Cross-Layered Secure and QoS Aware Design of VOIP over Wireless Ad-Hoc Networks

Shahin Vakilinia, Concordia University, Montréal, Canada
Mohammadhossein Alvandi, Concordia University, Montréal, Canada
Mohammadreza Khalili Shoja, AmirKabir University, Tehran, Iran
Iman Vakilinia, AmirKabir University, Tehran, Iran

ABSTRACT

In this paper, cross-layer design has been used to provide quality of service (QoS) and security at the same time for VOIP over the wireless ad-hoc network. In this paper the authors extend their previous work (i.e. Multi-path Multi-Channel Protocol Design for Secure QoS-Aware VOIP in Wireless Ad-Hoc Networks) by adding transport and application layers considerations. The goal of this paper is to support QoS and security of VOIP simultaneously. Simulation results shows that the proposed cross-layered protocol stack design significantly improve QoS parameters of the VOIP calls under the jamming or Denial-of-service attacks.

Keywords: Ad-Hoc Networks, Attacks, Quality of Service (QoS), Security, Voice Over Internet Protocol (VOIP)

INTRODUCTION

Wireless Ad-Hoc networks consist of a collection of nodes which are capable of communicating with each other without requiring a fixed infrastructure. In addition, in the case of mobile nodes, the interconnection between nodes can change continuously. Such a network is generally called a mobile Ad-Hoc network (MANET). Nodes within transmission range of each other communicate directly, and nodes which are far apart use other nodes in order to transmit their data through multiple hops.

Since our goal in this paper is to address QoS and security issues in mobile Ad-Hoc networks, we will choose various layer architectures based on QoS and security criteria and then focus on a cross-layer design to improve such performance. With such views in mind, at the MAC layer, we will focus on Multi-Channel MAC schemes that provide better performance in fading and jamming scenarios (Bahl et al.,

DOI: 10.4018/ijbdcn.2013100102
Among QoS-aware routing schemes (Marina & Das, 2001), INSIGNIA (Lee et al., 2000; Mohapatra et al., 2003), ASAP (Xue et al., 2003) and INORA (Dharmaraju et al., 2002), Multipath routing algorithms targeted at providing QoS will be considered as a basis. A good architecture for QoS-aware Ad-Hoc networks is proposed in (Chen & Heinzelman, 2004). Our architecture is similar to the approach proposed by Chen and Heinzelman while we try to enhance their approach by taking cross-layer issues into account and also improving the performance of protocols at each layer in all of the mentioned algorithms.

On the other hand, in order to provide security we have to secure our layers against attacks. In (Xu et al., 2005) detecting ways of jamming attacks of wireless Ad-Hoc networks were introduced and some good methods for defense against jamming attacks were explained in (Xu et al., 2004; Xu, 2007). In (IEEE Std 802.11i) one of the most effective common authentication methods, extensive authentication protocol (EAP) was described and (Alghathbar & Mahmoud, 2009) tried to expand 802.11 EAP suitable and more secure and non detectable for the wireless Systems. (Stamouli, 2003; Zhang & Lee, 2000) introduce some intrusion detection systems on the physical and MAC layers.

Routing attacks are being introduced in (Ayirci & Rong, 2009; Goyal et al., 2010; Kannhavong et al., 2007; Noubir & Lin, 2003). Some secure Ad-Hoc routing protocols have also been proposed in (Hu et al., 2002; Hu et al., 2005; Desilva & Boppana, 2005). SAODV is very well-known and resistant against a lot of attacks such as black hole and worm-hole attacks (Hu et al., 2005). However, it does not include problems such as sniffing in the network layer and end-to-end authentication. None of these papers has considered QoS issues. In other words, they do not consider the effect of making the networks secure on the QoS parameters of the wireless Ad-Hoc network.

Because of our focus to have the secure QoS-aware voice calls over the Ad-Hoc network, we have to consider both security and QoS and the interactions between them. In fact, main issue of this paper is based on considering QoS and security problems simultaneously. Our proposed QoS-aware algorithms support network QoS parameters with existence of security algorithms.

The organization of this paper is as follows. Physical Layer used briefly described in the following. After that Dedicated Control-Channel MAC approach is explained and equations for calculating QoS parameters and investigating the security issues of MAC layer such as jamming resistance and authentication are presented. Then, algorithms for improving network QoS parameters are proposed. We also suggest some multipath routing algorithms for reducing the effects of nodes mobility, we propose security algorithms in routing to make the Ad-Hoc network secure in the routing process and from the sniffing point. Finally, simulation results are presented, and the last section concludes the paper.

PHYSICAL LAYER

One of the most important characteristics of Ad-hoc networks is dynamic nature of its topology due to mobility of nodes affecting its transmission model. For example, Doppler Frequency \( f_D \) caused by movement of a node is given by \( \frac{v}{\lambda} \), where \( v \) represents node velocity and \( \lambda \) shows transmission wavelength. In our model, we assume the slow-fading scenario in which signal bandwidth is much larger than Doppler frequency of the channel \( (BW >> f_D) \). Given the wide transmission bandwidth and low power transmission criteria Direct-Sequence spread spectrum (DSSS) modulation with Rake receiver structure is chosen at the physical layer. Our first step to secure 802.11 is to make it non-detectable, so we increase the length of the 802.11b DSSS chip rate from 11 chips to 11.x chips where \( x \) is a simple constant for increasing the chip sequence while decreasing the transmission rate from \( C \) Mbps to \( C/x \) Mbps. As a result, our
Related Content

Modeling and Simulation of Traffic with Integrated Services at Media Getaway Nodes in Next Generation Networks
[www.irma-international.org/article/modeling-simulation-traffic-integrated-services/58651/](www.irma-international.org/article/modeling-simulation-traffic-integrated-services/58651/)

Agent Based Product Negotiation Models in Mobile Commerce
[www.irma-international.org/chapter/agent-based-product-negotiation-models/21705/](www.irma-international.org/chapter/agent-based-product-negotiation-models/21705/)

Designing an IP Link Topology for a Metro Area Backbone Network
[www.irma-international.org/article/designing-link-topology-metro-area/76941/](www.irma-international.org/article/designing-link-topology-metro-area/76941/)

Competition, Regulation and Broadband Diffusion in New Zealand
[www.irma-international.org/chapter/competition-regulation-broadband-diffusion-new/20437/](www.irma-international.org/chapter/competition-regulation-broadband-diffusion-new/20437/)

RFID Technology and Privacy
[www.irma-international.org/chapter/rfid-technology-and-privacy/115141/](www.irma-international.org/chapter/rfid-technology-and-privacy/115141/)