International Journal of Electronics and Communication Engineering (IJECE)
ISSN 2278-9901
Vol. 2, Issue 2, May 2013, 1-8
© IASET

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

IMPLEMENTING COMPARATIVE ANALYSIS OF WIRELESS LAN SECURITY PROTOCOLS IN NS2

VINAY BHATIA[1], DUSHYANT GUPTA[2] & H. P. SINHA[3]

[1,3]Department of Electronics & Communication Engineering, M.M. University, Mullana, India

[2]Department of Electronic Science, University College, Kurukshetra University, Kurukshetra, India

ABSTRACT

Wireless technology continues to play an emergent role in modern networks. Nowadays wide variety of wireless devices having various features is available for the users at competitive costs. This paper focuses on analytical study of one of the widely used networks, namely Wireless Local Area Network (LAN). There has been a tremendous increase in use and installation of wireless LANs these days. It is anticipated that the number of these LAN networks will increase further in the years to come. However, with the widespread utility of networks, security and performance has still been a bottleneck while communicating over wireless LANs. In this work, we have carried out a comparative study of throughput of wireless LANs implementing different security algorithms. Specifically performance analysis in terms of throughput is done, suiting Small-Office-Home-Office (SOHO) networks when WEP and WPA security algorithms are employed. In addition a complete analysis has also been done for these networks having different number of nodes.

KEYWORDS: Security, SOHO, Throughput, Wireless LAN, WEP, WPA

INTRODUCTION

The ubiquity of wireless networks is attributed mainly to the mobility that has been offered by these networks. Besides this, the wireless networks are characterized by flexibility, ad hoc connections and an unblended networking. Wireless LANs are the networks which inherit all these attributes of wireless networks so as to come up with their realistic use. A wireless LAN allows seamless networking without the need of entangled network of wires thereby providing mobility to the users. As a result large numbers of wireless LAN networks have cropped-up in past few years [1]. Although wireless LAN offers more advantages as compared to the wired counterpart, since data transfer is on air, its performance and security is compromised. Hence these parameters are of great concern which needs to be analyzed. In this paper we have tried to analyze the performance of wireless LANs in terms of throughput for different security protocols that are in practice these days. We have specifically implemented WEP and WPA security protocols in simulated wireless LANs using NS2. Various wireless LAN set-ups, pertaining to SOHO networks such that each set-up employs a different number of nodes have been analyzed using the results so computed by simulations.

WIRELESS SECURITY PROTOCOLS

Wired Equivalent Privacy

With an objective to bridge the breach between wireless usage and the security offered by wireless LAN, WEP standard was developed by the 802.11b task force in 1997 to protect 802.11 networks from wireless threats [1]. WEP was available in two modes: personal and enterprise. In the personal mode plain text is encrypted by a key which comprises of 40 bit pre-shared key and 24 bit initialization vector. The key is expanded to a sequence using pseudo random number generator. This sequence is used to encrypt the plain text. The encryption is accomplished with the use of RC4. RC4 is not specifically dedicated to WEP but is an algorithm being implemented in cryptography successfully. Another feature of

WEP is the Integrity Check that ensures that the packets are not altered during the transmission. This is accomplished using CRC-32 algorithm that generates an Integrity Check Value which is sent along with the plain text. Finally the initialization vector is concatenated with the encrypted key and transmitted [2].

At the receiver side the pre-shared key is used to extract the encrypted sequence and new Integrity Check Value is obtained. This value is used to decide whether the achieved text is valid or not. Since the key is shared between the sender and the receiver, it provides an opportunity with an attacker to extract the same. Thus security of the network becomes compromised. In addition WEP suffers from other weaknesses too which causes it to be more vulnerable to various types of attacks [3-7]. Despite its vulnerable nature WEP continues to be used in residential as well as commercial networks [8].

Although in enterprise mode, number of variants have been were produced namely, WEP2, e-WEP and WEP plus; still they have not been able to restrict the major attacks against wireless LAN encrypted with WEP [4, 6, 9]. Due to the problems being associated with WEP, IEEE recommended both manufacturers and users to stay away from WEP and better to prefer WPA for its being stronger and with resilient encryption.

