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.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.12.012

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

the more is the performance degradation. An experimental study to analyze the performance overheads associated by different security protocols was done by authors in (Nayak et al., 2005; Agarwal and Wang, 2007) for IEEE 802.11b/g based network. Further in (Begh et al., 2009; Ahmad et al., 2012), impact of security protocols on the performance of TCP and UDP traffic streams has been analyzed and was found that security protocols negatively affect the network performance. A more detailed analysis to study the security performance on IEEE 802.11g based wireless network by integrating cross layer security protocols was demonstrated in (Agarwal and Wang, 2007). Another experiment was performed in (Vibhuti, 2008) to calculate the security impact on end-to-end delay and packet delivery fractions. The impact of cryptographic primitives used in WEP and WPA on throughput and delay over WLAN IEEE 802.11g was investigated in (Boulmalf et al., 2007). The performance impact of secure IEEE 802.11g WLAN using Open VPN is done in (Likhar and Yadav, 2011). Experiments were performed on a wireless test-bed to analyze throughput, delay and jitter for four security settings: disabled security, WEP, WPA1, and WAP2 for multimedia applications in (Hayajneh et al., 2012). WPA2 security-bandwidth trade-off in 802.11n WLAN for IPv4 and IPv6 using different operating systems is studied in (Kolahi et al., 2012). Impact of transmission power on the performance of secure IEEE 802.11n wireless local area network was reported in (Singh and Jindal, 2014a,b). The available literature revealed that a number of researchers have carried out numerous experiments to quantify the security performance but with several limitations. Firstly the past researches have focused on the improvement of cryptographic aspects of security mechanisms in a small range of network scenarios (Begh et al., 2009). Secondly the previous work brings out the qualitative analysis and does not provide the complete quantitative results in terms of QoS and encryption cost (Hayajneh et al., 2012; Ahmad et al., 2012). The literature survey reveals that most of the research has focused on qualitative security performance of IEEE 802.11b and IEEE 802.11g standards but not considering IEEE 802.11n (Likhar and Yadav, 2011). Also the impact of different implementations of enterprise security layers on the performance of wireless LAN has not been taken much into consideration in the previous work. The past research was carried out to explore the pros and cons of individual security protocols, but security protocols exist at different network layers (Nayak et al., 2005; Begh et al., 2009; Hayajneh et al., 2012; Ahmad et al., 2012; Likhar and Yadav, 2011; Bhatia et al., 2013; Agarwal and Wang, 2007). It is certain and instinctive to study the effects of security protocols in a cross layer architecture. We aim to provide comparative experimental analysis to study the impact of security mechanisms on the performance of IEEE 802.11b/g/n standard in a variety of network scenarios at different packet lengths.

3. IEEE 802.11 WLAN standards

WLANs based on IEEE 802.11 standard have been extensively deployed worldwide for information access through wireless medium. However, the communication being in broadcast mode is highly vulnerable to security threats. It is therefore of utmost importance to analyze the security performance of wireless networks based on different versions of the IEEE 802.11 standard. In this section, we briefly introduce different IEEE 802.11 standards.

Institute of Electrical and Electronics Engineers (IEEE) has developed 802.11 and 802.11x, referred to as a group of standards/specifications for WLANs (Bhoyar et al., 2013). The standard IEEE 802.11 specifies an over-the-air interface between a wireless client and an access point or between two or more wireless clients. These WLAN standards were developed with the focus of increasing transmission speeds, range, improving QoS, and adding new amendments. All the amendments made in the specifications define the maximum speed of operation, the radio frequency band of operation, encoding of the data for transmission, and the characteristics of the transmitter and receiver. A number of versions of the standards have been developed including, IEEE 802.11a, IEEE 802.11b, IEEE 802.11e, IEEE 802.11f IEEE 802.11g, IEEE 802.11h, IEEE 802.11i, IEEE 802.11j, IEEE 802.11k, IEEE 802.11n, IEEE 802.11s, IEEE 802.11ac, IEEE 802.11ad and IEEE 802.11f. However, the most widely used standards are 802.11b, 802.11g, and 802.11n and 802.11i (security protocol). These network bearer standards operate in ISM (Industrial, Scientific and Medical) frequency bands. The band being license-exempt makes it economical and easy to deploy technology for common use. The respective features of these standards are shown in Table 1.

4. WLAN security protocols

To protect the wireless network from illegitimate users and to achieve data confidentiality, integrity and authentication, various WLAN security protocols were developed (Liu et al., 2010). The most popularly adopted security protocols are:

Wired Equivalent Privacy (WEP): WEP was the first security protocol developed to obtain security equivalent to the wired network. It provides data privacy using RC4 encryption

Table 1 WLAN standards.

Standards	Features				
	Publishing year	Data rate (Mbps)	Operating frequency (GHz)	Modulation used	Compatibility
IEEE 802.11b	1999	5.5–11	2.4	Complementary code keying (CCK), Direct sequence spread spectrum (DSSS)	Backward compatible with IEEE 802.11a
IEEE 802.11g	2003	54	2.4	Orthogonal frequency division multiplexing (OFDM)	Backward compatible with IEEE 802.11b
IEEE 802.11n	2009	600	2.4 and 5	(CCK, OFDM or DSSS Additional feature of MIMO)	Backward compatible with IEEE 802.11b/g

with 64/128 bit key, initialization vector and integrity check value (ICV) and provide confidentiality, simple integrity and shared key authentication. The weak implementation of RC4 and the proliferation of readily available hacking tools led to WEP being insecure and also not popular for enterprise wide distributed processing environments.

Wi-Fi Protected Access (WPA) is a security protocol that removes almost all the vulnerabilities of WEP. It is also known as WPA personal. WPA uses RC4 encryption along with temporal key integrity protocol (TKIP) which includes message integrity check, initialization vector (IV), key mixing and key management algorithms. Since security mechanisms associated with WPA are more, hence it provides confidentiality and authentication (based on 802.1x and EAP) with enhanced strength as compared to WEP. WPA is intended to work with existing 802.11-based products and offers forward compatibility with 802.11i (security standard).

WPA2 is an enhanced version of WPA where AES is used as an encryption algorithm. It is also known as WPA2 personal. Like WPA, WPA2 use 802.1x based authentication. It also includes a Robust Security Network Association (RSNA). RSNA provides two protocols TKIP and AES-CCMP (Counter Mode CBC MAC protocol) for data confidentiality. WPA2 uses key lengths of 128,192, 256 along with dynamic key distribution. Altogether these protocols deliver improved confidentiality, data integrity and authentication as compared to WPA.

5. Experimental testbed

In order to study the impact of different security layers on the performance of WLAN in different network scenarios, an experimental testbed is developed in a roaming and non-roaming environment while considering the users mobility. In this section hardware and software configuration of the experimental testbed, which is miniature of WLAN is illustrated. Although we have shown a simple WLAN architecture; with the use of different hardware and software configurations, a heterogeneous environment can be created that captures the mobile aspects of WLANs. The existing testbed offers itself to be mapped to large scale wireless networks. We have also performed a comparative analysis of the performance in non-roaming and roaming WLAN scenarios. The two network scenarios and the corresponding hardware and software configurations, security protocols used in the setup are as discussed below:

5.1. Non-roaming network scenario (NR)

Non-roaming network scenario, represented as *NRS*, deals with the situation when mobile node (MN) (a wireless node) is communicating with its home agent (HA) (a server who is giving services to client) in the network and the communication path is wireless. This scenario aims to study the impact of security layers only in one domain when nodes are communicating over a secure network. Experimental architecture and used hardware and software configurations for non-roaming network are shown in Fig. 1 and Table 2 respectively.

5.2. Roaming network scenario (RS)

The roaming scenario, represented as *RS* deals with the situation when any of the communication mobile users is in a foreign domain. In our testbed we have taken roaming scenario as, a client (A) from its home network is moving in the foreign network and gets connected with AP in the foreign network and is communicating with HA which is an application server (A) in the home network. Experimental architecture and used hardware and software configurations for non-roaming network are shown in Fig. 2 and Table 3 respectively.

Table 2 Network configurations in a non-roaming network scenario.

Network configuration in non-roaming network scenario	
Hardware configuration	- A server (Window server 2008 with 3.20 GHz processor, 4 GB RAM was used as a RADIUS server) - A client (Windows 7 professional, I3 second generation processor, 3.2 GHz, 4 MB of RAM) - An access point (Cisco WAP4140n) - RJ45 Ethernet cable for wired connectivity - The experiments were based on windows 7 (both clients and server) as it has built in implementation of 802.1x authentication protocol
Software configuration	- *The Ethereal* is a packet analyzer and is used to capture live network statistics and measurements were obtained from the server (Ethereal, http://www.ethereal.com/) - *IP Traffic Generator* is windows based software testing tool designed for both fixed and wireless networks that can run on any system with windows 98, 2000 or XP window 7. It can generate, receive, capture, replay IP traffic, measure end-to-end performance and quality of service over any fixed or mobile network. (IP traffic, www.zti-telecom.com/) - *RADIUS* server functionality is provided by FreeRadius and is installed on all machines (RADIUS, http://www.freeradius.org)

Figure 1 Experimental test-bed design for non-roaming wireless LAN.

5.3. Security policies

Experiments are performed on a layered security model. Performance analysis with nine security layers is carried out. First six security layers are; SSID (no security layer), WEP/64 (WEP used with 64 bit key), WEP/128 (WEP used with 128 bit key), WPA/AES (WPA used with Advanced Encryption Standard algorithm), WPA2/AES (WPA2 used with AES encryption algorithm), WPA2/AES/TKIP (WPA2 mixed with both AES and TKIP). These are MAC layer security protocols and provide confidentiality, integrity and authentication and are consistent with IEEE 802.11 standard (Holt and Huang, 2010). Security layers from 7 to 9 are enterprise security layers; WPA/AES Enterprise, WPA2/AES Enterprise, WPA2/AES/TKIP Enterprise (in all the cases authentication is performed using RADIUS server) and exist at the application layer, which make use of the RADIUS (Remote Authentication Dial in User Service) server. It provides advanced authentication through digital signatures and provides more security as compared to layer 1-6. Table 4 shows the security protocols and their associated security services. We have studied these nine security protocols because of their prevalent use in many networks for security provisioning.

5.4. System modeling

To carry out experimental analysis we have selected different system parameters. Table 5 presents the system parameters selected for system modeling during the experiments.

Table 3 Network configuration in a roaming network scenario.

Network configuration used in roaming network scenario	
Hardware configuration	- A mobile node is a wireless node, which is able to change its position - The test bed is placed in two subnets including four laptops (HP laptops (dual 2 core processor 2.4 GHz), HCl laptops (dual 2 core processor 2.4 GHz), HCl laptop with i3 processor 2.4 GHZ) - Two access points (Cisco WAP4140n) to configure a traditional client/server architecture in a wireless connection - A switch (D-Link) to provide connectivity between subnets - RJ-45 cable for connectivity between switch, access points and a server - Two laptops with one configured as a server (Home Agent (HA)) and the other as a client (A) in a home network. Third laptop configured as a server station (Foreign Agent (FA)) and the fourth as a client (B) in a foreign network
Software configuration	Software installed in the server and client machines used in roaming scenarios are similar to the one used in non-roaming network scenarios

6. Relative security strength index (RSSI)

To analyze the security strength offered by various security protocols is known to be one of the most challenging issues. A simple measurement for the analysis of security strength referred to as relative security strength index is presented in this section. All the security protocols including WEP, WPA, WPA2, make use of different encryption and authentication mechanisms and offer security services, like confidentiality, integrity, access control, authentication, mutual authentication

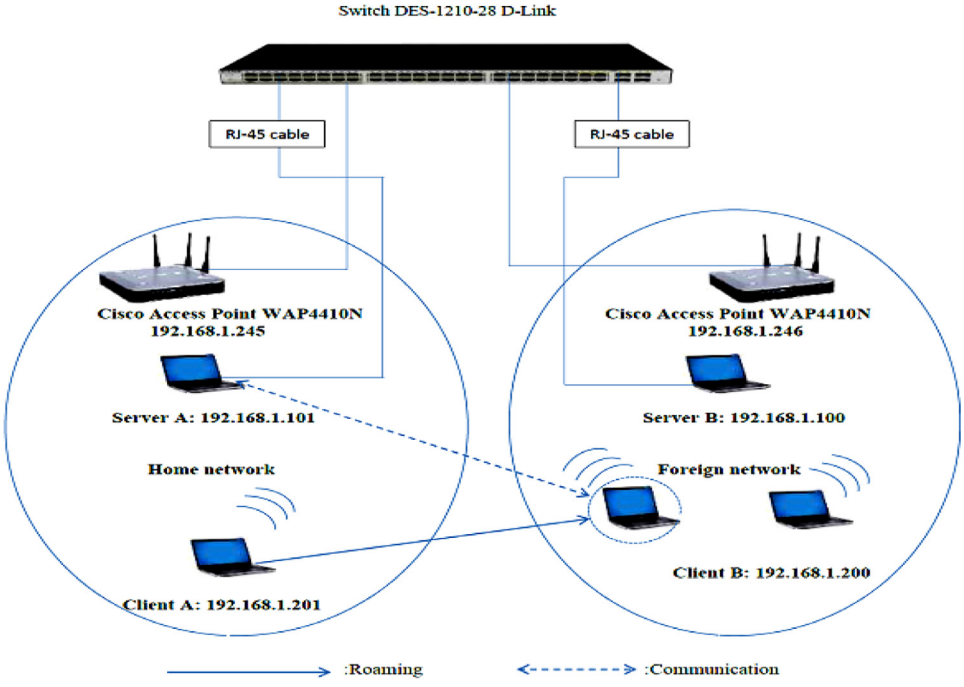

Figure 2 Experimental test-bed design for roaming wireless LAN.

