

EINLADUNG

Zeit: Mittwoch, 22. Juni 2011, 15:00 Uhr

Ort: Raum 5055, Ahornstr. 55

Referent: M.Sc. Fahad Samad
Informatik 4, RWTH Aachen University

Titel: Securing Wireless Mesh Networks – A Three
Dimensional Perspective

Abstract:

Wireless Mesh Networks (WMNs) are multi-hop networks that have secured a significant position in the technological world due to their unique characteristics. These networks are dynamically self-healing, self-organizing, and self-configurable. They help to realize the future of network connectivity anywhere and anytime. Moreover, WMNs substantially minimize the complexity in network deployment and maintenance hence reduce the deployment costs of the networks.

Different schemes to protect the nodes in WMNs from adversaries and brutal attacks have been proposed over the years. Many of these schemes have certain limitations. Either the schemes use cryptographic mechanisms which are computationally complex or assume to have centralized trusted authorities and authentication strategies. However, a WMN does not usually have a centralized trust and being a multi-hop network, does have relay nodes. Therefore, security solutions in these networks must be computationally efficient, lightweight, and must handle the additional threats possible from relay nodes. For instance, WMNs are highly prone to severe security attacks such as denial of service attacks. This sense of being insecure demotivates the users and companies to deploy and provide astonishing wireless services through WMNs. Moreover, these networks may offer various services to users having distinguishing capabilities and security requirements.

We try to present the security issues of WMNs in three dimensions. Firstly, we present a lightweight protection mechanism based on neighborhood trust to gain security in a clustered WMN. Our approach renders a lightweight protection scheme against security vulnerabilities using hash chains and does not require any trusted authority. Secondly, we propose two schemes to mitigate severe denial of service attacks known as channel assignment attacks and jellyfish attacks in mesh networks. Finally, we suggest an adaptive service-level association mechanism to provide tunable security level in these networks.

Es laden ein: Die Dozenten der Informatik