Wi-fi Protected Access (WPA)

Since various security limitations were posed by WEP, the Wi-Fi Alliance discovered Wi-Fi Protected Access (WPA) [3]. WPA was also made available in two modes: personal and enterprise. The personal WPA or WPA-PSK (Pre-Shared Key) is used for SOHO networks and is targeted for domestic use. Personal WPA does not use any authentication server and the data cryptography key can go up to 256 bits. Another improvement which WPA offers over WEP is that any alphanumeric string can be used to negotiate the initial session with the Access Point (AP) [10]. Since both the client and the AP already possess this key, WPA provides mutual authentication, and the key is never transmitted over the air. WPA uses more complex encryption technology than WEP called Temporal Key Integrity Protocol (TKIP) which facilitates pre-packet key mixing and a message integrity check [5, 11].

TKIP utilizes a longer encryption key than WEP employing a forty-bit key which is relatively weak even when properly implemented. In addition it is supported by Message Integrity Check (MIC) which helps in contesting bit flipping attack, to which WEP can be easily be subjected to. The Enterprise mode uses Remote Authentication Dial In User Service (RADIUS) for authentication [5]. Here the RADIUS server puts a check that whether the information is correct while authentication scheme called Extensible Authentication Protocol (EAP) is processing the information. RADIUS is the de facto standard for authentication and other protocols are being rarely used. WPA2 made further changes to WPA by making Advanced Encryption Standards (AES) encryption mandatory and using Counter Cipher Mode Protocol (CCMP) in place of MIC for integrity check.

Modeling Throughput

Throughput for a wireless network depends on number of dependent and independent factors. Therefore several models have been developed to bring out behavior of wireless networks. Some of the models describe the variation of throughput in a wireless network when nodes are fixed [12], while in some the nodes are in motion [13] while formulating the throughput model. For an error-free acknowledgment, AGWN (Additive Gaussian White Noise) channel with a Signal to noise ratio SNR, the throughput for j^{th} mode in physical channel is given by [14]

$$T_p(j) = \frac{n_b.L_p}{L_p + h_j} r_j.r_{ps}^j(n_p, L_p, SNR).$$

Where n_b is number of bits per symbol, L_p is payload, h_j is header overhead, r_j rate of flow for the j[th] node and r_{ps}^{j} is packet success rate for jth node. We have utilized the NS2 network simulator for simulation of different security protocols. Therefore the Xgraph utility of NS2 is utilized to calculate the throughput using the awk file.

SIMULATION RESULTS FOR WEP

This section deals with results obtained when the security algorithm is WEP employing different number of nodes. The results so obtained are plotted using X-graph utility in NS2. Figure 1 shows the variation in throughput when 10 number of nodes have been considered for the wireless LAN. As inferred from the plot in Figure 1, the throughput initiates 10 second after commencement of the simulation. After initial connection set-up phase, the nodes start moving in different directions due to which the throughput initially drops down then rises steadily with a small slope. Reasonable throughput levels have been achieved at simulation time of 20 seconds with peak performance lying between 40 to 50 seconds. The average throughput during the complete simulation is found to be 419.02 Kbps.