Table 4 Security protocols implemented on the testbed.

Security protocols		Confidentiality	Authentication	Integrity	Mutual authentication	Non-repudiation
P_1	SSID	–	–	–	–	–
P_2	WEP/64	✓	✓	✓	–	–
P_3	WEP/128	✓	✓	✓	–	–
P_4	WPA/AES	✓	✓	✓	✓	–
P_5	WPA2/AES	✓	✓	✓	✓	–
P_6	WPA2/AES/TKIP	✓	✓	✓	✓	–
P_7	WPA/AES/RADIUS	✓	✓	✓	✓	✓
P_8	WPA2/AES/RADIUS	✓	✓	✓	✓	✓
P_9	WPA2/AES/TKIP/RADIUS	✓	✓	✓	✓	✓

Table 5 Security protocols implemented on the testbed.

System parameters	
Bandwidth	For IEEE 802.11b/g/n the nominal bandwidths are 11 Mbps/54 Mbps/72 Mbps respectively For IEEE 802.11b, 12 Mbps for congested and 5 Mbps for uncongested network For IEEE 802.11g, 55 Mbps for congested and 30 Mbps for uncongested network For IEEE 802.11n, 75 Mbps for congested and 50 Mbps for uncongested network
Traffic type	TCP and UDP traffic streams
Packet length	500, 1000, 1500, and 2000 bytes
Total number of packets	The choice of number of packets did not affect the performance observed in the results. Thus we have selected this parameter as 0. As long as our session is 'on', packets are transmitted continuously
Traffic generation	IP traffic generator tool has been used to generate WLAN traffic. IP packets are transferred in a predefined number, size, content and bandwidth in order to measure the performance impact of security algorithms in the wireless LAN

and non-repudiation. On the basis of security services provided by a security protocol in the network, it is very difficult to make any statement on the strength of the security protocol. For example, a security protocol SP_1 is having features of integrity and non-repudiation (2 features) and another protocol SP_2 is having features of confidentiality, access control, authentication (3 features but weak as compared to SP_1). On the comparison of SP_1 and SP_2 with respect to 2 strong security services of SP_1 it can be deduced that SP_1 gives more strength as compared to SP_2. Similarly on the comparison of both protocols SP_1 and SP_2, on the basis of the features not present in SP_1 but present in SP_2, the same deductions may be reached. We will interpret that SP_2 is stronger than SP_1. Hence, it is not an easy task to quantify the absolute dissimilarities between the strength of the two protocols. The confirmation of which one is the better security protocol between the two protocols depends upon several parameters like 'what are the network requirements?', 'which security protocol and features are enabled in the network?' Various studies have been reported in the past to define the quality of protection of a system (QoP). Different security models to evaluate the QoP of a system are discussed in (Luo et al., 2009; Chen et al., 2011) and it is found that it is very hard to differentiate the strength offered by two protocols with similar status.

Another approach to analyze the security strength of VoIP is shown in (Casola et al., 2005). In this method weights are assigned to each security feature and are framed in a matrix form. It is observed that though this matrix approach is efficient but incurs more processing time and power consumption. For the analysis of mobile multimedia applications a different framework is given in (Ong et al., 2003) which defines QoP parameters. A similar study to analyze the security strength provided by various security protocols is demonstrated in (Agarwal and Wang, 2007), where security strength is evaluated by defining utility function and reward model and obtained the cumulative strength offered by security protocols. In this paper the same approach as described by the author in (Agarwal and Wang, 2007) is adopted to quantify the security strength provided by security protocols. In this paper, we analyze the security strength by measuring RSSI, which is determined by utilizing associated weights derived from the security services offered by each protocol.

To measure RSSI the first step includes weight assignment. Weights are assigned in a manner such that when two security protocols provide the same number of security features, higher weights are assigned to the protocol with stronger security features. It ensures that the protocol with stronger security services is given a higher security strength index relative to security protocols with weak strength. Security index defined in the past (Agarwal and Wang, 2007) quantified different ranges of security protocols as compared to the protocols presented in this paper. So to accommodate security protocols used in this paper, weight assignment is done on the basis of the strength of associated security services of these protocols which in turn depends upon the parameters like length of key used, hash functions, message authentication code, digital signatures and so on. This weight assignment only gives comparative strength of one protocol with respect to another but not the absolute strength measurement. It can be illustrated as, if two distinct mechanisms supply the same service of integrity but are assigned weights of 3 and 2 respectively, it doesn't mean that the service with weight 3 is 3 times stronger than the service with weight 2. It simply infers that the service with weight 3 has more strength as compared to service with weight 2. The weights assigned to each security service associated with each security protocol are shown in Table 6 and weight assignment criteria is detailed below:

Service set identifier (SSID): is a network identifier number and is usually broadcasted by access point (AP) so that a station (STA) can access the network. SSID does not provide any

security and is known to be a 'No Security' layer. No security features are provided by SSID, hence no weights are assigned to any feature in SSID.

Wired Equivalent Privacy (WEP): WEP/*64*/*128* is used in our experimental testbed. WEP/128 employs a 128 bit key which provides more strong confidentiality as compared to WEP/64 due to long key. So weights assigned to WEP/64 are lowest as compared to other protocols and weight values assigned to WEP/128 have higher values as compared to WEP/64.

Wi-Fi Protected Access (WPA): In the experimental testbed WPA is used with TKIP disabled and Advanced Encryption Standard (AES) (as it is optional in WPA) enabled (WPA/AES). Since security mechanisms associated with WPA/AES are more, it provides confidentiality and authentication (based on 802.1x and EAP) with enhanced strength as compared to WEP. The security features are assigned with more weight values as compared to WEP/64/128.

WPA2: WPA2 is used in two ways one with TKIP disabled and Advanced Encryption Standard (AES) (as it is optional in WPA) enabled (WPA2/AES), and another when both TKIP and AES are enabled *(WPA2/AES/TKIP)*. Mechanisms used in WPA2/AES are more in number and strong enough as compared to WPA/AES and WEP, so weights assigned to the security features associated with WPA2/AES are higher than WPA/AES. WPA2/AES/TKIP is using a number of mechanisms even more than WPA2/AES, resulting in higher weight values.

WPA and WPA2 are also used with RADIUS server and are called as enterprise security layers. WPA/AES and WPA2/AES explained above are not making use of Radius server to hold per user key. It is generally used in large networks to control the individual access. It supports all the features of WPA/AES and WPA2/AES personal thus providing the same security features. Including this, digital certificates are used in the RADIUS server to authenticate each user, hence enhancing the strength of the protocol. Based on the security mechanisms used (as discussed above for WPA/AES and WPA2/AES) along with digital signatures, weights are assigned as shown in Table 6. Similarly WPA2 is used with both AES and TKIP enabled along with the RADIUS server and provides the maximum number of strong security features and the weights assigned to the associated features are having highest value.

After weight assignment, the second step during the measurement of RSSI is to find out the cumulative effect of all the security features provided by the individual protocol or hybrid protocol (WPA/TKIP/AES). The cumulative effect of security services associated with security protocols is evaluated by finding the linear sum of the weights associated security services. Weights are obtained as defined in the step one. With the assumption that a security protocol SP_x is having N security mechanisms then Relative security strength (RSSI) is measured as:

$$\mathrm{RSSI}(SP_x) = \sum_{n=1}^{N} w_A^j s_A + w_C^j s_C + w_I^j s_I + w_{MA}^j s_{MA} + w_{NR}^j s_{NR} \tag{1}$$

where, w_A^j is the assigned weight of an algorithm on authentication, w_C^j is the assigned weight of an algorithm on confidentiality, w_I^j is the assigned weight of an algorithm on integrity, w_{MA}^j is the assigned weight of an algorithm on mutual authentication and w_{NR}^j is the assigned weight of an algorithm on non-repudiation. $S_{(.)}$ is a service function that indicates if a particular security service is supplied by the algorithm j or not. If yes then its value is 1 otherwise zero. Now if RSSI of security protocol P_9 (WPA2/TKIP/AES/RADIUS) is evaluated, the weights with all the security services given in Table 6 are $w_A^j = 3$, $w_C^j = 3$, $w_I^j = 2.5$, $w_{MA}^j = 3.5$, $w_{NR}^j = 2$ and service function $S_{(A)} = 1$, $S_{(C)} = 1$, $S_{(I)} = 1$, $S_{(MA)} = 1$, $S_{(NR)} = 1$ (represents that all the security features are provided by security protocol). RSSI value for security protocol P_9 is $3 * 1 + 3 * 1 + 2.5 * 1 + 3.5 * 1 + 2 * 1 = 14$ (highest value). Similarly RSSI for $P_2 = 0.5 * 1 + 0.5 * 1 = 0.5 * 1 + 0 + 0 = 1.5$ and for $P_1 = 0$ (lowest value). To study the security strength of various protocols comparative analysis is done by normalizing RSSI values of all the protocols on the basis of the highest value of P_9 and actual RSSI value and normalized values are tabulated in Table 7. From the obtained RSSI values it is observed that the security protocol with stronger security services is obtaining the highest security strength value. Security protocols P_{4-6} are having the same number of security features but have variable RSSI values based on the strength of security services provided by security protocols. Hence the RSSI model maps the security strength to a quantifiable numerical value and provides a clear view of the security strength provided by each protocol. Thus by looking into these security strength values provided by each protocol, application users or designers can access the security protocol and then make the decision if a particular protocol meets their requirements or not.

Table 6 Weights assigned to the implemented security protocols.

Security service	Confidentiality (w_C)	Integrity (w_I)	Authentication (w_A)	Mutual authentication (w_{MA})	Non repudiation (w_{NR})
P_1	–	–	–	–	–
P_2	0.5	0.5	0.5	–	–
P_3	1	0.5	0.5	–	–
P_4	1.5	1	1	1	–
P_5	2	1.5	1.5	2	–
P_6	2.5	2	2	2.5	–
P_7	2	1.5	1.5	1.5	1
P_8	2.5	2	2	2.5	1.5
P_9	3	2.5	2.5	3	2

Table 7 Normalized RSSI values.

Security protocols	Actual RSSI (P_x)	Normalized RSSI
P_1 SSID	0	0
P_2 WEP/64	1.5	11.5
P_3 WEP/128	2	15.3
P_4 WPA/AES	4.5	34.6
P_5 WPA2/AES	7	53.8
P_6 WPA2/AES/TKIP	9	69.2
P_7 WPA/AES/RADIUS	7.5	57.6
P_8 WPA2/AES/RADIUS	11.5	88.4
P_9 WPA2/AES/TKIP/ RADIUS	13	100

7. Performance metrics

We have measured the performance of wireless local area network in terms of throughput, response time, encryption overheads, jitter, and frame loss. These parameters can be defined as:

(a) Throughput (TP) (Megabits/s): is the measure of total number of bytes transmitted over the network in a given time. TP is measured as follows:

$$TP = \frac{I}{T_l(P_x) - T_f(P_x)} \tag{2}$$

where, I is the total amount of data exchanged between two participating nodes. $T_l(P_x)$ and $T_f(P_x)$ represent the last and first data packet sent per unit time between the sender and receiver with security protocol (P_x).

(b) Response Time (RT) (msec): is defined as the total time required for the data stream to travel between two points which includes connection establishment and security negotiation time. We have measured the response time between the server (server is sending the traffic) and the access point. RT is calculated as the time interval between the moment the server sends a traffic stream to access point and the moment the access point acknowledges the server under various conditions. The obtained numerical values are measured in milliseconds.

