A Systematic Study and Analysis of Security Issues in Mobile Ad-hoc Networks

Jhum Swain, Department of Computer Science and Engineering, Siksha ‘O’ Anusandhan University (Deemed), Bhubaneswar, India
Binod Kumar Pattanayak, Department of Computer Science and Engineering, Siksha ‘O’ Anusandhan University (Deemed), Bhubaneswar, Odisha
Bibudhendu Pati, Department of Computer Science and Engineering, C. V. Raman College of Engineering, Bhubaneswar, India

ABSTRACT

A Mobile Ad Hoc Networks (MANETs) is an assortment of a variety of portable nodes that are linked collectively in a greater number in a wireless medium that has no permanent infrastructure. Here, all the nodes in the network act as both router and host and is in charge for accelerating and forwarding packets to other nodes. Due to the frequent link failure and high speed of mobile nodes, there are many challenges in MANET. As security is the basic challenge in a MANET, this article discusses the various protocols developed for security issues in MANET and IoT and presents a comparative analysis on their performance. After detailed analysis and comparison, it was observed that when security features are imposed at different levels during routing, various protocols perform in different ways. Also, the network performance and network life times vary from one approach to another. So, this article also presents the effect of security features on data drop and delay of prominent protocols after simulation.

KEYWORDS
Confidentiality, IoT, MANET, Network Layer, Protocol, Security

DOI: 10.4018/IJISP.2018040103

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
1. INTRODUCTION

A MANET is a group of autonomous systems which are portable in nature and are linked by wireless links. Each node not only acts as an end system but also has a router to forward packets. As nodes freely move around the system and they organize themselves into a network, so for this reason its structure changes frequently. So, a special kind of algorithm is needed to accommodate the changing topology. As nodes dynamically establish paths among each other its attractive to various types of attackers, so we need secured communication among each other. Dynamically the nodes in MANETs join and leave the network. In MANET nodes openly connect and disappear at any point of time to maintain the connection. Some of the typical applications of MANET include Military applications, emergency and rescue operations, aircrafts, wireless sensor network, medical service, commercial use and personal area network. As MANETs is an infra-structure less network which consists of mobile nodes with wireless network interfaces, so nodes dynamically establish paths among one another. This is one of the reasons that it is attractive to various types of attacks by the intruders. So, a protected communication protocol is needed for this network and hence, security is an important feature in MANET. In this paper a detailed analysis of secured routing protocols in MANET has been carried out with basic consideration being the security mechanism imposed.

2. RELATED WORK

This section presents a detail study and review of advanced approaches proposed by eminent researchers in this field of security in MANET. Transmission of audio data with secured mechanism has been discussed in Athulya and Sheeba’s work (2012) where the authors have provided dual safety measures by encrypting and decrypting the audio at each node in the route using stream ciphering method. Security threats and their possible solutions have been discussed in Jan Von Mulert, Ian Weich and Winston K.G. Seah’s research (2012), and it also focuses on how modification of data is done using optimization technique for security. Praveen Joshi (2011) discusses about the various security problems and how to prevent them which are adopted in the network layer. Spoofing attack and their prevention techniques has been discussed in Yuseok, Tae-Hyung, and Jong’s (2012) work. The author proposed a model i.e. PBM (Policy Based Management) that deals with 4 entities in (Bostjancic & Timecenko) such as QoS, network resources, configuration and security. It has discussed about the vulnerability, challenges and security attacks on ad-hoc routing protocols. A bargained hub may disregard the secrecy rule of security and uncover vital data like private and open keys, status of hub, passwords, ideal course to approved hubs, geographic area of hubs and other control information in parcel headers to unapproved hubs introduce in the system (Dhivya, Karthik & Kumaran). A secured on-demand routing protocol has been proposed in (Wan, Ren, & Gu) that prevents various attacks in MANET and another regression based trust model for MANET has been implemented in
Proposed Isomorphic Graph Model for Risk Assessment on a Unix Operating System
www.igi-global.com/article/proposed-isomorphic-graph-model-for-risk-assessment-on-a-unix-operating-system/80020?camid=4v1a

User Authentication Based on Dynamic Keystroke Recognition
www.igi-global.com/chapter/user-authentication-based-on-dynamic-keystroke-recognition/167237?camid=4v1a