Load Balancing Aware Multiparty Secure Group Communication for Online Services in Wireless Mesh Networks

Neeraj Kumar, Neeraj Kumar, CSED, Thapar University, Patiala (Punjab), India

ABSTRACT

The internet offers services for users which can be accessed in a collaborative shared manner. Users control these services, such as online gaming and social networking sites, with handheld devices. Wireless mesh networks (WMNs) are an emerging technology that can provide these services in an efficient manner. Because services are used by many users simultaneously, security is a paramount concern. Although many security solutions exist, they are not sufficient. None have considered the concept of load balancing with secure communication for online services. In this paper, a load aware multiparty secure group communication for online services in WMNs is proposed. During the registration process of a new client in the network, the Load Balancing Index (LBI) is checked by the router before issuing a certificate/key. The certificate is issued only if the value of LBI is less than a predefined threshold. The authors evaluate the proposed solution against the existing schemes with respect to metrics like storage and computation overhead, packet delivery fraction (PDF), and throughput. The results show that the proposed scheme is better with respect to these metrics.

Keywords: Group Communication, Key Management, Load Balancing, Multiparty, Wireless Mesh Networks (WMNs)

1. INTRODUCTION

Over the years, wireless mesh network (WMN) has gained lot of attention due to unique features such as multihop nature, easily scalable and maintainable with low network cost applicable to wide range of applications, and self healing and self configurable nature (Akyildiz, Wang, & Wang, 2005). A generalized architecture of the WMN consists of mesh gateways (MG), mesh routers (MRs) and mesh clients (MCs). Every node in WMNs may acts as a router, forwards the packet to other nodes. Some of these routers may act as gateways which are directly connected to internet (1). A WMN combines the fixed network (backbone) and mobile network (backhaul). Every node in WMNs can act as a router and is able to forward the packet to other nodes. A node which didn’t have access to the backbone network can establish a connection by routing the packets from a neighbouring node that has a backbone network connection.
MCs in WMNs connect to the internet using gateways which act as a relay nodes as shown in Figure 1.

There are number of applications where WMN can be used such as video on demand, Voice over IP (VoIP), online single/multiple player/players multimedia games etc. Because users accessing the different services are located in different domains, security is a major concern for all these service provided by the underlying network. Only the legitimate users are allowed to access the available resources over the network, i.e., before performing any operation in the network these users must use the key provided by the trusted party for a particular duration. The key to these users is given for a particular time interval and may be renewed for the next duration by trusted party so that only the authenticated person can use the available services of the network. Because most of the traffic flows from mesh routers (MRs) to mesh clients (MCs), so key is kept at MRs for the duration of communication between MRs and MCs. Broadly, there are two types of attacks boundaries namely as outside and inside within which an attacker can access the network resources. The attacker from outside the boundary can destroy the MRs or MCs while within the inside boundary it can access the messages that are not meant for it (2).

Although security in wireless networks has been investigated by various researchers from different prospective such as data confidentiality, integrity, trust management etc.. The existing solutions for the security are divided into two folds namely as for centralized and distributed scenarios. In case of centralized scenario, standard encryption/decryption mechanisms are applied but these techniques have single point of failure (Han, Gui, Wu, & Yang, 2011; Rafaeli & Hutchison, 2003). The distributed approaches divide the group of users into several subgroups with each group uses a separate shared key for communication or multicasting the message (Han, Gui, Wu, & Yang, 2011; Han & Gui, 2009; Wu, Mu, Susilo, & Qin, 2009). Han, Gui, Wu, and Yang (2011) have used the proxy based secure multicast group communication mechanism. Both centralized and distributed strategies have their advantages and disadvantages. As the MCs are distributed in different regions which are controlled by the respective mesh points,
Information Theoretic Approach with Reduced Paging Cost in Wireless Networks for Remote Healthcare Systems


Security Across Disparate Management Domains in Coalition MANETs
[www.igi-global.com/chapter/security-across-disparate-management-domains/58853?camid=4v1a](www.igi-global.com/chapter/security-across-disparate-management-domains/58853?camid=4v1a)