(c) Encryption overheads*:* on configuring different security protocols into the network, it has been found that different security protocols have different impacts on the performance of wireless networks. We have analyzed the overheads associated with each security layer. Overheads incurred by each security layer have been evaluated as follows (Hayajneh et al., 2012):

Let P_1 denote the security layer with almost zero security level. Overheads caused by this layer are zero and thus this 'No Security' layer is used to compare the other security protocols with some security level. P_x denotes the security policy with some security level (with some encryption and authentication operations) where $x = \{1, 2, 3\ldots\ldots9\}$.

$T^s(n, P_x)$ is the time required to process the nth packet by a sender i with security policy P_x.

$T^r(n, P_x)$ is the time required to process the n^{th} packet by a receiver j with security policy P_x.

$T^t(n, P_x)$ is the time taken by the nth packet to travel in the network between the sender and the receiver with security policy P_x.

Total time taken in the processing of the nth packet to travel between the sender and the receiver with security policy P_x is represented by $T(n, P_x)$ and is equal to

$$T(n, P_x) = T^s(n, P_x) + T^r(n, P_x) + T^t(n, P_x) \tag{3}$$

Assume that K packets have been sent from client i to client j. Therefore the total time required for processing K packets between clients using security policies P_x is represented as a sum of time involved in processing all K packets:

$$\sum_{n=1}^{k}(T(n, P_X)) = \sum_{n=1}^{k}(T^S(n, P_X) + T^r(n, P_X) + T^t(n, P_X)) \tag{4}$$

If we assume that the size of the nth packet is l_n bits, and then the total number of bits in k packets, denoted by B_k, is:

$$B_k = \sum_{n=1}^{k} l_n \tag{5}$$

Using Eqs. (2) and (3), bit rate with security policies P_x can be represented as:

$$BR(P_X) = \frac{B_k}{\sum_{n=1}^{k}(T(n, P_X)) = \sum_{n=1}^{k}(T^S(n, P_X) + T^r(n, P_X) + T^t(n, P_X))} \tag{6}$$

where $BR\ (P_x)$ denotes the bit rate (bits/s), that can be obtained with each security policy P_x.

$$BR(P_1) = \frac{B_k}{\sum_{n=1}^{k}(T(n, P_1)) = \sum_{n=1}^{k}(T^S(n, P_1) + T^r(n, P_1) + T^t(n, P_1))} \tag{7}$$

where $BR\ (P_1)$ is the bit rate (bits/s), achieved by configuring the security policy with zero security level P_1.

Now assume that $O(P_X)$ refers the encryption overheads associated with different security policies (P_X) and is defined as the difference between the bit rate for security layers (P_X) and (P_1). Encryption overheads $O(P_X)$ can be calculated as:

$$O(P_X) = BR(P_X) - BR(P_1) \tag{8}$$

(d) Jitter (J) (msec): is the measure of variation in the time between the data packets caused by the network.

(e) Frame Loss (FL): is the measure of loss of the data frames, that is, frame transmitted over the wireless network but not received at the destination. Frame loss is measured as

$$\%\text{Frame Loss} = \frac{\text{Load(Mbps)} - \text{through put across the load}}{\text{Load(Mbps)}} \tag{9}$$

8. Experimental results and analysis

Experimental results are obtained for analyzing the impact of security protocols on the performance of wireless networks in a class of network scenarios for three IEEE 802.11b/g/n standards. Experiments are performed in both roaming and non-roaming environments. A total of nine security protocols are implemented over the testbed. Detailed specifications/

parameters settings of traffic generator, system configurations, Flow rates for congested and uncongested networks, two different traffic streams, packet number, and packet length used during the experiment is mentioned in Section 5. Performance metrics as defined in Section 7 has been used for the evaluation of the security performance of a secure wireless local area network. First set of experiment was performed for analyzing the security performance of IEEE 802.11b/g/n WLAN standards in the roaming environment. Second set of experiment was performed in non-roaming environment. Though we have performed experiments for all the network scenarios with different packet lengths for the sake of simplicity and due to space constraints we have presented elaborate results for the TCP congested network with 1000 bytes of packet length. However similar trends are observed in all network scenarios.

8.1. Throughput analysis in the roaming scenario

Experiments were performed to study the impact of security protocols on the throughput of IEEE 802.11b/g/n WLAN standards in the roaming network in different network scenarios. The obtained experimental results are elaborated below.

8.1.1. Throughput measurement on the basis of applied security protocol

Variation in the throughput in response to the particular security protocol in roaming scenario for three standards IEEE 802.11b/g/n is shown in Fig. 3. For IEEE 802.11b and IEEE 802.11g the data rate was set to 12 Mbps and 55 Mbps respectively. It is observed that different security protocols have different impacts on the throughput of the network. As shown in Fig. 3 throughput is highest for Service set identification (SSID (P_1)), which is known to be a 'No Security' layer as it provides almost zero level of security. P_1 is also used as a reference for comparison with other security protocols. It is observed that on increasing the complexity of security mechanisms, throughput decreases significantly. Taking average of all the nine protocols $P_{1–9}$ it is found that throughput decreases by 2.36% and 1.36% in IEEE 802.11b and IEEE 802.11g respectively. This throughput degradation is due to an increase in computations of the security protocols, which in turn consume more system resources. As discussed above in Section 5.3 experiments are performed for security protocols at the MAC layer ($P_{1–6}$) and the Application layer (enterprise security $P_{7–9}$). From the obtained numerical results, it is demonstrated that throughput degradation with $P_{7–9}$ is more than $P_{1–6}$. It is due to an increased number of messages in the authentication phase. These obtained numerical values however confirmed the general trends reported in (Baghaei et al., 2004; Turab and Moldoveanu, 2008; Boulmalf et al., 2007).

It is verified from the throughput analysis of two IEEE 802.11b/g standards that the stronger the security mechanism the more is the throughput degradation. But throughput results for IEEE 802.11n (75 Mbps) are dispelling these observations. As shown in Fig. 3 it is depicted that throughput degradation with protocols $P_{2–3}$ (WEP64/128) is approx. 55% higher than that of $P_{1, 4-9}$, though these are the security protocols with less complexity. This is due to the fact that IEEE 802.11n requires AES to be enabled on its WLAN used by its client but the WEP protocol uses RC4 encryption instead of AES. It prohibits the use of high throughput with WEP and drop data rates to 54Mbps as reported in (http://www.intel.com/support/wireless/wlan). From security protocols $P_{1, 4–9}$ (P_4, WPA/AES) throughput decreased to about 1.31% with an increase in the security strength of protocols, also throughput degradation of P_{7-9} is more than that of $P_{4–6}$ but less than $P_{2–3}$.

8.1.2. Throughput on the basis of congested and uncongested network

Experiments are performed to analyze the impact of security protocols on the throughput of network in both congested and uncongested networks by selecting the data rates for access point as 11 Mbps, 54 Mbps and 72 Mbps for IEEE 802.11b/g/n respectively. The obtained experimental results are shown in Fig. 4(a–c). For IEEE 802.11b uncongested and congested networks the traffic was generated at a rate of 5 Mbps and 12 Mbps respectively. The obtained experimental numerical values for uncongested and congested IEEE 802.11b with TCP traffic streams are plotted in Fig. 4(a). It is revealed that for the uncongested network the maximum throughput obtained for P_1 is 6.31 Mbps, which is close to its data flow value. Thereafter throughput decreased gradually depending upon the complexity of the implemented security protocols ($P_{1–9}$), where as in the congested network throughput obtained for P_1 is 6.19 Mbps, very low as compared to its traffic flow value (12 Mbps). Throughput degradation in the TCP congested network is 1.7% higher than the TCP uncongested network Fig. 4(a). From the obtained numerical values it is depicted that throughput in the congested network is less as compared to the uncongested network and this is due to the congestion caused in the network by high traffic generation rates. There is not enough bandwidth available in the network

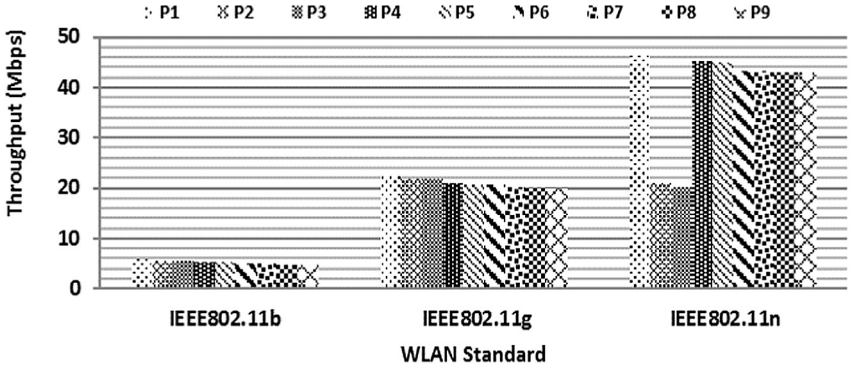

Figure 3 Impact of security protocols on throughput.

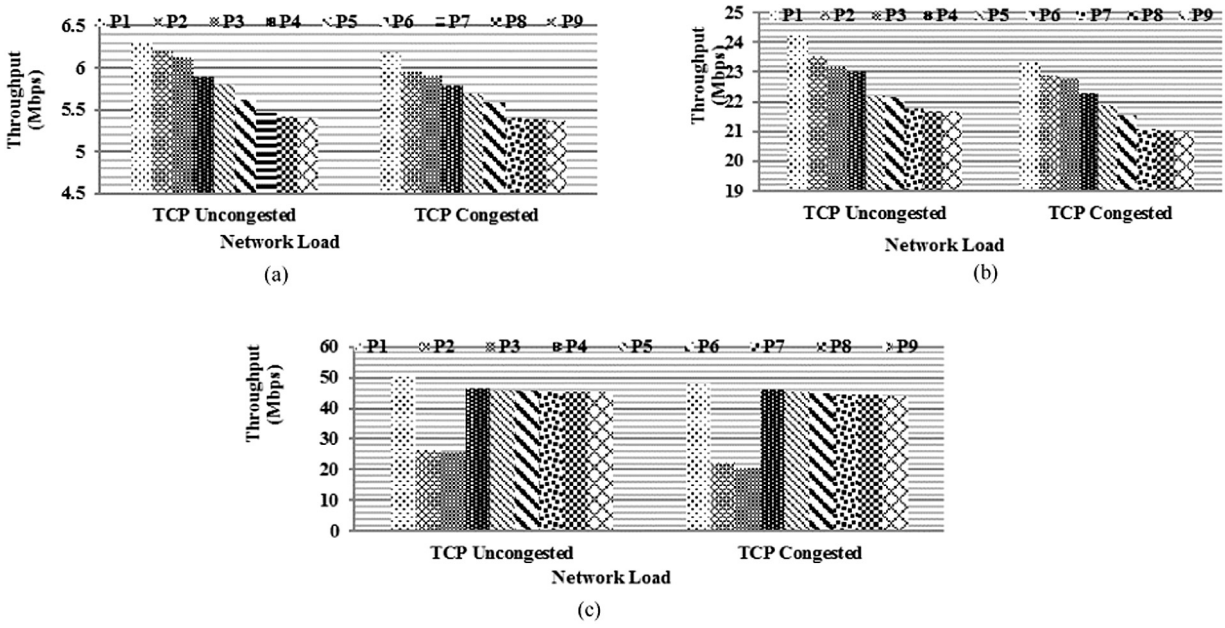

Figure 4 Throughput in roaming scenario IEEE 802.11n network with TCP uncongested and congested (a) IEEE 802.11b, (b) IEEE 802.11g (c) IEEE 802.11n.

and packets can be dropped at the access point. Further throughput decreased significantly with an increase in the strength of the implemented protocol. The traffic was generated at a rate of 30 Mbps and 55 Mbps to make the network uncongested and congested respectively in IEEE 802.11g network. For security protocol P_1 maximum throughput obtained for the TCP uncongested network is 24.2 Mbps and throughput obtained for the TCP congested network is 23.37 Mbps. From the obtained numerical values it is depicted that throughput for the TCP uncongested network is higher than the congested network. Experimental results plotted in Fig. 4 (b) demonstrate that average throughput degradation in the TCP congested network is 2.7% more than the TCP uncongested network. In IEEE 802.11n based network the traffic was generated at a rate of 50 Mbps and 75 Mbps to make the network uncongested and congested respectively. From the experimental results plotted in Fig. 4(c) it is depicted that average throughput decreased about 2.01% for security protocols $P_{1,\ 4–9}$ in the TCP congested network as compared to the TCP uncongested network. For security protocols $P_{2–3}$, similar trends are obtained as described in Section 8.1.1, throughput degradation is maximum for $P_{2–3}$.

