"Distributed PAAA Protocol Framework for Secure Communication in Mobile Adhoc Networks"

Sidagouda Basagouda Patil

Research Scholar, Bundelkhand University, Jhansi

Abstract – In this paper we present about the protocol framework for secure communication in mobile adhoc networks. Securing access network is the primary fortification against fraudulent access to network services. Authentication method is essential for securing the access to the network. This mechanism is as much susceptible as the media communication is eavesdropping responsive.

Keywords: Wireless Network, Routers, Connectivity, Nodes

----------♦----------

INTRODUCTION

Wireless mesh networks (WMNs) have appeared as a promising concept to meet the confronts in next-generation wireless networks such as providing elastic, adaptive, and reconfigurable architecture while offering cost-effective solutions to service providers [1]. Wireless mesh networks are multi-hop networks consisting of mesh routers (MRs), which form wireless mesh backbones and mesh clients (MCs). The mesh routers provide rich radio mesh connectivity which considerably reduces the up-front operation cost of the network. Mesh routers are classically stationary and do not have power constraints. However, the clients are mobile and energy-constrained. Some mesh routers are elected as gateway routers which are linked to the Internet through a wired vertebral column. Gateway routers provide access to conservative clients and interconnect ad hoc, sensor, cellular, and other networks to the Internet. The gateway routers are also referred to as the Internet gateways (IGWs). A mesh network can provide multi-hop communication paths between wireless clients, thus serving as a public network, or can present multi-hop paths between the client and the gateway router, thereby providing broadband Internet access to the clients [2].

REVIEW OF LITERATURE:

In mobile ad-hoc networks, nodes play a role as both routers and terminals. For the lack of routing transportation, they have to assist to communicate. Cooperation at the network layer takes place at the level of routing, i.e. ruling a path for a packet, and forwarding, i.e. relaying packets for other nodes. This network is typically characterized by a dynamic topology, a limited bandwidth, power restraints, the heterogeneity nodes, and a limited physical security. The applications having recourse to the ad hoc networks cover a very broad spectrum. For example in the tactical applications (fires, flood, etc.), in the soldier's field, in the monitoring systems, and the world of transport [3].

An attack is an action which aims at compromising the security of the network. They are many and varied in these MANET:

BlackHole attack: consists in dropping some routing messages that node receives [1, 2, 3, 4, 5, 27]. It was declined in several particularity alternatives, having different objectives, among which we can quote:

- Routing loop, which makes it possible for a node to create loops in the network;
- Grayhole, which lets pass only the packages of routing and diverts the data;
- Blackmail, which makes it possible for a node attacker to isolate another node.

Several solutions exist to counter these types of attacks, among which we name the technical estimate relation [9].

REQUIREMENTS FOR AUTHENTICATION IN WMNS:

On the basis of whether a central authentication server is available, there are two types of implementations of

access control enforcements in WMNs [2]:

(i) Centralized access control and

(ii) Distributed access control.

For both these approaches, the access control policies should be implemented at the border of the mesh network. In the distributed access control, the access points could act as the distributed authentication servers [2]. The authentication could also be performed in three different places:

- A remote central authentication center
- Local entities such as IGWs or MRs that play the role of an authentication server
- Local MRs

CONCLUSION:

In this paper we found that Mobile ad-hoc routing and forwarding are susceptible to misconduct, which can happen due to selfish, malevolent, or faulty nodes. Solution to the problem of misbehavior has so far been categorized into three major categories: payment systems, secure routing, and detection and reputation systems. Secure routing suggestions aspire at the prevention of malevolent misbehavior. Self-policing systems consist of recognition, character, and response components target at the isolation of misbehaved nodes regardless of the reason for misbehavior.

REFERENCES:

1. Akyildiz, I. F.; Wang, X. & Wang, W. (2005). Wireless Mesh Networks: A Survey. Computer Networks, Vol 47, No 4, pp. 445–487, March 2005.

2. Jaydip Sen, Secure and Privacy-Preserving Authentication Protocols for Wireless Mesh Networks

3. Wiley John: Security for Wireless ad hoc networks. Eyrolles, book 2007, pages 247.

4. Adjido Idjiwa, Benamara Radhouane, Benzimra Rebecca, Giraud Laurent: Protocol of secure routing ad hoc in a clusterized architecture. University Pierre and Marie Curia(Paris VI), FRANCE, November 2005,pages 4.

5. Curtmola Reza. Security of Routing Protocols in MANET. 600.647-Advanced Topics in Wireless Networks,February 2007,pages 26. International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November 2011 345

6. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei. A Survey of Attacks and Countermeasures in MANET. Department of Computer Science and Engineering Florida Atlantic University, Decembre 2005

7. Chen Ruiliang, Snow Michael, Park Jung-Min, M. Refaei Tamer, Eltoweissy Mohamed. Defense against Routing Disruption Denial-of-Service Attacks in MANET. Department of Electrical and Computer Engineering Virginia Polytechnic Institute and State University Blacksburg, VA, USA, November 2005,pages 15.

8. E. Venkat Reddy. Trustworthy Robust Routing Protocol for Mobile Ad Hoc Network, International Journal of Engineering Science and Technology Vol.2 (2), 2010, 77-86, Amina Institute of Technology, Hyderabad, Andhra Pradesh-India, Fevrier 2010, pages 10

9. Dr Karim KONATE and Abdourahime GAYE," Modelling of a secure mechanism in routing protocol of manets: application of theory of games" International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November 2011