"Secure Data Communication in Mobile Adhoc Networks"

Chidambar R Joshi

Research Scholar, Bundelkhand University, Jhansi

Abstract – The rising need for mobile ad hoc networks and secured communication and data transmission is of vital importance depending upon the environments where secure data communication is required. In this paper we present about the aspect of secure communication in mobile ad hoc networks.

Keywords: Transmission, Mobile Ad Hoc Networks, Security

---♦---

INTRODUCTION

In Mobile adhoc network, consistent delivery of information to the proposed destination is of main interest to users sending information across that network. The information on the network might not be delivered to the destination as it is interrupted by the system because of many reasons. These reasons can be grouped into two parts, network faults and security attacks. In the former, major difficulty is to detect abnormal changes in the network and classify them. Security attacks [1, 2] can be protected and authenticated by cryptography.

The most important features of this new networking paradigm are as follows:

1) Mutual support of basic networking functions, such as routing and data transmission;

2) Lack of organizational limits of the network nodes;

3) Absence of a central entity in the network;

4) Transient, in general, relations of the network nodes.

As a result, a node cannot make any statement about the trustworthiness of its peers, which help the node with its communication and, in general, does not possess their credentials.

REVIEW OF LITERATURE:

The accessible protocol SMT [3] for secured data communication provides end to end secure and robust feedback method. A set of varied and node disjoint paths are used at a time for data transmission and are known as Active Path Sets.

The message and the redundancy are separated into a number of parts, so that even a partial reception is able to reconstruct the data, called as Message dispersion [4]. The source updates the ratings of the paths based on the criticism. Secure Routing Protocol [5] is an overlay security layer for previously existing routing protocol such as DSR [6]. The protocol bases its security on the assumption that the source and the destination share an verification primitive. The routing messages are secluded by nodes end-to-end authentication. SRP uses the route redundancy between the two end-hosts to amplify the robustness against malevolent nodes. The network is secluded against flooding of route requests by limiting the rate of route request processed at each node. The problem is that the neighbors are not genuine so a malevolent node can blackmail other nodes by sending fake route requests.

Besides, SRP does not make any hypothesis on the route request propagation algorithm as it is using the underlying protocol's one which is not optimized to find disjoint paths.

MESSAGE DISPERSION AND TRANSMISSION:

The information spreading scheme is based on Rabin's algorithm [7], which acts in spirit as an erasure code: it adds partial redundancy to the data to allow revival from a number of fault.

The message and the redundancy are divided into a number of parts, so that even a limited reception can lead to the successful rebuild of the message at the receiver. In belief, the encoding (and dispersion) allows the renovation of the original message with successful reception of any M out of N transmitted pieces. The ratio r = N/M is termed the redundancy factor[8].

CONCLUSION:

In this paper we found that SMT is one of the most usable protocols for secure data communication in ad hoc networks. This protocol is widely applicable, as it provide frivolous end-to-end security services, and operate without knowledge of the reliability of individual network nodes.

REFERENCES:

1. N. Milanovic, M. Malek, A. Davidson and V. Milutinovic “Routing and Security in Mobile Ad Hoc Networks”, IEEE Computer Magazine, vol. 37, no. 2, February 2004.

2. Karlof and D. Wagner “Secure Routing in Sensor Networks: Attacks and Countermeasures” in Proc. of the 1st IEEE Workshop on Sensor Network Protocols and Applications, May 2003, pp.1-15.

3. Papadimitratos, P. Haas, Z.J.]”Secure data communication in mobile adhoc networks” IEEE Journal on Publication Date: Feb. 2006, Volume: 24, Issue: 2, on page(s): 343- 356

4. M. O. Rabin, “Efficient dispersal of information for security, load balancing and fault tolerance”, Journal ACM (1989) 36 no. 2, pp. 335–348.

5. Sebastien Berton, Hao Yin, Chuang Lin, Geyong Min, “Secure, Disjoint, Multipath Source Routing Protocol (SDMSR) for Mobile Ad-Hoc Networks”, (2006) Proc of the Fifth International Conference on Grid and Cooperative Computing (GCC'06), pp. 387-394.

6. D. Johnson, D. Maltz and J. Broch., “DSR The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks”, chapter 5, Addison-Wesley, 2001. Pages 139–172.

7. M.O. Rabin, “Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance,” Journal of ACM, Vol. 36, No. 2, pp. 335-348, Apr. 1989.

8. Panagiotis, Papadimitratos and Zygmunt J. Haas,” Secure Data Transmission in Mobile Ad Hoc Networks” ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003