8.1.3. Throughput with variable packet length

Experiments are performed to study the impact of different packet lengths (500/1000/1500/2000 bytes) on the throughput of secure wireless network in three WLAN standards IEEE 802.11b/g/n in roaming scenarios. The obtained experimental values are plotted in Figs. 5–7. Throughput plots with different packet lengths for IEEE 802.11b in different network scenarios for all the security protocols are shown in Fig. 5(a, b). Average throughput increased to about 4.01% with an increase in packet length for TCP in the congested network whereas throughput increased to about 4.1% for the UDP congested network with an increase in packet length. Experimental results are obtained for the IEEE 802.11g network, in the similar manner as for IEEE 802.11b WLAN network. Obtained experimental numerical values are plotted in Fig. 6(a, b). From the obtained numerical values it is demonstrated that with increase in packet length throughput increased by 1.2% and 2.6% in TCP and UDP congested networks respectively. Throughput increased to about 1.3% and 2.4% for TCP and UDP congested networks respectively with an increase in packet length in IEEE 802.11n WLAN as given in Fig. 7(a, b).

8.1.4. Throughput with TCP and UDP traffic streams

Experiments are performed to study the impact of traffic streams on the throughput of a secure wireless network in three WLAN standards IEEE 802.11b/g/n and the obtained experimental results are plotted in Fig. 8(a–c). In the uncongested network TCP throughput is 11.6%, 42.8% and 44% more than that of UDP throughput whereas in the congested network TCP throughput is 2.9%, 6.01% and 4.4% more than UDP throughput averaged over the security layers $P_{1–9}$ for IEEE 802.11b, IEEE 802.11g and IEEE 802.11n WLAN respectively. It is due to the fact that TCP is associated with retransmission of the packets, lost due to congestion and error. Percentage throughput variation averaging over the nine security protocols with all the network scenarios in three WLAN standards is shown in Table 8.

8.2. Response time in roaming scenario

Next set of experiments was performed to study the impact of security protocols on the Response time of IEEE 802.11b/g/n WLAN standards in the roaming network in different network scenarios. Response time (RT) is defined as the total time required for the data stream to travel between two points which includes connection establishment and security negotiation time. We have also investigated how the quality of wireless link affects the response time of secure WLAN. We have measured the response time between the server (server is

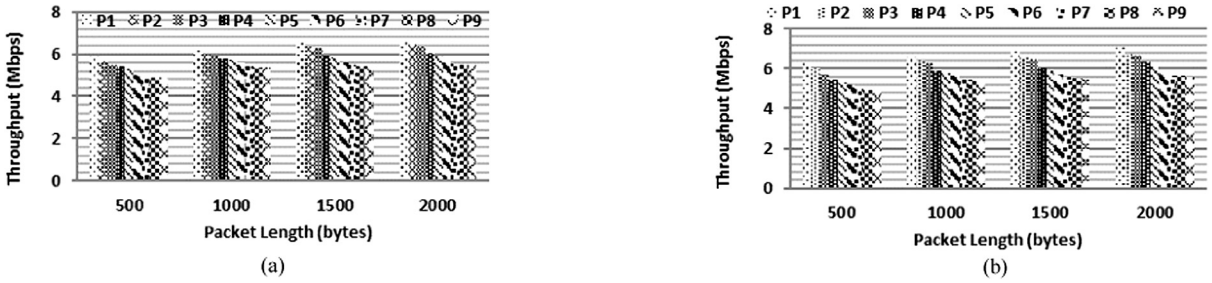

Figure 5 Throughput for different packet lengths in IEEE 802.11b with (a) TCP congested (b) UDP congested.

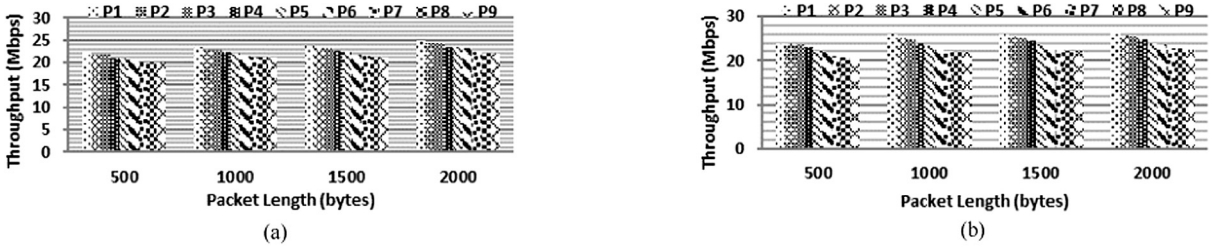

Figure 6 Throughput for different packet lengths in IEEE 802.11g with (a) TCP congested, (b) UDP congested.

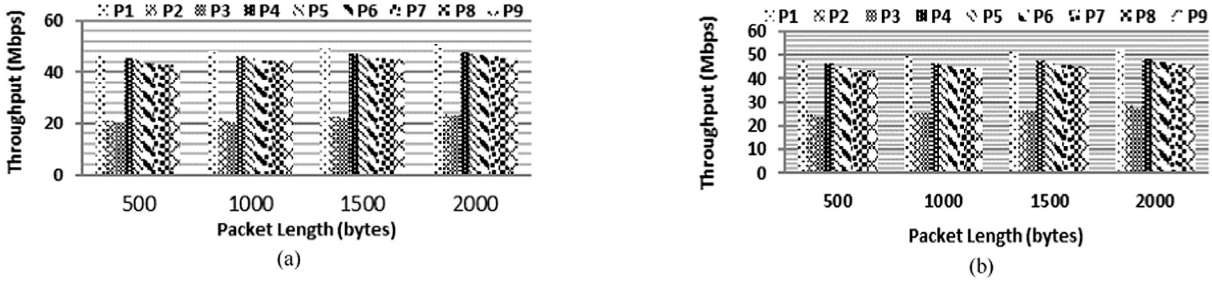

Figure 7 Throughput for different packet lengths in IEEE 802.11n with (a) TCP congested, (b) UDP congested.

sending the traffic) and the access point, and is defined as the time interval between the moment the server sends a traffic stream to the access point and the moment the access point acknowledge the server under various conditions. The obtained numerical values are measured in milliseconds. The obtained experimental results are elaborated below:

8.2.1. Response Time measurement on the basis of applied security policy

Response time variation in response to the particular security policy in the roaming scenario for three standards- IEEE 802.11b/g/n is shown in Fig. 9. It is depicted that different security policies differ from each other in their impact on response time of the network. Response time is lowest for security layer SSID (P_1). With an increase in complexity of security mechanisms and the time involved in initial negotiation during the authentication phase, response time increases significantly as shown in Fig. 9. It is observed that on average response time increased by 1.8% and 1.32% from the security layers $P_{1\text{-}9}$ for IEEE 802.11b and IEEE 802.11g respectively. For IEEE 802.11n response time for protocols $P_{2\text{-}3}$ (WEP64/128) is approx. 48% higher than that of its no security layer. Average increase in RT for security protocols $P_{1,\ 4\text{-}9}$ is 1.6%.

8.2.2. Response Time on the basis of congested and uncongested network

Experiments are performed to analyze the impact of security protocols on the response time of network in congested and uncongested network for IEEE 802.11b/g/n and are shown in Figs. 10–12. The obtained experimental numerical values of RT for uncongested and congested IEEE 802.11b and IEEE 802.11g network with TCP and UDP traffic streams are plotted in Figs. 10 and 11(a, b), it is revealed that response time for TCP congested network is 2% and 3.04% more than that of TCP uncongested network and RT for the UDP congested network is 10.5% and 41% more than that of UDP uncongested network for IEEE 802b and IEEE 802.11g respectively. Security protocols in IEEE 802.11n followed similar trends as detailed for throughput in Section 8.1. From the experimental results plotted in Fig. 12(a, b) it is depicted that average RT increased by about 2.02% for security protocols $P_{1,\ 4\text{-}9}$ in the TCP congested network as compared to the TCP uncongested

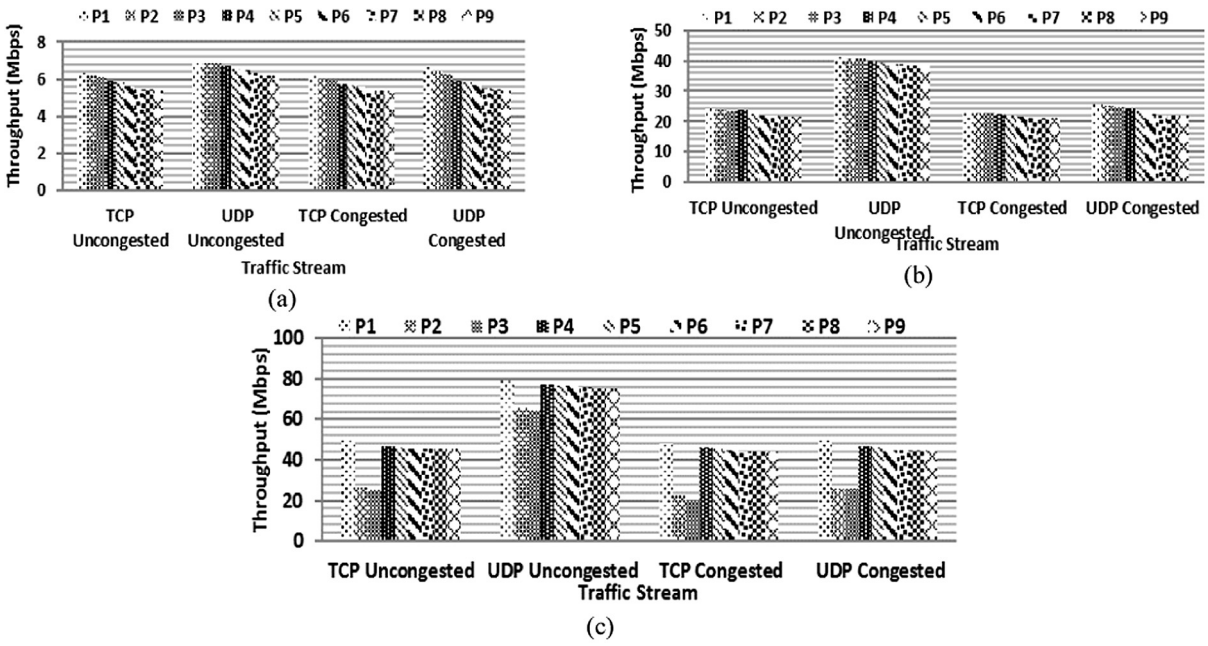

Figure 8 Impact of TCP and UDP traffic stream on throughput with uncongested and congested network (a) IEEE 802.11b, (b) IEEE 802.11g, (c) IEEE 802.11n.

network. For the UDP congested network RT is 40.2% more than in the UDP uncongested network for $P_{1,\ 4–9}$. It is found that RT for security protocols $P_{2–3}$ is highest in both congested and uncongested networks.

8.2.3. Response time with TCP and UDP traffic streams

Experiments are performed to study the impact of traffic streams on the response time of the secure wireless network in three WLAN standards IEEE 802.11b/g/n and the obtained experimental results are plotted in Fig. 13(a–c). In the congested network TCP response time is 3.2%, 5.9%, and 0.98% more than UDP averaged over the security layers $P_{1–9}$ in all IEEE 802.11b, IEEE 802.11g and IEEE 802.11n networks respectively.

We have obtained RT values at different packet lengths in various network scenarios. Due to the space limitation we have not discussed here the results for analysis of the impact of packet length on RT. Average percentage variation in response time in all the network scenarios is presented in Table 9.

8.3. Encryption overheads in roaming scenario

Third set of experiments was performed to study the encryption overheads incurred due to the implemented security protocols in IEEE 802.11b/g/n WLAN standards in roaming network in different network scenarios. Overheads are evaluated in the manner as described in Section 5. The obtained experimental results are elaborated below:

8.3.1. Encryption overheads on the basis of applied security protocols

With an increase in complexity of the security algorithm, the number of computations also increases which further increase the associated overheads. In security protocols overheads are associated in encryption and decryption of information. From the experimental analysis it is found that overheads are minimum for P_1 and maximum for P_9. This is because P_1 provides zero security and no encryption and decryption are performed whereas P_9 provides multilayer security including RADIUS server authentication which enhances the complexity of the security protocol and hence the associated overheads. It is observed that on taking the average over the security protocols $P_{1–9}$ overheads incurred are increased by 15.4% and 18.9% for IEEE 802.11b and IEEE 802.11g respectively as shown in Fig. 14. For IEEE 802.11n, EO for protocols P_{2-3} (WEP64/128) are very high. Average increase in EO for security protocols $P_{1,\ 4–9}$ is 11.3%.

