Chapter 10
Security in Ad-Hoc Networks (MANETS)

Piyush Kumar Shukla
UIT RGPV, India

Kirti Raj Bhaitele
UIT RGPV, India

ABSTRACT

Wireless Networks are vulnerable in nature, mainly due to the behavior of node communicating through it. As a result, attacks with malicious intent have been and will be devised to exploit these vulnerabilities and to cripple MANET operation. In this chapter, we analyze the security problems in MANET. On the prevention side, various key and trust management schemes have been developed to prevent external attacks from outsiders. Both prevention and detection method will work together to address the security concern in MANET.

BACKGROUND

Security is an essential requirement of mobile Ad-hoc network. In the past few years, we have seen a rapid expansion in the field of mobile computing due to the proliferation of inexpensive, widely available wireless devices. However, current devices, applications and protocols are solely focused on cellular or wireless local area networks (WLANs), not taking into account the great potential offered by mobile ad hoc networking. The mobile ad-hoc network consists of the nodes that are mobile in nature such as laptops, sensors, smart phones etc. The ad-hoc network does not have any pre-defined or fixed infrastructure. The nature of the ad-hoc network is wireless in nature which operates in distributed manner. The network can oper-

DOI: 10.4018/978-1-4666-8687-8.ch010

Copyright ©2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Security in Ad-Hoc Networks (MANETS)

Ates as standalone network or can have multiple points for connection. Application scenarios include, but are not limited to: emergency and rescue operations, conference or campus settings, car networks, personal networking, etc. Due to openness MANET is vulnerable to several attacks i.e. external or internal attacks. To Secure MANET several security solutions have been proposed by various scientists. In this chapter, we discuss the security issues, solution and research issues that need to be addressed in mobile ad-hoc network Overview.

Nature of MANET brings new security challenges to network design. Because node in mobile ad-hoc network generally communicates with each other via open and shared broadcast wireless channels, they are more vulnerable to security attacks. In addition, their distributed and infrastructure less nature means that centralized security control is hard to implement and the network has to rely to individual security solution from each mobile node. Furthermore, as ad-hoc network are often designed for specific environments and may have to operate with full availability even in adverse condition, security solution applied in more traditional networks may not be directly suitable.

DESCRIPTION

Mobile ad-hoc networks (MANETs) are spontaneously deployed over a geographically limited area without well-established infrastructure. The networks work well only if the mobile nodes behave cooperatively. MANETs is very vulnerable to various attacks from malicious nodes. In order to reduce the hazards from such nodes and enhance the security of network several security solutions have been introduced. Both prevention and detection method will work together to address the security concern in MANET.

INTRODUCTION

Today one of the major problems that the ad-hoc network is facing is the Security (Yi, Dai, Zhang, Zhong, 2010). Ad-hoc network requires the robust security schemes for transmitting information over the network. As the ad-hoc network are having dynamic topology, mobile nodes, wireless transmission media there the privacy and security of the node is to be maintained. There are two levels of security schemes that can be applied to the network: Low Level and High Level. The low level security scheme is applied to the network where the security has to be kept of the minimum level. The main focus is the low level scheme is to make the network secure applying security mechanisms. This implies key exchange, privacy, capture node attack,
Related Content

Network Design and Performance Evaluation of Wireless Sensor Network for Precision Agriculture
www.igi-global.com/chapter/network-design-and-performance-evaluation-of-wireless-sensor-network-for-precision-agriculture/129216?camid=4v1a

Multiple Attributes Decision Making Algorithms for Vertical Handover in Heterogeneous Wireless Networks
Enrique Stevens-Navarro, José D. Martínez-Morales and Ulises Pineda-Rico (2012). Wireless Multi-Access Environments and Quality of Service Provisioning: Solutions and Application (pp. 52-71).
www.igi-global.com/chapter/multiple-attributes-decision-making-algorithms/61836?camid=4v1a
What Can People Do with Your Spatial Data?: Socio-Ethical Scenarios
www.igi-global.com/chapter/what-can-people-do-with-your-spatial-data/164310?camid=4v1a

Doubly Cognitive Architecture Based Cognitive Wireless Sensor Networks
www.igi-global.com/article/doubly-cognitive-architecture-based-cognitive/55880?camid=4v1a