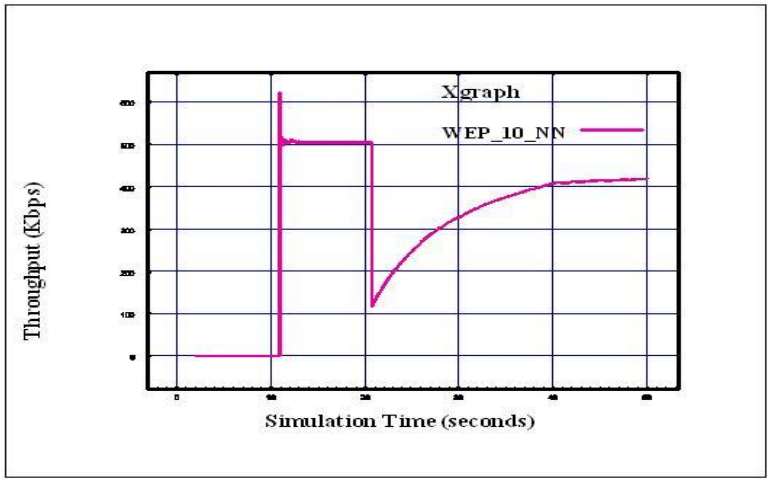

Figure 1: Variation of Throughput for WEP Protocol in WLAN of 10 Nodes

Similarly when numbers of nodes in wireless LAN are considered to be 20, the variation can be plotted as shown in Figure 2. In this case, the average throughput during the complete simulation comes out to be 425.01Kbps.

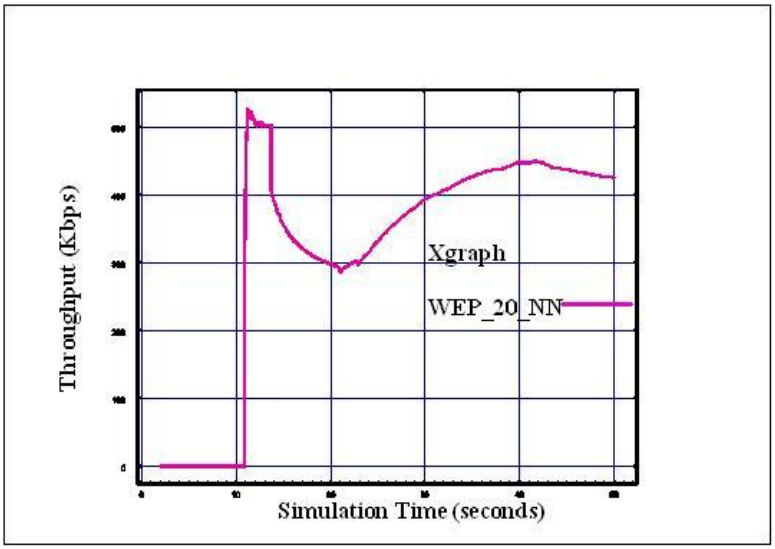

Figure 2: Variation of Throughput for WEP Protocol in WLAN of 20 Nodes

Finally, we consider a SOHO network comprising of 30 nodes using WEP as a security algorithm. Total simulation time taken is 50 seconds and all nodes are wirelessly connected to each other. The variation is plotted as given in Figure 3 where it is noticed that the throughput increases steadily after 25 seconds of simulation time and the average value for this simulation is computed as 425.06 Kbps.

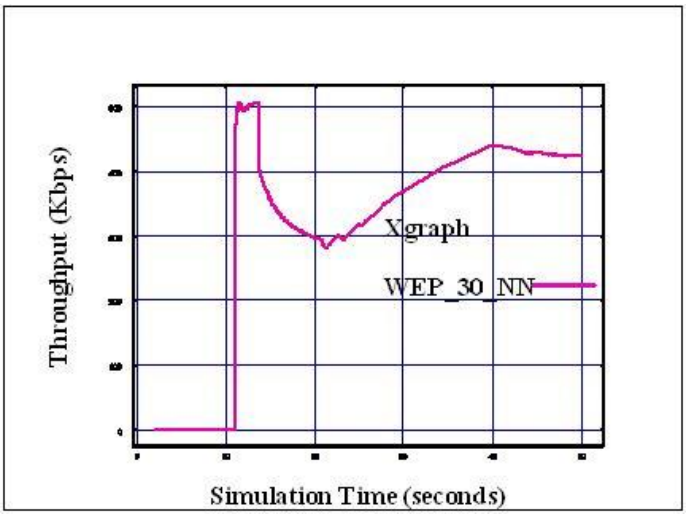

Figure 3: Variation of Throughput for WEP Protocol in WLAN of 30 Nodes

SIMULATION RESULTS FOR WPA

In this section, the results have been computed for WPA security algorithm, employing different number of nodes. The results obtained are plotted using X-graph utility in NS2. Figure 4 shows the variation in throughput when the scenario comprises of 10 numbers of nodes. Figure 4 illustrates similar variation as has been computed in case of a wireless LAN set-up comprising 10 nodes while employing WEP as the security algorithm with a differentiation that there is a decrease in throughput. The average value of the throughput in this case has been computed as 339.23 Kbps.