8.3.2. Encryption overheads on the basis of congested and uncongested network

Experiments are performed to analyze the overheads associated in congested and uncongested secure networks. The obtained experimental numerical values for uncongested and congested IEEE 802.11b/g network with TCP and UDP traffic streams are plotted in Figs. 15 and 16(a, b). It is revealed that overheads incurred with TCP congested network are 16.4% and 22% more than that of the TCP uncongested network and EO for the UDP congested network is 41.7% and 14.2% more than that of the UDP uncongested network for IEEE 802.11b and IEEE 802.11g respectively. From the experimental results plotted in Fig. 17(a, b) it is depicted that for IEEE 802.11n average EO increased by about 22.4% for security protocols $P_{1,\ 4–9}$ in the TCP congested network as compared to the TCP uncongested network Fig. 17(a). For the UDP congested network RT is 28% more than in the UDP uncongested network for $P_{1,\ 4–9}$.

8.3.3. Encryption overheads with TCP and UDP traffic streams

Experiments are performed to study the encryption overheads incurred due to different traffic streams in a secure wireless net-

Table 8 Percentage variation of throughput in a secure wireless network in different network scenarios.

Decrease in TP with increase in complexity of security policy (averaging over all the security protocols)										
IEEE 802.11b				IEEE 802.11g				IEEE 802.11n		
2.36%				1.36%				1.31%		
Increase in TP of uncongested network as compared to the congested network (averaging over all the security protocols)										
IEEE 802.11b				IEEE 802.11g				IEEE 802.11n		
TCP	UDP			TCP	UDP			TCP	UDP	
1.7%	10.5%			2.7%	41%			2.01%	47.2%	
Increase in TP with UDP traffic stream as compared to the TCP stream (averaging over all the security protocols)										
IEEE 802.11b				IEEE 802.11g				IEEE 802.11n		
Congested	Uncongested			Congested	Uncongested			Congested	Uncongested	
2.9%	11.6%			6.01%	42.8%			4.4%	44%	
Increase in TP with an increase in packet length (averaging over all the security protocols)										
TCP congested				TCP uncongested				UDP congested			UDP uncongested	
IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
4.01%	1.2%	1.3%	3.1%	4.3%	2.1%	4.1%	2.6%	2.4%	2.02%	3.5%	2.5%

work in three WLAN standards IEEE 802.11b/g/n and the obtained experimental results are plotted in Fig. 18(a–c). Overheads are more in TCP than in UDP only for P_2 and the overheads incurred are 28.2% and 32.1% more in the UDP congested network for $P_{3–9}$ as compared to TCP traffic stream for IEEE 802.11b and IEEE 802.11g respectively. For IEEE 802.11n WLAN overheads are 11.9% more in TCP than in UDP for $P_{2–5}$ and the overheads incurred are 3.7% more in the UDP congested network for $P_{6–9}$ as compared to the TCP traffic stream.

8.4. Frame loss

Another set of experiments is performed for the measurement of frame loss for all the three standards at different load values. We have plotted percentage frame loss versus load only for four security protocols because similar observations are made for the rest of the security protocols. Load is varied from low to high values i.e. from congested to uncongested range. Frame loss is calculated using Eq. (9). Following observations are made:

8.4.1. Frame loss in IEEE 802.11b/g/n WLAN

The experimental results presented in Figs. 19–24 and numerical values shown in Tables 10–15 indicate that percentage frame loss increases with an increase in load for both TCP and UDP traffic stream. It is found that frame loss is less in the uncongested network and is very high in the congested network. Frame loss with UDP traffic stream is more than that of the TCP stream. Similar trends are observed in all the three WLAN standards IEEE 802.11b/g/n. Further it is revealed that FL increases with an increase in security strength.

8.5. Jitter

Experimental results are also obtained to study the impact of different security protocols on jitter in different network scenarios. It is observed that different security implementations have no impact on jitter values in all the network scenarios. It is found that for IEEE 802.11b jitter value varies from 0 to 2 ms. For IEEE 802.11g/n jitter is almost zero at the application layer and this value reaches 1 ms at enterprise security layers.

8.6. Performance analysis in the non-roaming scenario

Experiments are performed to study the impact of implemented security protocols on the performance of WLAN in the non-roaming environment where the access point and client are in same domain. Results are obtained in a class of network scenarios similar to the scenarios used for the roaming network. It is observed that performance variations in the non-roaming network are similar to the roaming network in all the network scenarios but the performance degradation in the non-roaming network is less than that of the roaming network. Because of the similar trends followed by all the network scenarios for all the performance parameters we have presented results only for throughput and response time. Further for numerical analysis, TCP congested and UDP congested

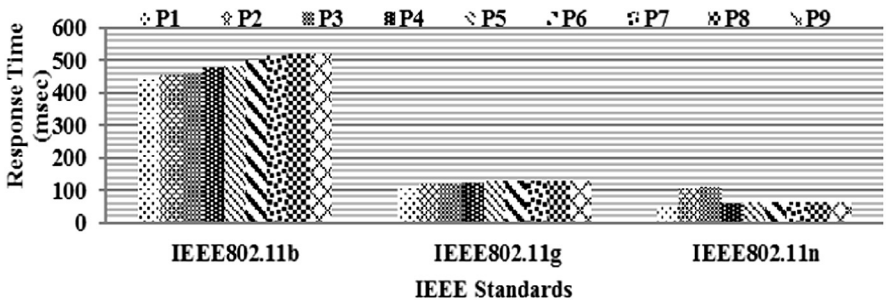

Figure 9 Impact of security protocols on response time.

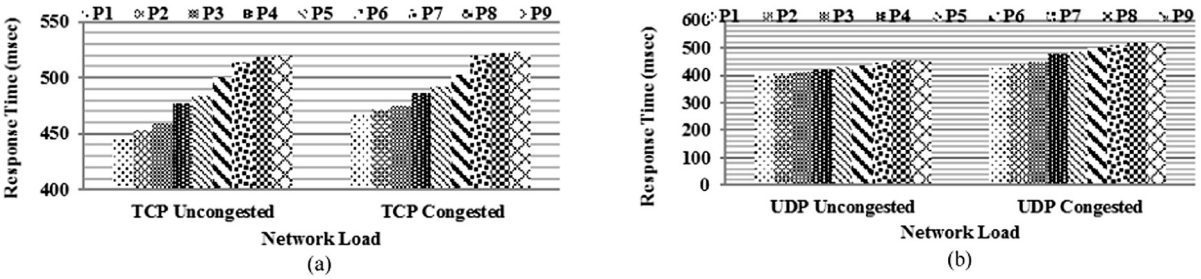

Figure 10 Response time in roaming scenario for IEEE 802.11b uncongested and congested network for (a) TCP, (b) UDP.

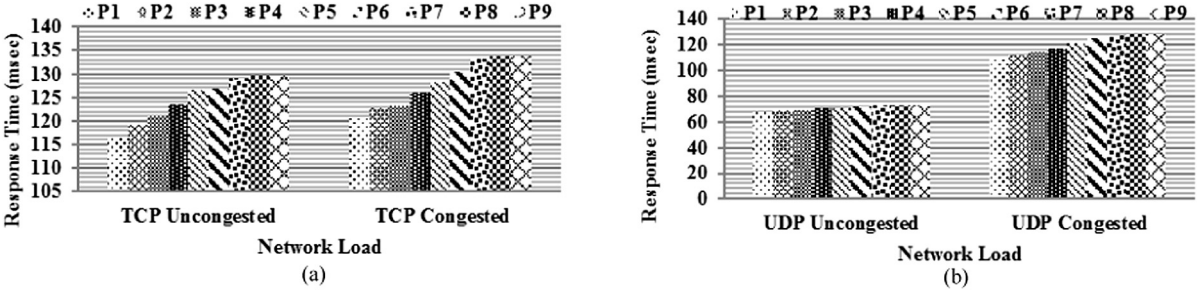

Figure 11 Response time in roaming scenario IEEE 802.11g network for uncongested and congested (a) TCP, (b) UDP.

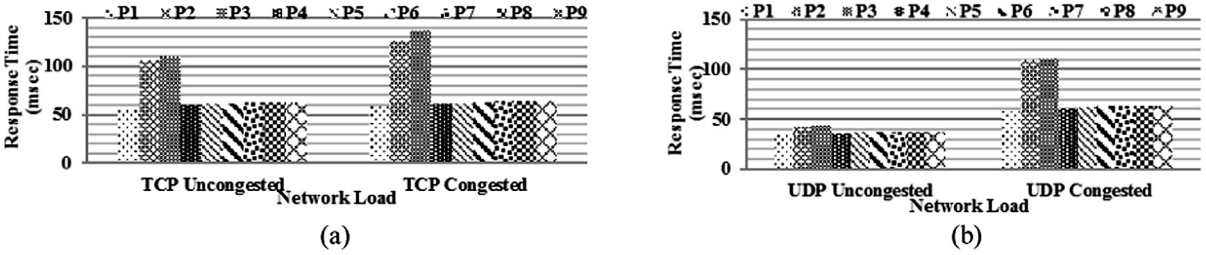

Figure 12 Response time in roaming scenario IEEE 802.11n network for (a) TCP uncongested and congested, (b) UDP uncongested and congested.

network with a packet length of 1000bytes are considered for all network scenarios. Throughput and response time values obtained from the experimental analysis of IEEE 802.11b/g/n WLAN standards depict that variations in throughput and response time for the non-roaming network are similar to the roaming network in all network scenarios. Throughput decreases and response time increases with an increase in security strength. Also a decrease in TP is more in the congested network as compared to the uncongested network whereas response time increases with an increase in security strength. Percentage decrease or increase in throughput and response time in different network scenarios is shown in Table 16. The comparative analysis of performance degradation in both roaming and non-roaming scenarios is presented in Table 17.

From the above analysis it is found that different security layers behave differently in various network scenarios. Every layer has a different security strength and different performance impact in terms of throughput, response time, encryp-

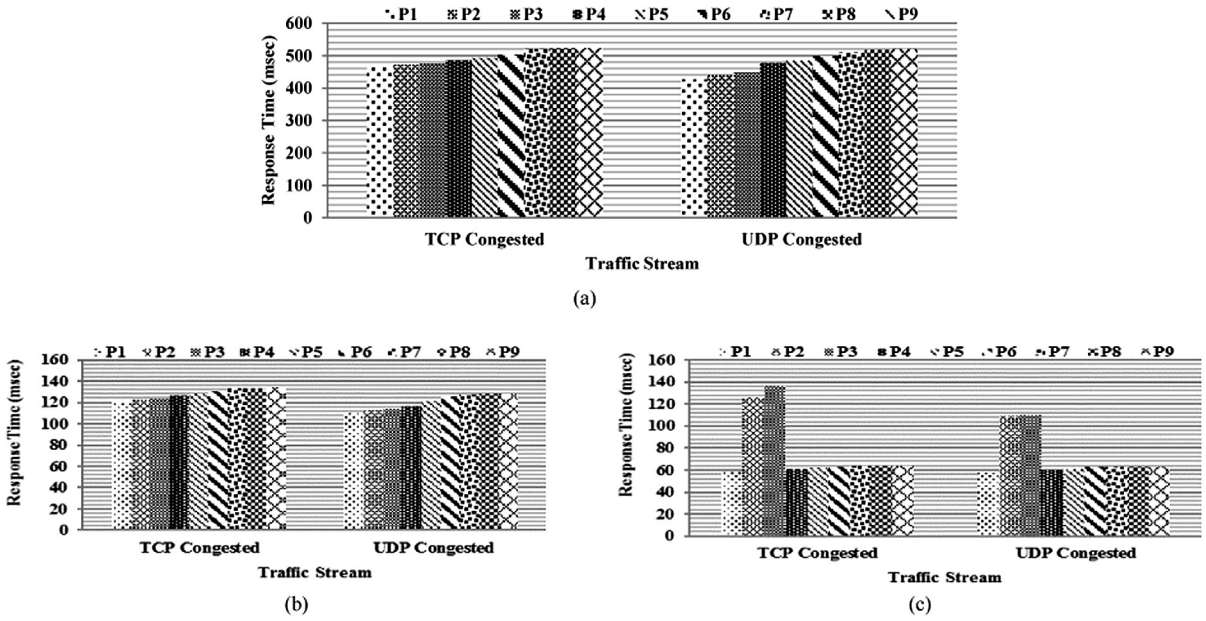

Figure 13 Impact of TCP and UDP traffic stream on response time with congested network (a) IEEE 802.11b, (b) IEEE 802.11g, (c) IEEE 802.11n.

Table 9 Percentage variation of response time in a secure wireless network in different network scenarios.

