# Chapter 1
# Mobile Ad Hoc Networks Security Enhancement With Trust Management

**Vaishali Vilas Sarbhukan**
*Terna Engineering College, University of Mumbai, India*

**Lata Ragha**
*Father Conceicao Rodrigues Institute of Technology, University of Mumbai, India*

## ABSTRACT

*The mobility and scalability brought by wireless networks made it possible in many applications. In MANET, discovering the stable, secure, and reliable routes is a challenging research problem due to the open nature of wireless communications. In Zhexiong Wei Routing Trust scheme (ZWRT), Bayesian approach and Dempster Shafer theory is used to evaluate more realistic trust value. Mohamed et al proposed Establishing STAble and Reliable Routes (ESTAR) system in heterogeneous multihop wireless networks. The above existing methods failed to solve the complete problem of information loss in MANETs. There are several other reasons due to which the information may loss in MANETS, such as mobility and congestion of mobile nodes. Therefore, the novel Enhanced Trust-based Secure Routing (ETSR) scheme is presented to deliver stable, reliable, and secure data communication in MANETs. The simulation results demonstrate that ETSR routing protocol improve QoS performance as compared to state-of-the-art techniques.*

DOI: 10.4018/978-1-5225-9493-2.ch001

## INTRODUCTION

Due to self-setup and self-upkeep abilities of MANETs, nowadays mobile ad hoc networks (MANETs) have become a mainstream inquire about subject. A dynamic network can be designed with the help of wireless hubs which do not require a settled infrastructure. Because of portability and flexibility brought by remote framework made it conceivable in number of applications. Among all the modern remote systems, Mobile Ad hoc Network (MANET) is a champion amongst the foremost essential and distinctive applications. Tragically, the open medium, distributed nature and dynamic topology of MANET make it helpless against different sorts of assaults (Yu et al., 2013), (Wang et al., 2014). These assaults include black hole assault, grey hole assault, sybil assault, packet dropping assault and sleep deprivation assault etc. Hence, security is principle snag in strategic MANETs (Chapin & Chan, 2011). There are primarily two methodologies that can give security in MANETs. These methodologies are prevention based and detection based methodologies (Bu et al., 2011a), (Bu et al., 2011 b).Prevention based methodologies are based on cryptography and detection based methodologies focus on trust threshold. Prevention based methodologies are contemplated completely in MANETs (Fang, 2009), (Yu et al., 2010). One disadvantage of prevention based methodologies is that they require a centralized key administration foundation. But it is not possible practically in conveyed systems, for example, MANETs. Likewise, a centralized infrastructure will be the primary focus of opponents in war zones. On the off chance that the framework is annihilated, the entire system might be incapacitated. Moreover, in spite of the fact that prevention based methodologies can avert bad conduct, but still there are some possibilities stayed for noxious hubs. Noxious hubs can take an interest in the routing strategy and exasperate appropriate routing foundation. Albeit some fantastic work has been done on detection based approaches like reputation based schemes, payment schemes, cryptographic schemes and trust schemes, these schemes cannot guarantee route stability, reliability and security at the same time. Basically most of authors focus only on malicious users in network but while working in MANET authors have to consider parameters like mobility, energy level, density of nodes etc. Also most existing trust based approaches in MANETs, do not consider first-hand information and second-hand information at the same time to evaluate the trust of watched hub. Therefore, it results in inaccurate trust value estimation. Existing techniques failed to solve the complete problem of information loss in MANETs. There are several other reasons due to which the information may loss in MANETS such as mobility and congestion of mobile nodes. By considering above loopholes of existing methods a novel enhanced trust based secure routing scheme (ETSR) is designed to establish stable, reliable and secure routing path for data transmission.