.-dec.,2014/01-05
- [3] Kanika Pasrija, Ashok Kajal and Seema, "SURVEY: SHORTEST PATH ROUTING OVER MOBILE AD HOC NETWORKS", International Journal of Advanced Research in Engineering and Applied Sciences, Vol. 2 | No. 4 | April 2013
- [4] Sumitha J. "Routing Algorithms in Networks", Research Journal of Recent Sciences, Vol. 3(ISC-2013), 1-3 (2014)
- [5] KARAMJEET KAUR 1, SUKHJEET SINGH, RAHUL MALHOTRA, "DESIGN OF OPEN SHORTEST PATH FIRST PROTOCOL –A LINK STATE PROTOCOL USING OPNET MODULAR", International Journal of Computer Science and Mobile Computing, Vol. 1, Issue. 1, December 2012
- [6] Mr. K.J. Pavithran Kumar, Mr. K. Rajasekhar² and Mr. N. Siddaiah, "Improving Security Using Dynamic Routing for Data Transmission", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013
- [7] Rajesh R Mane, "A Review on Cryptography Algorithms, Attacks and Encryption Tools", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 9, September 2015
- [8] Divya sukhija, "A Review Paper on AES and DES Cryptographic Algorithms", International Journal of Electronics and Computer Science Engineering, Volume 3, Number 4
- [9] Mitali¹, Vijay Kumar² and Arvind Sharma, "A Survey on Various Cryptography Techniques", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, July-August 2014
- [10] Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013
- [11] Asmaa Shaker Ashoor, "Performance Analysis Between Distance Vector Algorithm (DVA) & Link State Algorithm (LSA) For Routing Network", IJSTER Volume 4, Issue 02, FEB 2015
- [12] Sumitha J. "Routing Algorithms in Networks", Research Journal of Recent Sciences, ISSN 2277-2502 Vol. 3(ISC-2013), 1-3 (2014)
- [13] Cheolgi Kim, Young-Bae Koy and Nitin H. Vaidya, Link State Routing Protocol for Multi-Channel Multi-Interface Wireless Networks, IEEE (978-1-4244-2677-5/08)/\$25.00c (2008).