Increase in RT with an increase in complexity of security policy (averaging over all the security protocols)					
IEEE 802.11b		IEEE 802.11g		IEEE 802.11n	
1.8%		1.3%		1.6%	
Decrease in RT of uncongested network as compared to congested network (averaging over all the security protocols)					
IEEE 802.11b		IEEE 802.11g		IEEE 802.11n	
TCP	UDP	TCP	UDP	TCP	UDP
2%	10.5%	3.04%	41%	2.02%	40.2%
Decrease in RT with UDP traffic stream as compared to the TCP stream (averaging over all the security protocols)					
IEEE 802.11b Congested		IEEE 802.11g Congested		IEEE 802.11n Congested	
3.2%		5.9%		0.98%	
Decrease in RT with an increase in packet length (averaging over all the security protocols)					
TCP congested			UDP congested		
IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
3.99%	3.5%	1.58%	4.1%	2.5%	1.59%

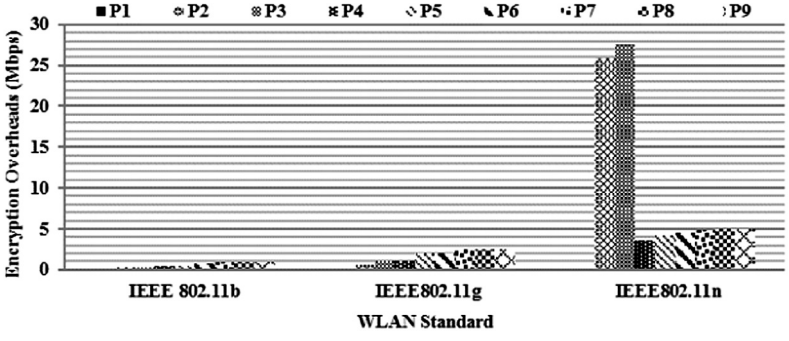

Figure 14 Impact of security protocols on encryption overheads.

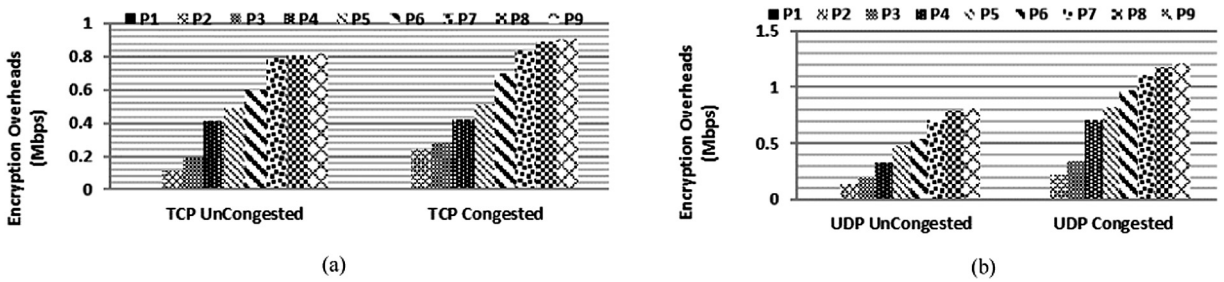

Figure 15 Encryption overheads in the roaming scenario for IEEE 802.11b for an uncongested and congested network (a) TCP, (b) UDP.

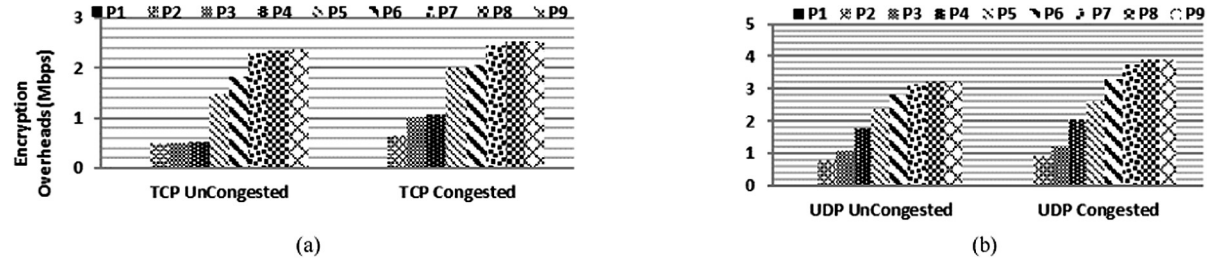

Figure 16 Encryption overheads in roaming scenario IEEE 802.11g uncongested and congested network for (a) TCP, (b) UDP.

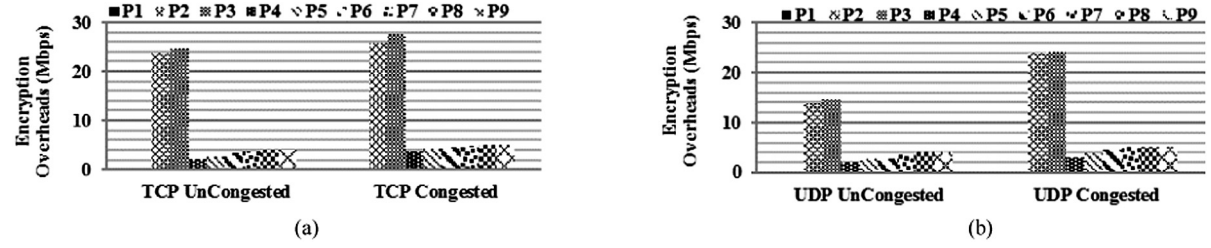

Figure 17 Encryption overheads in the roaming scenario IEEE 802.11n network for (a) TCP uncongested and congested, (b) UDP uncongested and congested.

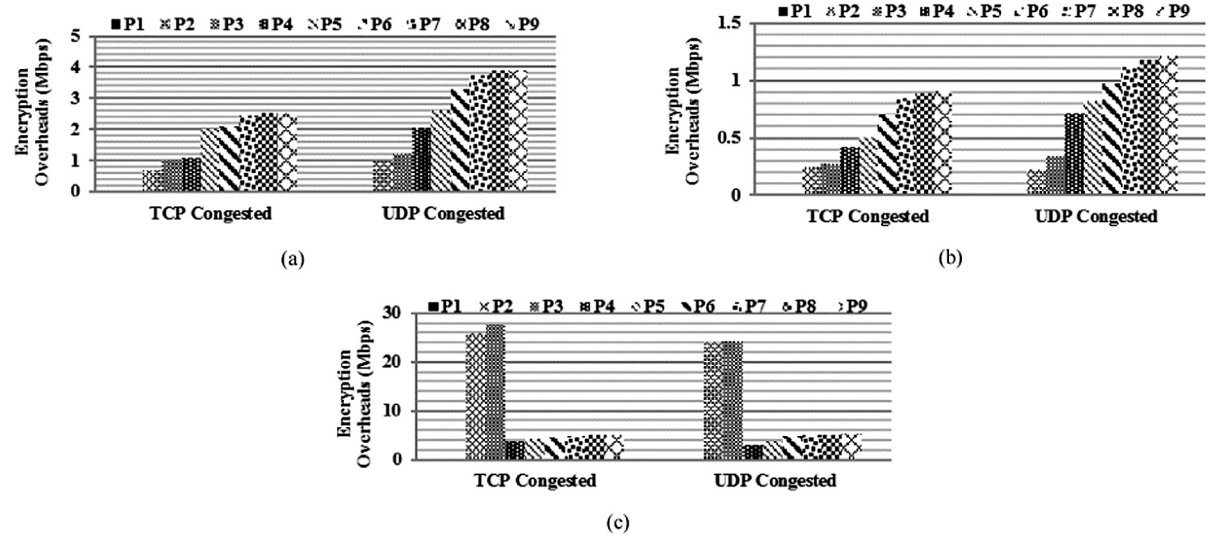

Figure 18 Impact of TCP and UDP traffic stream on encryption overheads with the congested network (a) IEEE 802.11b, (b) IEEE 802.11g, (c) IEEE 802.11n.

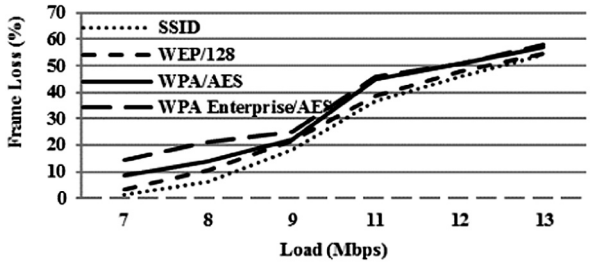

Figure 19 TCP frame loss percentage with different security protocols in IEEE 802.11b.

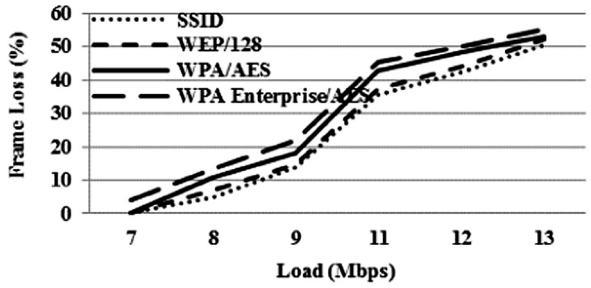

Figure 20 UDP frame loss percentage with different security protocols in IEEE 802.11b.

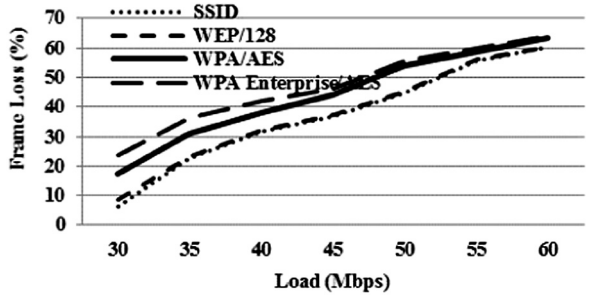

Figure 21 TCP frame loss percentage with different security protocols in IEEE 802.11g.

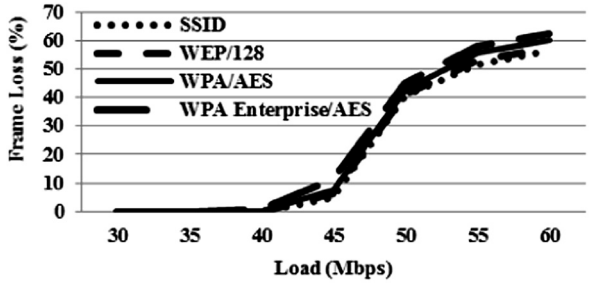

Figure 22 UDP frame loss percentage with different security protocols in IEEE 802.11g.

tion overhead, and frame loss. Including the encryption all the network parameters, type of traffic stream, network load,

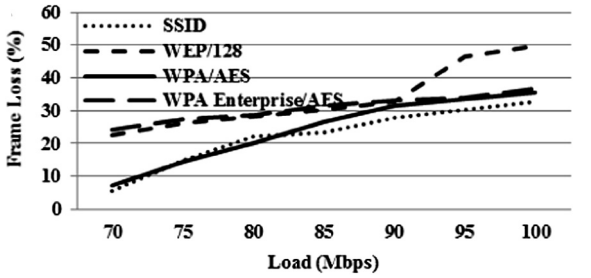

Figure 23 TCP frame loss percentage with different security protocols in IEEE 802.11n.

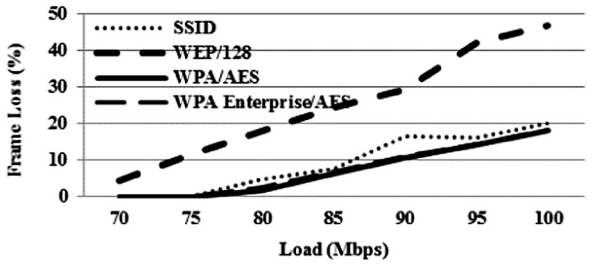

Figure 24 UDP frame loss percentage with different security protocols in IEEE 802.11n.

Table 10 Frame loss with TCP traffic stream in IEEE 802.11b.

Network load (Mbps)	Security protocols			
	P_1	P_3	P_4	P_7
7	1.5	3.4	8.5	14.57
8	6	10.62	14.13	21.13
9	18.1	21.56	22.11	24.88
11	36.5	38.73	45	45.82
12	45.83	48	50.66	51
13	53.93	54.69	56.93	57.92

Table 11 Frame loss with UDP traffic stream in IEEE 802.11b.

Network load (Mbps)	Security protocols			
	P_1	P_3	P_4	P_7
7	0	0	0	4
8	5	7.1	10.87	13.5
9	13.89	14.77	18	21.78
11	35.63	37.36	42.82	45.27
12	42.5	44.08	48.58	50
13	50.61	52.15	53.15	55.08

packet size, also affect the performance of the wireless local area network. Encryption overheads increases, throughput decreases, and response time increases continuously with an increase in strength of security. Security layers 7–9 are enterprise security layers. These are more complex, highly secure

Table 12 Frame loss with TCP traffic stream in IEEE 802.11g.

