Journal of King Saud University – Computer and Information Sciences (2017) **29**, 246–268

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

Quantitative analysis of the security performance in wireless LANs

Poonam Jindal *, **Brahmjit Singh**

National Institute of Technology, Faculty of Electronics and Communication Engineering Department, Deemed University, Kurukshetra 136118, India

Received 2 August 2014; revised 3 November 2014; accepted 9 December 2014
Available online 2 November 2015

KEYWORDS

Frame loss;
Roaming network;
Security protocols;
Throughput;
TCP;
UDP

Abstract A comprehensive experimental study to analyze the security performance of a WLAN based on IEEE 802.11 b/g/n standards in various network scenarios is presented in this paper. By setting-up an experimental testbed we have measured results for a layered security model in terms of throughput, response time, encryption overheads, frame loss and jitter. Through numerical results obtained from the testbed, we have presented quantitative as well as realistic findings for both security mechanisms and network performance. It establishes the fact that there is always a tradeoff between the security strength and the associated network performance. It is observed that the non-roaming network always performs better than the roaming network under all network scenarios. To analyze the benefits offered by a particular security protocol a relative security strength index model is demonstrated. Further we have presented the statistical analysis of our experimental data. We found that different security protocols have different robustness against mobility. By choosing the robust security protocol, network performance can be improved. The presented analysis is significant and useful with reference to the assessment of the suitability of security protocols for given real time application.

1. Introduction

There has been tremendous growth of wireless communication services over the last decade due to their ease of accessibility, mobility and flexibility. Due to the release of the restrictions of physical boundaries, Wireless Local Area Networks (WLANs) have been extensively deployed worldwide (Ergen, 2002). The universality of these networks ranges from homes, business, online banking, social networking, cafes, military, and research sectors to many more. Due to open access of the shared wireless medium, existing studies reveal that WLANs are susceptible to several attacks such as sniffing, spoofing, eavesdropping, denial of service and man in the middle attack; hence provisioning of the security in these networks is a major research challenge (Sheldon et al., 2012). Such security issues raise the need of applying strong security mechanisms to protect the information over the network. Consequently, several

* Corresponding author.
E-mail addresses: poonamjindal81@yahoo.co.in, poonamjindal81@nitkkr.ac.in (P. Jindal), brahmjit.s@gmail.com (B. Singh).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.12.012
1319-1578 © 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

security protocols and mechanisms are being developed to enhance the security in WLANs (Feng, 2012).

The implementation of security protocols induce additional cryptographic overheads and further the cumulative effect of the cryptographic overheads with basic impairments of wireless network results in a severe obstruction in attaining adequate quality of service (QoS) (Potlapally et al., 2006; Jindal and Singh, 2013). Although it is certain that security mechanisms affect the performance of the network in terms of the resultant throughput, packet loss, response time, jitter, encryption cost, and authentication time (Baghaei et al., 2004; Turab and Moldoveanu, 2008; Boulmalf et al., 2007). Investigations have not been reported anywhere in much detail as to what extent network performance is affected by security protocols in both roaming and non-roaming scenarios with different applications. Therefore, it is imperative to analyze quantitatively the impact of security protocols on the performance of networks and to study how the QoS degrades in real time networks with the application of security protocols. As security is a constituent of wireless LAN, good comprehension of its implications on WLAN performance is necessary.

To achieve a secure wireless communication different security protocols are developed at different network layers. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2 at MAC layer, IPsec (IP security), SSL (Secure Socket Layer), and RADIUS (Remote access Dial in User Service) exist at the network layer, transport layer and application layer respectively and are the various security protocols to prevent the network from malicious attacks (Vibhuti, 2008; Lashkari et al., 2009). Most of the previous research has concentrated on the enhancement of cryptographic mechanisms in security protocols, though they are not quantifying the associated performance degradation due to security protocols in much detail (Peteriya, 2012; Mitchell, 2005).

To achieve the above goal we have developed a real time experimental testbed and performed the comprehensive experimental analysis to investigate the performance impact of nine different security protocols including the enterprise security layers. The used testbed is a miniature of existing wireless networks and ensures the consistency of our experimental scenarios with typical deployment of WLANs. We are using the experimental testbed because testbed results not only give naturalistic results, but also explore various issues such as communication in roaming environment and processing delays in wireless devices that cannot be flawlessly formed in simulation and analytical models. In this work, we report on the comparative analysis of the performance impact of different security protocols (SSID, WEP/64/128, WPA/AES, WPA2/AES, and WPA2/AES/TKIP at MAC layer) including security layers with RADIUS server (WPA/AES, WPA2/AES, and WPA2/AES/TKIP at application layer). We have used our testbed with mobile IP for roaming network. We have made this testbed a heterogeneous network with the help of various hardware and mobile devices. Comprehensive experimental analysis is carried out in this paper to investigate the performance impact of nine different security policies including the enterprise security policies in roaming and non-roaming environment. Our obtained experimental results perceive that based upon the network scenario and traffic type, security is always achieved at the cost of network performance. It is observed that very high security protocols are not always a good choice for all network scenarios and also it is found that the stronger the security protocol, the more are the associated overheads. Our study aims to address the following issues:

- Impact of different security mechanisms on the performance of wireless LAN (IEEE 802.11b/g/n).
- Impact of congested and uncongested network on the performance of secure WLAN.
- Impact of different packet lengths on the performance of secure WLAN.
- Network performance under TCP and UDP traffic streams.
- Security performance in non-roaming and roaming scenarios.

Furthermore, security strength of various protocols is analyzed using a relative security strength index model (RSSI) (Luo et al., 2009). It is always presumed that the more the number of security mechanisms or security services provided by any protocol, more is the protocol strength. On evaluating the security strength using RSSI it is observed that the stronger the security service provided by security algorithm the stronger will be the security protocol. A detailed view of the benefits offered by a particular security protocol is provided by the RSSI model that helps the system designers to choose a security protocol with the desired strength. The security performance observed through experimental analysis validates our results obtained from the RSSI model. Further a descriptive statistical analysis is performed to analyze the robustness related with each security protocol. It is revealed that each security protocol varies in robustness against mobility. Analysis of variance is performed and it is found that all the network scenarios and performance metrics taken under consideration are significant. All the factors (security protocols, traffic type, and network load) affect the performance of wireless networks. Our experimental results provide a wide quantitative vision of the impact of various security protocols on network performance. Including this, our analysis is useful in understanding the applicability of security protocols in real time applications and design challenges of future security protocols.

The remainder of the paper is organized as follows. Existing studies are discussed in Section 2. A brief summary of WLAN standard and WLAN security protocols is described in Sections 3 and 4 respectively. Section 5 details the experimental testbed along with different security layers and the system modeling considered in the testbed. A RSSI model is presented in Section 6. Performance metrics under consideration is discussed in Section 7. Numerical results for different security layers in different network environments are explained in Section 8. Statistical analysis is done in Section 9. Conclusion is drawn in Section 10.

2. Related work

To determine the realistic view of the performance impact of security mechanisms, measurements play an important role. Therefore to gain the fundamental understanding of the impact of various security mechanisms on the network performance, a number of research papers have appeared in the literature reporting the security performance of IEEE 802.11b/g based wireless local area networks. In (Baghaei et al., 2004) authors have performed throughput and response time analysis for IEEE 802.11b wireless LAN in a non-roaming environment. It was found that the stronger the security mechanism