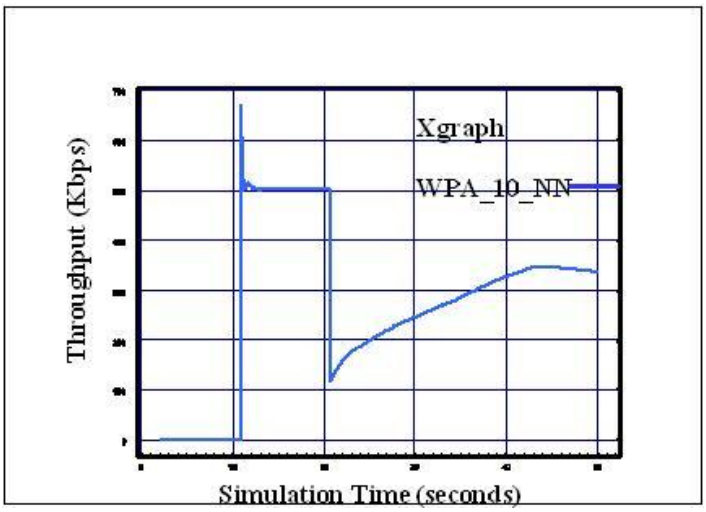

Figure 4: Variation of Throughput for WPA Protocol in WLAN of 10 Nodes

Similarly when numbers of nodes have been considered of double the value, i.e., 20, the variation with respect to throughput being computed has been depicted in Figure 5.

As seen from Figure 5 the variation in throughput for WPA is similar as that of WEP but again a dip is seen in the throughput, with an average throughput of 407.8 Kbps.

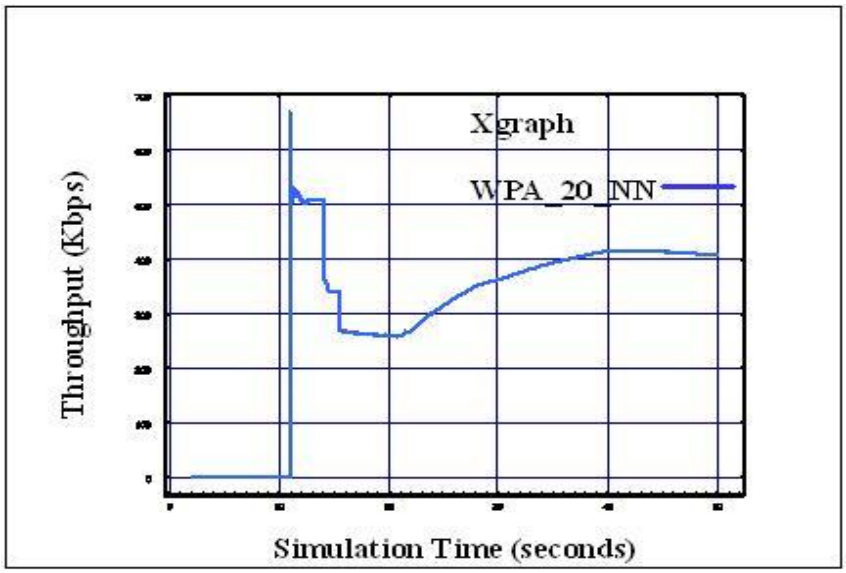

Figure 5: Variation of Throughput for WPA Protocol in WLAN of 20 Nodes

Finally, a SOHO network is considered comprising 30 nodes while using security algorithm as WPA.

Here total simulation time is 50 seconds when all the nodes are assumed to be wirelessly connected to each other and the variation has been plotted as shown in Figure 6.

In this case too, a similar observations have been are observed; firstly variation in throughput for WEP and WPA are similar and then a dip is observed for WPA protocol.

The average throughput for this set-up is found to be 359.8 Kbps.

