Abstract

In wired networks, building reliable and secured network connections is becoming extremely important. Security and Routing in wired networks remain challenging problem due to the complexity involved such as improper path discovery, congestion, network traffic and delay. In this paper, we first analyze the vulnerabilities for networks under different types of attacks.
Then, we propose an Authentication and key assignment protocol to hierarchical routing to overcome those vulnerabilities with the security functionality to prevent malicious attacks. Hence, both Security and routing analysis is provided for Hierarchical Network Routing using Authentication and Integrity, and Key Assignment protocol. A class of continuous metrics to evaluate the vulnerability as a function of security and routing protocols used in networks has been formulated. Joint analysis of Security and Routing is used as it reveals the weaknesses in the network that remain undetected when Security and Routing protocols are analyzed independently. Interleaving has also been considered to increase performance. Performance metrics such as Packet Delivery Fraction, End-to-End Delay, and Packet Loss are considered.

Reference

- Seung Yi, Prasad Naldurg and Robin Kravets, “Security Aware Ad hoc routing for Wireless Networks”.
- NS-2 Simulator. URL:http://www.isi.edu/nsnam/ns.
- Chao Lv, Maode Ma, Hui Li and Jianfeng Ma, “A Security Enhanced Authentication and Key Distribution Protocol for Wireless Networks,” 2010 IEEE.
- Huaiyong Li, Zhenliu Chen, Xiangyang Qin, Chengdong Li and Hui Tan, “Secure Routing in Wired Networks and Wireless Ad Hoc Networks, April 2002”, Department of Computer Science,
An Approach to Secure Hierarchical Network using Joint Security and Routing Analysis

University of Kentucky.

Index Terms

Computer Science
Network Security

Key words

Authentication
Hierarchical Routing
Key
Assignment Protocol
Network Security
Routers
Vulnerability
Attack