International Journal of Information Security and Privacy
Volume 14 • Issue 1 • January-March 2020

Manifold Surveillance Issues in Wireless Network and the Secured Protocol

Mamata Rath, Birla School of Management (IT), Birla Global University, Odisha, India

Bibudhendu Pati, Department of Computer Science, Rama Devi Women's University, Bhubaneswar, India

Binod Kumar Pattanayak, Department of Computer Science and Engineering, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India

ABSTRACT

With rapid growth of internet users and frequently emerging communication technology, the issues of using web as a worldwide platform and the requirement to design the smart applications to coordinate, discuss, register, and outline gradually emerges. Information transmission through a wireless network involves the radio signals, the arrangement of information packets, and the network topology. As each segment is correlated to each other, it is very essential to employ security mechanism in these components and real security control must be connected on them. Thus, security plays a critical factor in wireless network. This article highlights security issues in current wireless networks such as mobile ad-hoc network and IoT-supported networks and it also proposes a security-based S-RAID protocol design for security control in cluster based wireless networks. Simulation results show proficiency and better transmission rate of the proposal when it was compared with other similar approaches.

KEYWORDS

authenticity mobile agent, Network security, secured protocol, wireless network

1.INTRODUCTION

As wireless network is a centre innovation developed in new age, the essential security challenges incorporate consistent communication with unwavering quality in the network. In a wireless network with no foundation where there is no base station and access point, the possibility of defenselessness is more. The cell phones are allowed to move toward any path as yet keeping up network with other portable hubs. Because of this exceptional nature of wireless network, outline of wireless network convention with high security includes in particularly basic. Again, because of dynamic change in topology, the network change happens powerfully thus the network is decentralized and more defenseless than wired based network in numerous angles.

In a special wireless networks like WSN and Mobile Ad-hoc Network (MANET), electronic devices and gadgets such as tablets, PCs, mobile phones, machines with specially appointed correspondence capacity are connected together to make a system. MANET is a self-organizing structure of flexible switches related hosts associated by secluded connections. The routers move randomly and compose themselves accordingly; along these lines, the systems remote topology may change quickly and capriciously. In these type of network each node acts as router and because of dynamic changing topology the accessibility of hubs is not generally ensured. It likewise does not ensure that the way between any two hubs would be free of pernicious hubs. The remote connection between hubs is exceptionally vulnerable to connection assaults such as passive eavesdropping, active

DOI: 10.4018/IJISP.2020010102

interfering, etc.Due to inflexibility in the infrastructure of it affects the security feature whenever any kind of extreme computation is done to perform encryption. So due to this problem it is important to build a secured connection which can provide high security solution to provide secured services like authentication, confidentiality, integrity, non-repudiation and availability. So here security is provided in each and every layer

Wireless networks have all around refreshing as of late because of its incredible highlights, for example, self configurable work stations called hubs and they themselves can do their own upkeep . There are many open security issues in wireless network, for example, its open design of network, its common medium, the issue of asset limitations, and alterable network topology. In the network layer of the network different attacks happens amid directing of the data packets from one station to other. There are some special attack types in which routing tables are changed, however, most of the attacks takes place on smart devices because there is very few security policy employed to protect them. Wireless networks have got well appreciated in recent years due to its fantastic features such as self configurable work stations called nodes and they themselves can do their own maintenance . There are many open security issues in wireless network such as its open architecture of network, its shared medium, the problem of resource constraints, and changeable network topology and real time applications[26].In the network layer of the network model various attacks takes place during routing of the packets from one mobile device to other. There are some forwarding attacks which leave the routing tables alone, but changes the delivery of packets. Due to any weakness of the design of the underlying protocol, many attacks happen as a result of which there is denial of service to authenticated devices and many other type of problems take place.

Basic motivation of our work is that we found various types of attacks in wireless transmission and then we proposed a security mechanism to prevent the wireless transmission from vulnerability and attacks. The article has been organised as follows. Section 2 describes Related work section. Section 3 describes security threats in wireless network. Section 4 describes mobile agent as a means of prevention of attack. Section 5 describes the proposed security protocol S-RAID. Section 6 describes comparative analysis and simulation results and at last section 7 concludes the paper.

2. RELATED WORK

Comprehensive revise and a short re-evaluate has been conducted at this part of the article to understand various contributions made by eminent researchers in this field. Transmission of audio data with secured mechanism has been discussed in Athulya and Sheeba (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 Mulert, Weich, and Seah (2012) and it also focuses on how modification of data is done using optimization technique for security. 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 et al. (2012). The author proposed a model i.e. PBM (Policy Based Management) that deals with 4 entities in Slavica et al. (2014) 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, 2015). A secured on-demand routing protocol has been proposed in Wan, Ren, and Gu (2012) that prevents various attacks in MANET and another regression based trust model for MANET has been implemented in Venkataraman, Pushpalatha and Rao (20102) that ensures guaranteed packet delivery in wireless medium. Marchang and Datta (2012) proposed a light weight trust based routing protocol that prevents any external attacks in MANET and a mobile agent based secured platform has been designed by Rath and Pattanayak (2017) that ensures improved network life time with better throughput when compared with other similar approaches.