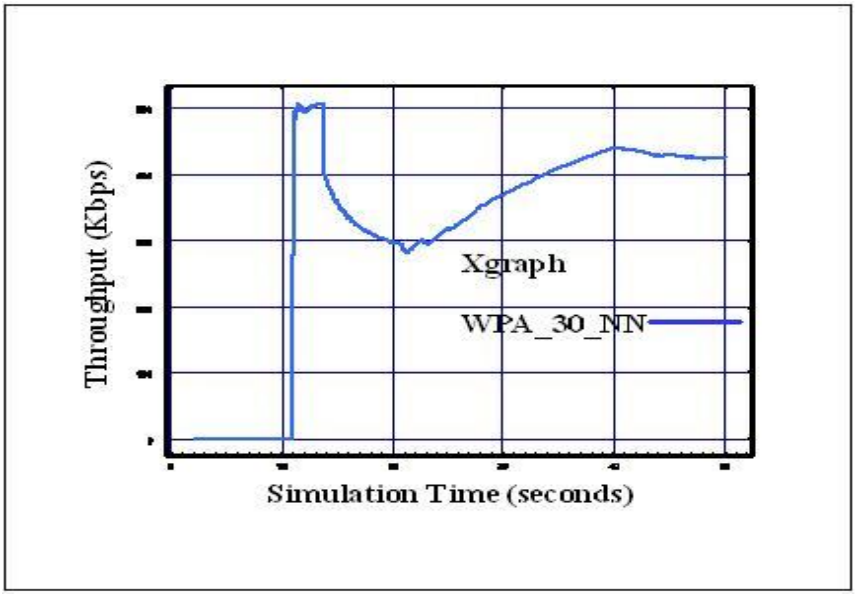

Figure 6: Variation of Throughput for WPA Protocol in WLAN of 30 Nodes

COMPARATIVE ANALYSIS

In this section, for a given number of nodes, we have tried to compare the analytical results that are being computed for two different security algorithms and have been drawn by utilizing the X-graph utility of NS2.

Figure 7 depicts the comparison when number of nodes is 10 but for two different security algorithms.

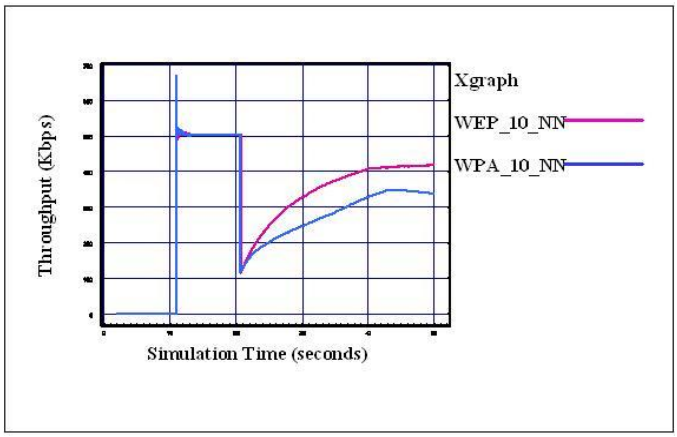

Figure 7: Throughput Comparison of WPA and WEP for 10 Nodes

Similarly for a case when the numbers of nodes are set as 20, the comparative variation of throughputs in wireless LANs, employing WEP and WPA has been depicted in Figure 8.

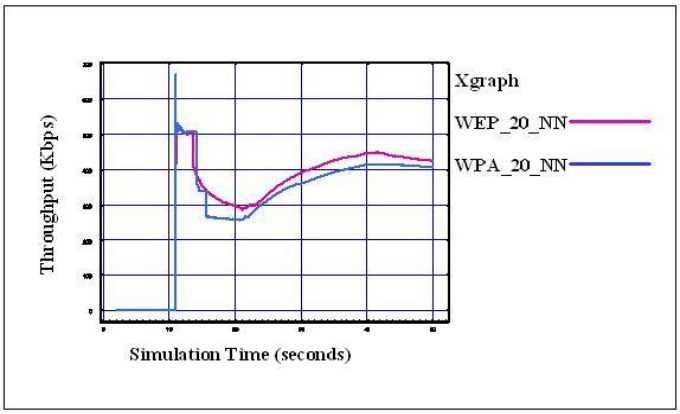

Figure 8: Throughput Comparison of WPA and WEP for 20 Nodes

As observed from Figure 7 and Figure 8 the variation in the throughput is almost similar in each case, but the throughput magnitude is greater for WEP than WPA for two sets of number of nodes.

