

Chapter 86

Security Issues in Mobile Ad Hoc Networks: A Survey

Sunil Kumar

National Institute of Technology, India

Kamlesh Dutta

National Institute of Technology, India

ABSTRACT

A Mobile Ad hoc NETWORK (MANET) is a self-organizing, infrastructure-less network of mobile nodes connecting by wireless links. In operation, the nodes of MANETs do not have a central control mechanism. It is known for its properties of routable network, where each node acts as a router to forward packets to other specific nodes in the network. The unique properties of MANET have made it useful for large number of applications and led to a number of security challenges. Security in the mobile ad hoc network is a very critical job and requires the consideration of different security issues on all the layers of communication. The countermeasures are the functions that reduce or eliminate security vulnerabilities and attacks. This chapter provides a comprehensive study of all prominent attacks in Mobile Ad Hoc Networks described in the literature. It also provides various proactive and reactive approaches proposed to secure the MANETs. Moreover, it also points to areas of research that need to be investigated in the future.

INTRODUCTION

Wireless cellular system has been in operation since the 1980s. Wireless system operates through a centralized support structure such as an access point. Recent advancement of wireless technologies such as Bluetooth (Karygiannis, & Owens, 2002), IEEE 802.11 (Borisov, Goldberg, &

Wagner, 2001) introduced a new type of wireless system known as Mobile ad hoc networks (MANETs), which operate in the absence of a central access point (Toh, 2001; Chlamtac, Conti, & Liu, 2003). It provides high mobility and portability of the device, which allows a node to communicate with the network and communication with each other in the network.

DOI: 10.4018/978-1-4666-8751-6.ch086

Security Issues in Mobile Ad Hoc Networks

In Latin “Ad hoc” means “For a particular purpose only”. The ad hoc Network is a spontaneous network and it is especially useful where installation of fixed network is not so easy (Chlamtac et al., 2003). A mobile ad hoc network is infrastructure-less network comprising of autonomous collection of mobile nodes connected by wireless medium and is capable of organizing itself into arbitrary changeable topologies (Perkins, 2001; Stallings, 2009). It is a system of mobile nodes with routing capabilities where each node operates both as host as well as router to forward the packets to each other as shown in Figure 1. The mobile ad hoc network has the following typical characteristics (Murthy, & Manoj, 2004; Ilyas, 2010):

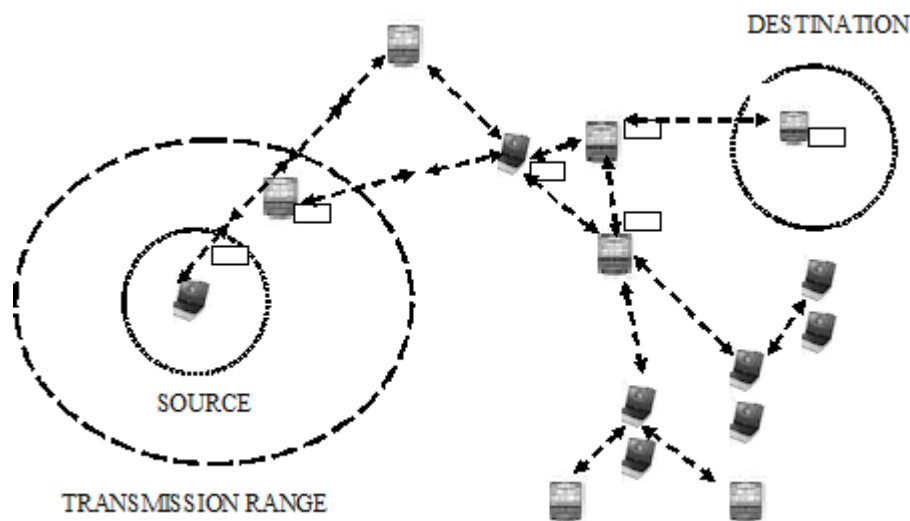
- Autonomous in Behaviour
- Multi-Hop Routing Paths
- Dynamic Topology
- No Infrastructure
- Distributed Operation
- Very Limited Transmission Range
- Device Size Limitation

A MANET environment has to overcome certain issues of limitation and inefficiency:

- Limited Range of Wireless transmissions
- Unreliability of wireless links between nodes
- Packet loss due to errors in the transmission
- Route Changes due to Mobility
- Frequent network Partition
- Limited Battery Life
- Bandwidth and Slower Data Transfer Rate
- Resource Constraints
- Weaker In Security (Lack of Centralized Management Facility)
- Limited Physical Security

Apart from these limitation MANET has many extensive application like: Military communication and operations, Automated battlefields, Search and rescue operations, Disaster recovery, Policing and fire fighting, supporting doctors and nurses in hospitals, Conferences, meeting rooms, Virtual classrooms, Wireless P2P networking etc. The unique properties of MANETs present a new set of non trivial challenges to the security design.

Figure 1. Mobile Ad Hoc Network.



44 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/security-issues-in-mobile-ad-hoc-networks/138364

Related Content

Factors Affecting WiFi Use Intention: The Context of Cyprus

Despo Ktoridou, Hans-Ruediger Kaufmann and Christos Liassides (2012). *Wireless Technologies: Concepts, Methodologies, Tools and Applications* (pp. 1760-1781).

www.irma-international.org/chapter/factors-affecting-wifi-use-intention/58867

BER Fairness and PAPR Study of Interleaved OFDMA System

Sabbir Ahmed and Makoto Kawai (2011). *International Journal of Wireless Networks and Broadband Technologies* (pp. 1-15).

www.irma-international.org/article/ber-fairness-papr-study-interleaved/55878

Analysis of Bandwidth Efficiency in IEEE 802.11 and 802.16 Interworking Networks

Mateen Yaqoob and Mustafa Shakir (2018). *International Journal of Wireless Networks and Broadband Technologies* (pp. 25-38).

www.irma-international.org/article/analysis-of-bandwidth-efficiency-in-ieee-80211-and-80216-interworking-networks/209433

Load-Balance Energy Aware Ad-Hoc On Demand Multipath Distance Vector Routing Protocol (LBEA-AOMDV) for WSN

Amany Sarhan, Nawal A. El-Fishawy and Mahmoud M. Shawara (2018). *International Journal of Wireless Networks and Broadband Technologies* (pp. 38-58).

www.irma-international.org/article/load-balance-energy-aware-ad-hoc-on-demand-multipath-distance-vector-routing-protocol-lbea-aomdv-for-wsn/236065

Printing Techniques and Performance of Chipless Tag Design on Flexible Low-Cost Thin-Film Substrates

Rubayet-E-Azim Anee, Sushim Mukul Roy, Nemai Chandra Karmakar, Ramprakash Yerramilli and Gerhard F. Swiegers (2012). *Chipless and Conventional Radio Frequency Identification: Systems for Ubiquitous Tagging* (pp. 175-195).

www.irma-international.org/chapter/printing-techniques-performance-chipless-tag/65981