Network load (Mbps)	Security protocols			
	P_1	P_3	P_4	P_7
30	6.3	8.76	17.26	23.73
35	22.68	23.17	30.88	36.48
40	31.46	32.13	38	42.17
45	36.64	37.28	44.27	46.2
50	44.64	45.06	53.8	55.6
55	55.72	56.18	58.76	59.78
60	60.08	60.16	63.15	64.2

Table 13 Frame loss with UDP traffic stream in IEEE 802.11g.

Network load (Mbps)	Security protocols			
	P_1	P_3	P_4	P_7
30	0	0	0	0
35	0	0	0	0
40	0	0	0	1.1
45	4.64	6.5	7.4	11.22
50	40.36	41.28	42.68	44.94
55	51.47	53.07	55.83	57.94
60	56.38	57.48	60.41	62.63

Table 14 Frame loss with TCP traffic stream in IEEE 802.11n.

Network load (Mbps)	Security protocols			
	P_1	P_3	P_4	P_7
70	5.6	22.66	7.32	24.11
75	14.8	26.33	14.46	27.4
80	22.26	28.38	20.15	28.85
85	23.34	30.44	26.53	31.68
90	28	32.85	31.56	33.14
95	30.4	46.52	33.52	34.02
100	32.74	49.8	35.39	36.84

Table 15 Frame loss with UDP traffic stream in IEEE 802.11n.

Network load (Mbps)	Security protocols			
	P_1	P_3	P_4	P_7
70	0	4.3	0	0
75	0	11.4	0	0
80	4.6	18.03	1.6	2.4
85	7.6	24.32	6.44	6.88
90	16.45	29.4	10.54	10.95
95	15.98	42.14	14.12	14.49
100	20.04	46.74	18.11	18.41

layers and have more performance degradation as compared to layers 1–6. These trends are followed in IEEE 802.11b/g WLAN standards. It is observed that IEEE 802.11n behaves differently as compared to two other standards where maximum performance degradation is observed with WEP64/128. The results presented in the paper reveal that security and network performance work in contrast to each other. An attempt to make a wireless application more secure, often results in performance degradation. Our comprehensive numerical analysis recommends the appropriate security algorithm in every network scenario. For designing an application, designers are always required to choose an acceptable level of both security and its associated performance. Application designers always have different inclinations, on the basis of the risk they can tolerate and the performance price they are ready to bear.

There are a variety of network services which varies in their security and QoS requirements. For example, consider real time applications which are classified into different categories such as conversational, interactive, streaming and background. In conversational applications real time conversation takes place such as Voice over IP (VoIP), video conferencing, interactive games (on line gaming), telemetry and telnet. For audio and video conversation high throughput and the response time less than 150 msec is preferred (Farkas et al., 2006). From the obtained numerical values it is observed that RT is less than 150 msec in all the network scenarios with all the security policies. Jitter value of 1 msec is acceptable for these audio and video conversation applications and our obtained numerical values for jitter in all network scenarios are between 0ms and 1ms except for enterprise security where the jitter value reaches to 2 ms. These applications are also tolerant to some degree of packet loss. For interactive games, telemetry and telnet services the acceptable RT values are 250 ms.

The obtained results reveal that in real time conversational applications though RT increases with an increase in security strength but observed RT values are within the acceptable range for IEEE 802.11g/n and hence not affecting the network performance. Similarly jitter is not affected by the implementation of security protocols. Since high throughput is required in conversational services, security protocols with higher strength cannot be used.

Interactive services include voice messaging, web browsing-HTML, email and Transaction services (such as e-commerce, ATM, Credit cards and online banking). Low throughput values, high RT (between 1s and 4s) more than conversational services is tolerable in these applications. Since transaction services require high security even at the cost of performance, higher security protocols are recommended. Streaming services include transfer of high quality music, movie clips, bulk data and images. These applications require high data rate values. Though high delays are tolerable to these applications but throughput degrades significantly at higher security layers security protocols with a lower strength are recommended in these applications.

Background services are email arrival notification, low priority transaction services, data downloading and short message service (SMS). These best effort services do not have particular performance constraints. Any security protocol required by the user can be implemented in these services. The numerical results presented in this paper can be used to choose a security policy, depending upon the sensitivity of data transmitted and the performance requirements by users. From the results it is observed that in the application where security is of major concern for example in bank transactions like ATMs, online payments etc. security layers which make use

Table 16 Percentage variation of throughput in a non-roaming wireless network in different network scenarios.

IEEE 802.11 LAN standards	Performance metrics	Percentage variation in various network scenario			
		Applied security policy	Congested and uncongested network	TCP and UDP traffic stream	With an increase in packet length
Percentage Variation in IEEE 802.11b	Throughput	1.26% (Throughput decreases with an increase in strength of the security protocol)	1.9% (TCP congested < TCP uncongested)9.79% (UDP congested < UDP uncongested)	3% (UDP congested > TCP congested)	3.4% (TP increase with an increase in PL)
	Response Time	1.28% (RT increases with an increase in strength of the security protocol)	1.8% (TCP congested > TCP uncongested)9.79% (UDP congested > UDP uncongested)	3.3% (UDP congested < TCP congested)	3.8% (RT decrease with an increase in PL)
Percentage Variation in IEEE 802.11g	Throughput	1.2% (Throughput decreases with an increase in strength of the security protocol)	2.8% (TCP congested < TCP uncongested)39.9% (UDP congested < UDP uncongested)	5.7% (UDP congested > TCP congested)	2.7% (TP increase with an increase in PL)
	Response Time	1.18% (RT increases with an increase in strength of the security protocol)	2.9% (TCP congested > TCP uncongested)39.9% (UDP congested > UDP uncongested)	5.9% (UDP congested < TCP congested)	2.9% (RT decrease with an increase in PL)
Percentage Variation in IEEE 802.11n	Throughput	1.33% (Throughput decreases with an increase in strength of the security protocol)	5.1% (On averaging over TCP congested < TCP uncongested)43% (UDP congested < UDP uncongested)	4.1% (UDP congested > TCP congested)	1.7% (TP increase with an increase in PL)
	Response Time	1.35% (RT increases with an increase in the strength of the security protocol from $P_{1,\ 4\text{-}5}$)	5.7% (On averaging over TCP congested > TCP uncongested)43.8% (UDP congested > UDP uncongested)	4.5% (UDP congested < TCP congested)	1.9% (RT decrease with an increase in PL)

Table 17 Comparative analysis of roaming and non-roaming networks.

Performance parameters	WLAN standards		
	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Throughput	(TP in NRS > RS) 7–8% in all TCP UDP congested and uncongested networks	(TP in NRS > RS) 4–5% in all TCP UDP congested and uncongested networks	(TP in NRS > RS) 3–4% in all TCP UDP congested and uncongested networks
Response Time	(RT in NRS < RS) 8% in all TCP UDP congested and uncongested networks	(RT in NRS < RS) 5% in all TCP UDP congested and uncongested networks	(RT in NRS < RS) 4% in all TCP UDP congested and uncongested networks
Encryption overheads	(EO in RS > NRS) 45% in all TCP UDP congested and uncongested networks	(EO in RS > NRS) 22.3% in all TCP UDP congested and uncongested networks	(EO in RS > NRS) 22% in all TCP, UDP congested and uncongested networks
Frame loss	(FL in RS > NRS)	(FL in RS > NRS)	(FL in RS > NRS)
Jitter	RS = NRS	RS = NRS	RS = NRS

of digital signatures as the basis can be used. For the applications where security is of less concern but a network with better performance is required lower security layers (WEP, WPA/AES) can be used.

9. Statistical analysis

A statistical analysis using a statistical tool, Minitab 17, is presented in this section (www.minitab.com). Statistical analysis of all the parameters discussed above in Section 7 has been done. In this paper we have elaborated the statistical results for throughput and response time in all the network scenarios for IEEE 802.11n.

This statistical analysis is based on null and alternative hypothesis. The hypothesis being considered is:

- There is no impact of security mechanisms on the performance of the network. The alternative hypothesis is that, the security mechanisms affect the performance of the network
- The traffic streams TCP and UDP have no effect on the network performance. The alternative hypothesis is that, the TCP and UDP significantly affect the performance of the network.
- Congested and uncongested networks (Network Load) do not affect the network performance. The alternative

hypothesis is that, both congested and uncongested networks affect the performance of the network.
- Packet length has no impact on the network performance. The alternative hypothesis is that the packet length affects the network performance.
- Different network scenarios such as security mechanisms, TCP and UDP traffic stream, congested and uncongested network, and packet length have no interaction among each other. The alternative hypothesis is that these network scenarios have some interaction with each other

Hypothesis testing is done by determining, whether the null hypothesis is rejected or is not rejected at a predetermined significance level known as α-value. This α-value is usually taken as 0.05. The α-value is compared with p-value to decide if the null hypothesis is or is not rejected. The null hypothesis is rejected if p-value is less than α-value (p-value < 0.05). To analyze the impact of various network scenarios on the network performance with implemented security protocols, statistical results are obtained using analysis of variance. Results obtained from the statistical analysis are detailed below.

9.1. Descriptive statistical analysis (mean and standard deviation)

While evaluating the network performance, understanding the QoS stability is an important issue. Like in the roaming scenario, it is not always possible to know the user's profile in advance. Wireless networks are always configured with a variety of protocols which offer users a large variation in QoS. Using descriptive analysis we are analyzing the security protocols with low variability. Statistical variations incurred by each protocol implemented in the experiments are measured in different network scenarios. Descriptive statistics such as mean (μ) and standard deviation (σ) are used to summarize and to measure the variability of data respectively. For descriptive analysis three factors; security protocols, traffic streams (TCP and UDP) and network load (congested and uncongested networks) have been considered. Mean and standard deviation for both TP and RT are shown in Tables 18 and 19.

We illustrate these statistical variations incurred in various network scenarios with the implemented security protocol as *robustness* of a security protocol against mobility. The obtained statistical mean values depict that throughput decreases and RT increases with an increase in security strength except for protocols 2 and 3 in IEEE 802.11n WLAN. From the standard deviation values of throughput shown in Table 18 it is found that in an uncongested environment with TCP traffic stream σ value for security protocols P_8 and P_9 is minimum hence are less variable protocols with low throughput values as compared to the other protocols. The protocol P_7 is having slightly more variation as compared to P_{8-9} but with high throughput. Though protocols P_{8-9} have low σ values as compared to P_7 but P_7 can be viewed as the best security protocol with good tradeoff between robustness and security strength. With similar reasoning in UDP uncongested network P_6, in the TCP congested network P_{4-5} and in the UDP congested network P_5 can be considered as best protocols with high tradeoff between robustness and security strength.

Table 19 represents the robust analysis of security protocols in terms of response time. It is observed that in TCP and UDP uncongested networks P_7 and P_6 respectively, in both TCP and UDP congested network P_5 provides the best tradeoff between robustness and security strength. The analysis of performance variation in different networks is an important issue. Generally security protocols are chosen in advance in mobile scenarios. However, if the administrators will choose security protocols merely on the basis of assumptions or at random, it will result in performance degradation specifically in real time services. Larger the performance variation in the network the larger will be the packet loss, hence larger will be the performance degradation. So prior knowledge of performance variation incurred with the implemented security protocol is essential. Results presented in Tables 18 and 19 depict that different security protocols vary in their robustness against mobility.

9.2. Analysis of variance (ANOVA)

To study the impact of different network scenarios on the network performance, an analysis of variance has been done using a general linear model that represents the relation between one or more factors and the response. In the present work the factors under consideration are; security mechanisms, traffic type, network load and packet size and their

Table 18 Mean and standard deviation of throughput in congested and uncongested WLAN.

Security protocols	Throughput (Mbps) in uncongested WLAN				Throughput (Mbps) in congested WLAN			
	TCP		UDP		TCP		UDP	
	Mean (μ)	Standard deviation (σ)	Mean (μ)	Standard deviation (σ)	Mean (μ)	Standard deviation (σ)	Mean (μ)	Standard deviation (σ)
1	51.5225	1.029316	80.8425	1.07009	49.9425	1.415306	51.435	1.773706
2	28.0525	0.719508	67.0775	1.740907	23.8675	0.955454	27.9875	1.487982
3	27.3325	0.834041	65.7825	1.719736	22.8075	0.948029	27.1	1.286883
4	48.695	0.850157	78.8775	0.597348	47.8525	0.650455	48.5525	0.647064
5	48.1225	1.110837	78.3625	0.508224	47.4325	0.682709	47.7225	0.539776
6	47.6975	1.041037	78.1	0.354401	46.4575	1.041997	46.975	0.659217
7	47.17	0.771924	77.4725	0.973392	46.205	0.975209	46.5275	0.715652
8	47.01	0.680245	77.0325	0.940687	45.9	0.763457	46.21	0.7313
9	46.9225	0.672675	76.9725	0.910325	45.9075	0.847482	46.105	0.701831

Table 19 Mean and standard deviation of throughput in congested and uncongested WLAN.