Finally, we have compared the throughput for a SOHO network comprising of 30 nodes using WEP as well as WPA as a security algorithm. Here total simulation time comes out to be 50 seconds and all nodes assumed to be wirelessly connected to each other and the variation so plotted has been depicted in Figure 9.

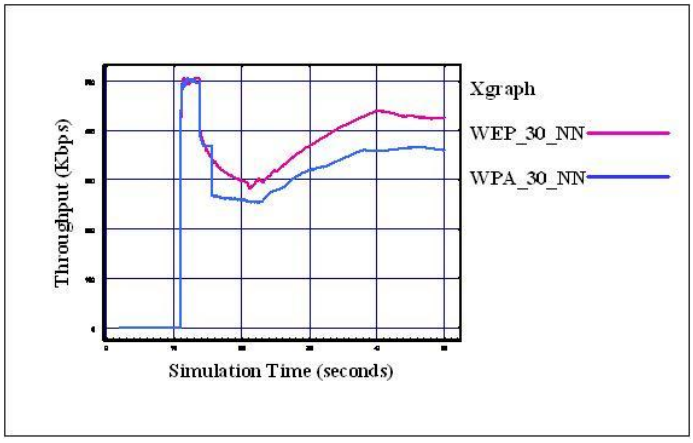

Figure 9: Throughput Comparison of WPA and WEP for 30 Nodes

It has been analyzed that the observation is consistent; the throughput variations are similar but magnitude is more for WEP than WPA. Table.1 lists the average throughputs during simulation for the three different cases of number of nodes as 10, 20 and 30.

Comparison of Average Throughput

Number of Nodes	WEP	WPA
10	419.02	339.23
20	425.01	407.8
30	425.06	359.8

These values are plotted in Figure 10 for analysis.

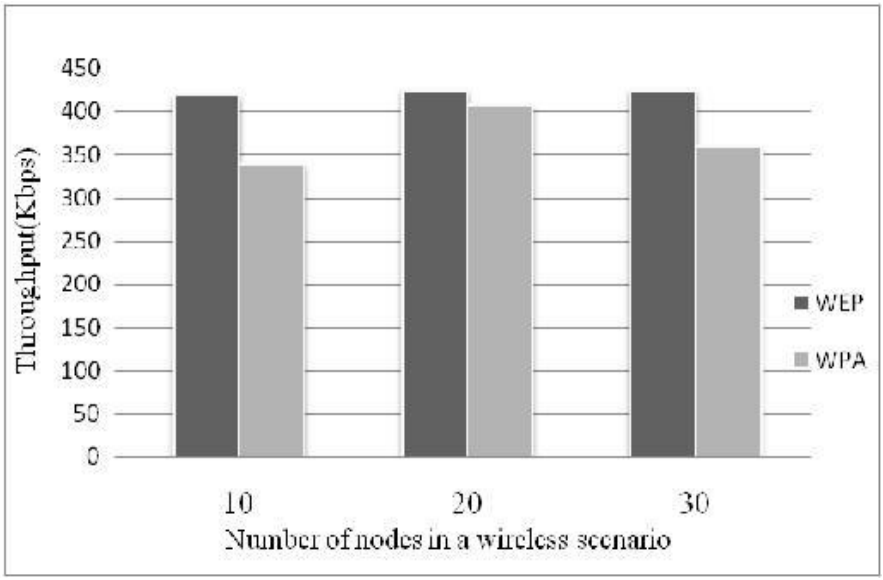

Figure 10: Throughput Comparison of WPA and WEP for 30 Nodes

Figure 10 has been plotted as a throughput comparison which shows that the average throughput decreases in each of the cases when WEP is replaced by WPA for security. Thus security has to be compromised for better throughput and vice-versa.

