A Survey of Efficient Trust Management Schemes in Mobile Ad-Hoc Network: Reliable Trust Management Framework of MANET

J. Kaur, J Kaur, Punjabi University, Patiala, India
S. Kaur, PURCITM, Punjab, India

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are comprised of an arrangement of self-sorting mobile hosts furnished with wireless interaction devices gathered in groups without the need of any settled framework as well as centralized organization to maintain a system over radio connections. Every mobile node can react as a host and also, the router freely utilizes the wireless medium inside the correspondence range to deal with the interaction between huge quantities of individual mobile nodes by framing a correspondence system and trading the information among them without using any described group of the base station. A trust-based model in MANET estimates and sets up trust relationship among objectives. Trust-based routing is utilized to keep away data from different attackers like a wormhole, DOS, black-hole, selfish attack and so forth. Trust can be executed in different steps like reputation, subjective rationale and from the supposition of the neighboring node. A trust estimation approach not just watches the behavior of neighbor nodes, additionally it screens the transmission of the information packet in the identification of the route for exact estimation of trust value. A survey is carried out to find some of the limitations behind the existing works which has been done by the researchers to implement various approaches thus to build the trust management framework. Through the survey, it is observed that existing works focused only on the authenticated transmission of the message, how it transmits packets to the destination node securely using a trust-based scheme. And also, it is observed that the routing approach only focused on the key management issues. Certain limitation observed in the implemented approaches of existing work loses the reliability of framework. Thus, to withstand these issues it is necessary to establish a reliable security framework that protects the information exchanged among the users in a network while detecting various misbehaving attacks among the users. Confidentiality, as well as the integrity of information, can be secured by combining context-aware access control with trust management. The performance parameters should be evaluated with the previous works packet delivery ratio, packet drop, detection accuracy, number of false positives, and overhead.

KEYWORDS

Attacks, Context-Aware Access Control, Framework, Mobile Ad Hoc Network

DOI: 10.4018/IJBDCN.2019070103

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
1. INTRODUCTION

PC frameworks were at first made to work by interfacing PCs together with wires and transmitting data over these wires. Framework sizes and occasions extended making a need for system interactions. This headed to the change of the internet and its suite of traditions. The use of the internet and its applications got the opportunity to be inescapable. A prerequisite in terms of network access to entities while not physically joined to the wired framework recently emerged.

Figure 1 demonstrates the framework model of the MANET. The different modules in the framework model are as per the following.

Module 1 - Sender module (Source node): The objective of this module is to capture the message and afterward partition the message into packets of 48 bytes long, send the packets to the final node with the help of intermediate node and get feedback from the receiver node through the intermediate node.

Module 2 - Intermediate module (Intermediate node): The objective of this module is to get a packet from the sender, modify/don’t vary the message and send it to the destination node. Get 2ACK packet from the recipient and send 2ACK packet to the sender.

Module 3 - Receiver module (Destination node): The objective of this module is to get a message from the intermediate node, take out final destination node name and hashcode and decrypted it. Analyze the hash code of the source node and destination node for security reason. Send 2ACK to source node with the help of intermediate node.

To enable this wireless systems administration, traditional devices with techniques are used to coordinate with a wired framework, using radio wave progressions through the wireless access point. At the same time, telephone frameworks were encountering a relative change. Cell framework efficiency was delivered to allow cell phones to interface in terms of base stations and confer in a circuit traded environment. Late advancements of remote innovations like Bluetooth, IEEE 802.11 displayed another sort of remote framework known as Mobile Ad-hoc networks. The region of mobile ad-hoc networking manages devices to perform wireless correspondence and systems administration (Marchang & Datta, 2012), which work without a central access point.

2. MANETS

2.1. Security Criteria in MANET

As of now said the mobile ad-hoc systems are defenseless against security issues than the wired systems, in this segment different vulnerabilities are investigated:
Green Characteristics of RFID Technologies: An Exploration in the UK Logistics Sector from Innovation Diffusion Perspective
[www.igi-global.com/chapter/green-characteristics-of-rfid-technologies/115142?camid=4v1a](www.igi-global.com/chapter/green-characteristics-of-rfid-technologies/115142?camid=4v1a)

Dual-Hop and Multi-Hop Cooperative Spectrum Sensing with an Improved Energy Detector and Multiple Antennae-Based Secondary Users