Security protocols	Response time (msec) in uncongested WLAN				Response time (msec) in congested WLAN			
	TCP		UDP		TCP		UDP	
	Mean (μ)	Standard deviation (σ)	Mean (μ)	Standard deviation (σ)	Mean (μ)	Standard deviation (σ)	Mean (μ)	Standard deviation (σ)
1	56.0996	1.5126	35.3753	0.6142	57.9511	2.0833	56.2410	2.3582
2	105.617	3.9901	42.8142	1.3260	125.4817	7.0943	106.113	6.9932
3	108.577	4.4419	43.6773	1.3986	131.7187	7.5202	109.743	6.9775
4	58.691	1.2314	36.2683	0.4208	60.52162	1.2476	59.621	1.1889
5	60.1935	1.8153	36.5104	0.3794	61.0753	1.2930	60.6871	1.0950
6	60.419	1.8879	36.6343	0.3048	61.7731	1.2914	61.6882	1.2840
7	61.4307	1.4480	36.9426	0.6240	62.7675	1.8095	62.3037	1.4022
8	61.6423	1.3323	37.1573	0.6160	63.1865	1.5334	62.7470	1.4606
9	61.7606	1.3284	37.1865	0.6019	63.1801	1.6513	62.8932	1.4295

Table 20 ANOVA analysis for throughput.

Source	DF	Adj SS	Adj MS	*F*-Value	*p*-Value
Security protocols	8	9263.7	1158.0	16.81	0.000
Traffic types	1	10015.8	10015.8	145.38	0.000
Network load	1	10544.4	10544.4	153.05	0.000
Packet size	3	87.7	29.2	0.42	0.036
Error	130	8956.2	68.9		
Total	143	38867.9			

Table 21 ANOVA analysis for response time.

Source	DF	Adj SS	Adj MS	*F*-Value	*p*-Value
Security protocols	8	44218.7	5527.3	37.45	0.000
Traffic types	1	12655.0	12655.0	85.74	0.000
Network load	1	13923.0	13923.0	94.33	0.000
Packet size	3	426.8	142.3	0.96	0.012
Error	130	19188.2	147.6		
Total	143	90411.8			

corresponding responses are throughput and response time. Analysis of variance results for throughput and response time is shown in Tables 20 and 21. The ANOVA output is prepared in a table including the list of the sources of variation (factors), their degrees of freedom (DF), the total sum of squares (SS), and the mean squares (MS). The analysis of the variance table also includes the *F*-statistics and *p*-values. These parameters are used to study whether the factors are significantly related to the response. The obtained results depict that the considered four factors have a significant impact on the response (throughput and response time). For all the factors *p*-value is less than 0.05 in both throughput and response time. Hence the null hypothesis is rejected and an alternative hypothesis is accepted. From ANOVA results it is observed that the data variability obtained using (R-Sq) model is 76.96% and 78.78% for both throughput and response time respectively.

The statistical analysis presented above shows that security protocols, traffic types, network load and packet size has a significant impact on the network performance. Though statistical results for throughput and response time are presented in this paper we have done statistical analysis of all parameters presented in Section 8. The obtained results in all the network scenarios in both roaming and non-roaming environments follow similar trends as observed in Section 6 for all the parameters. It is found that throughput and response time are in inverse proportion to each other. Null hypothesis in all cases is rejected and an alternative hypothesis is accepted as *p*-value is always less than the α-value and hence validates our experimental results.

10. Conclusion

In this paper, we have presented the comprehensive experimental results on the security performance of 802.11 standards of WLAN. An in-depth analysis has been performed to study the impact of various security layers on the network performance in terms of throughput, response time, encryption overheads, frame loss and jitter in different network scenarios.

Experimental results show that, policies 1 (SSID) provide very low level security, give better network performance as compared to all the security policies in all the network scenarios and is used as a reference for the comparative analysis with other security protocols. Complexity increases further in layers 2-5 (WEP 64/128, WPA/AES, WPA2/AES and WPA2/AES/TKIP) result in enhanced security with slightly more performance degradation. Performance degradation increases further on implementing higher security layers 6-9 (WPA/AES, WPA2/AES and WPA2/TKIP/AES with RADIUS server). But this fact is true only for two IEEE WLAN standards (IEEE 802.11b/g). In IEEE 802.11n performance degrades heavily with WEP 64/128. It is observed that performance in congested networks is more degraded than uncongested networks also security performance in the non-roaming network is better than the roaming network. Security protocols WPA/AES, WPA2/AES perform better than the policies WPA/TKIP and WPA2/TKIP. It reveals that depending on the network scenarios and the traffic types there is always a tradeoff between the security protocol and the associated network performance. We have found that at the MAC layer best tradeoff between security and network performance is achieved with security protocols P_{4-6} and with P_7 at the application layer for all the three WLAN standards. It is realized that due to this

tradeoff security protocols with higher strength may not always be the best choice for all the applications. Enterprise security layers provide more security than security protocols at the MAC layer but with more overheads. Therefore it is recommended that security protocols $P_{7–9}$ are to be used for the applications or the networks carrying more sensitive information. MAC layer security protocols are suitable for the applications where network performance is of great concern.

Also we have elaborated the RSSI model to evaluate the security strength associated with each security protocol. It is revealed that the security strength is not only dependent on the number of security services provided by each security protocol but it also depends on the strength of security services provided by the individual protocol. Statistical analysis of experimental data is also performed in this paper. We have also recommended the most robust security protocol against mobility in each network scenario under consideration. Overall the security protocols $P_{5–7}$ are providing the best tradeoff between robustness and mobility. On the comparison of the impact of secure wireless network on the three WLAN standards IEEE 802.11b/g/n it is found that in all the network scenarios IEEE 802.11n outperforms IEEE 802.11b/g.

In a nutshell, the experimental results presented in this paper recommend the most suitable security protocol in each network scenario. Also we have provided the quantitative analysis of the security strength and the overheads associated with each protocol. This comprehensive quantification can help the designers in developing a new and improving the existing security protocol. Designers can easily choose which security protocol can be implemented in a given network scenario while keeping a good tradeoff between security and overheads. Thus our experimental results provide valuable measurements which would be very useful in determining the best security policy and quality of service in future wireless networks. The comprehensive performance analysis reported in the paper may be used as reference for selecting the security policy for given applications or services required.

References

Agarwal, A.K., Wang, W., 2007. On the impact of quality of protection in wireless local area networks with IP mobility. Mob. Networks Appl. 12 (1), 93–110.

Ahmad, M., Taj, S., Mustafa, T., Asri, M., 2012. Performance analysis of wireless network with the impact of security mechanisms. In: The International Conference on Emerging Technologies, IEEE, pp. 1–6.

Baghaei, N., Hunt, R. IEEE 802.11 wireless LAN security performance using multi-clients. In: Proceedings of the 12th IEEE International Conference on Networks, vol. 1, November 2004, pp. 299–303.

Begh, G. R., Mir, A. H. 2009. Quantification of the effect of security on performance in wireless LANs. In: The Third International Conference on Emerging Security Information, Systems and Technologies, , IEEE, pp. 57–62.

Bhatia, V., Gupta, D., Sinha, H. P. 2013. Impact of security algorithms on various performance metrics of wireless LAN. In: Proceedings of the World Congress on Engineering, vol. 2.

Bhoyar, R., Ghonge, M., Gupta, S., 2013. Comparative study on IEEE standard of wireless LAN/Wi-Fi 802.11 a/b/g/n. Int. J. Adv. Res. Electron. Commun. Eng. (IJARECE) 2 (7).

Boulmalf, M., Barka, E., Lakas, A., 2007. Analysis of the effect of security on data and voice traffic in WLAN. Comput. Commun. 30 (11), 2468–2477.

Casola, V., Rak, M., Mazzeo, A., Mazzoccca, N. 2005. Security design and evaluation in a VoIP secure infrastructure: a policy based approach. In: Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on, vol. 1, pp. 727–732. IEEE.

Chen, J., Zeng, H., Hu, C., Ji, Z., 2011. Optimization between security and delay of quality-of-service. J. Network Comput. Appl. 34 (2), 603–608.

Ergen, M. 2002. IEEE 802.11 Tutorial. University of California Berkeley, 70. Ethereal, <http://www.ethereal.com/>.

Farkas, K., Wellnitz, O., Dick, M., Gu, X., Busse, M., Effelsberg, W., Serpanos, D.N., 2006. Real-time service provisioning for mobile and wireless networks. Comput. Commun. 29 (5), 540–550.

Feng, P. 2012. Wireless LAN security issues and solutions. In: Robotics and Applications (ISRA), 2012 IEEE Symposium on (pp. 921–924). IEEE.

Hayajneh, T., Khasawneh, S., Jamil, B., Itradat, A. 2012. Analyzing the impact of security protocols on wireless LAN with multimedia applications. In: SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies, pp. 169–172.

Holt, A., Huang, C. Y. 2010. 802.11 wireless networks: security and analysis, Springer. <http://www.intel.com/support/wireless/wlan/4965agn/sb/cs-025643.htm>.

Jindal, P., Singh, B., 2013. Performance evaluation of security-throughput tradeoff with channel adaptive encryption. Int. J. Comput. Network Inform. Secur. 5 (1).

Kolahi, S.S., Li, P., Argawe, M., Safdari, M. 2012. WPA2 security-bandwidth trade-off in 802.11 n peer-peer WLAN for IPv4 and IPv6 using Windows XP and Windows 7 operating systems. In: Computers and Communications (ISCC), 2012 IEEE Symposium on (pp. 000575–000579). IEEE.

Lashkari, A.H., Danesh, M.M.S., Samadi, B. 2009. A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i). In: Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on (pp. 48–52). IEEE.

Likhar, P., Yadav, R.S., 2011. Securing IEEE 802.11g WLAN using open VPN and its impact analysis. Int. J. Network Secur. Appl. (IJNSA) 3 (6), 97–113.

Liu, Y., Jin, Z., Wang, Y. 2010. Survey on security scheme and attacking methods of WPA/WPA2. In: Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on (pp. 1–4). IEEE.

Luo, A.A., Lin, C., Wang, K., Lei, L., Liu, C., 2009. Quality of protection analysis and performance modeling in IP multimedia subsystem. Comput. Commun. 32 (11), 1336–1345.

Mitchell, C.H.J.C. 2005. Security analysis and improvements for IEEE 802.11 i. In: The 12th Annual Network and Distributed System Security Symposium (NDSS'05) Stanford University, Stanford, pp. 90–110.

Nayak, D., Phatak, D.B., Gulati, V.P., 2005. Modeling and evaluation of security architecture for wireless local area networks by indexing method: a novel approach. In: Information Security Practice and Experience. Springer, Berlin, Heidelberg, pp. 25–35.

Ong, C.S., Nahrstedt, K., Yuan, W. 2003. Quality of protection for mobile multimedia applications. In: Multimedia and Expo, 2003. ICME'03. Proceedings. 2003 International Conference on (Vol. 2, pp. II-137). IEEE.

Peteriya, P.K., 2012. A pragmatic study on different stream ciphers and on different flavors of RC4 stream cipher. Int. J. Comput. Sci. Network Secur. 12 (3).

Potlapally, N.R., Ravi, S., Raghunathan, A., Jha, N.K., 2006. A study of the energy consumption characteristics of cryptographic algorithms and security protocols. Mob. Comput. IEEE Trans. 5 (2), 128–143.

Sheldon, F.T., Weber, J.M., Yoo, S.M., Pan, W.D., 2012. The insecurity of wireless networks. Secur. Privacy IEEE 10 (4), 54–61.

Singh, U., Jindal, P. 2014a. Performance analysis of secure wireless local area network using test-bed. In: Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on (pp. 386–389). IEEE.

Singh, U. Jindal, P. 2014b. Impact of transmission power on the performance of secure wireless local area network. Engineering and Systems (SCES), 2014 Students Conference on, vol., no., pp. 1–6, 28–30 May 2014, doi: 10.1109/SCES.2014.6880056.

Turab, N., Moldoveanu, F. 2008. The impact of various security mechanisms on the WLAN performance. Series C, vol. 70, no. 4.

Vibhuti, S. 2008. IEEE 802.11 WEP Wired Equivalent Privacy Concepts and Vulnerability. Accessed on, 29. <www.minitab.com>.