CONCLUSIONS

Thus the simulation results help us to compare performance versus security of a wireless LAN. As discussed the security provided by WPA algorithm is better for SOHO networks but at the cost of poorer performance. It is further concluded that for a small LAN usually practiced at homes or small offices with number of nodes restricted to 30, the throughput decreases when WEP is replaced by WPA.

REFERENCES

1. K. J. Hole, E. Dyrnes, P. Thorsheim, “Securing Wi-Fi networks,” IEEE Computer journals & magazines, Digital Object Identifier: 10.1109/MC.2005.241, Volume: 38, Issue: 7, pp 28 – 34, 2005.
2. J. S. Park, D. Dicoi, “WLAN security: current and future,” IEEE Internet Computing, Digital Object Identifier: 10.1109/MIC.2003.1232519, Volume: 7, Issue: 5, pp 60 – 65, 2003.

3. H. Feil, “802.11 wireless network policy recommendation for usage within unclassified government networks,” IEEE Military Communications Conference, MILCOM '03, Digital Object Identifier: 10.1109/MILCOM.2003.1290220, Volume: 2, pp 832 - 838, 2003.

4. Zhang Longjun, Zou Tao, “An Improved Key Management Scheme for WEP,” IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC '08, Digital Object Identifier: 10.1109/EUC.2008.67, Volume: 2 , pp 234 - 239, 2008.

5. C. Maple, H. Jacobs, M. Reeve, “Choosing the right wireless LAN security protocol for the home and business user,” The First International Conference on Availability, Reliability and Security, ARES 2006. Digital Object Identifier: 10.1109/ARES.2006.42, 2006.

6. V. Bhatia, D. Gupta and H.P Sinha, “Analysis of dictionary attacks on different number of nodes”, Journal of Information Systems and Communications, ISSN0976-8742, Volume: 3, Issue: 1, Page(s): 167-169, 2012.

7. V. Bhatia, D. Gupta and H.P Sinha, “Throughput and Vulnerability Analysis of an IEEE 802.11b Wireless LAN”, International Journal of Computer Applications Digital Object Identifier: 10.5120/8182-1509, Volume 52, Number 3, Pages 21-26, 2012.

8. F.C.C. Osorio, “State of wireless security implementations in the United States and Europe - empirical data,” 3rd IEEE International Conference on Malicious and Unwanted Software, MALWARE 2008, Digital Object Identifier: 10.1109/MALWARE.2008.4690863, pp 594 - 599, 2008.

9. H. R. Hassan, Y. Challal, “Enhanced WEP: An efficient solution to WEP threats,” Second IFIP International Conference on Wireless and Optical Communications Networks, WOCN 2005, Digital Object Identifier: 10.1109/WOCN.2005.1436095, pp 92 - 97, 2005.

10. A. H. Lashkari, M. Mansoor, A. S. Danesh, “Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA),” 2009 IEEE International Conference on Signal Processing Systems, Digital Object Identifier: 10.1109/ICSPS.2009.87, pp 445 - 449, 2009.

11. B. Potter, “Wireless security's future,” IEEE Security & Privacy, Digital Object Identifier: 10.1109/MSECP.2003.1219074, Volume: 1 , Issue: 4 pp 68 - 72, 2003.

12. P. Gupta, P, P.R. Kumar, “The capacity of wireless networks” IEEE/ACM Transactions on Information Theory, Volume: 46, Issue: 2, Digital Object Identifier: 10.1109/18.825799, pp 388 - 404, 2000.

13. M. Grossglauser, D.N.C. Tse, “Mobility increases the capacity of ad hoc wireless networks” IEEE/ACM Transactions on Networking, Volume: 10, Issue: 4, Digital Object Identifier: 10.1109/TNET.2002.801403, pp 477- 486, 2002.

14. M. Ekpenyong, J. Isabona, “Modeling Throughput Performance in 802.11 WLAN”, International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, pp 16 - 22, 2010.