

## Throughput and Delay Analysis of Wireless LAN Security Protocols Implementing NS2

**Vinay Bhatia and Dushyant Gupta**

*Department of Electronics and Communication Engineering  
Baddi University of Emerging Sciences and Technology  
Baddi, H.P, INDIA*

*[vinay4research@yahoo.com](mailto:vinay4research@yahoo.com)*

*Department of Electronics and Communication Engineering  
G.J. University of Science and Technology  
Hissar, Haryana, INDIA  
[gupty2kuk@yahoo.co.uk](mailto:gupty2kuk@yahoo.co.uk)*

### Abstract

Recent years have witnessed tremendous increase in the use of wireless LANs. However, with increase in popularity of WLANs, security has always been a key issue that has led to the development of various security algorithms like, WEP, WPA, etc. Analyzing the performance metrics of such algorithms has also been a prime concern for WLANs. While test-bed analysis has been done by some researchers for some security algorithms with only a few numbers of nodes, in practice a WLAN comprises larger number of nodes. Keeping this in view, a simulation approach has been implemented in this study for a detailed analysis of throughput and end-to-end delay (EED) for WLANs equipped with different algorithms of WEP and WPA. A comparative analysis has also been carried out for these security algorithms on the basis of throughput and end-to-end delay parameters.

**Keywords**— Ad hoc networks;, Computer networks; Local area networks, Security; Wireless LAN

### I. INTRODUCTION

The wireless networks are characterized by flexibility, ad hoc connections and an unblended networking. However, the ubiquity of wireless networks is mainly attributed to the mobility that makes it more popular as compared to the wired counterparts. Wireless LANs are the most popular form of such networks which allow

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]. Since WLANs use radio waves, the data transfer is not limited to physical boundaries such as walls, floors and ceilings while also being prone to various types of attacks. Hence various security standards have been suggested by IEEE such as WEP and WPA to enhance the level of security but various performance metrics of these security algorithms are still not explored to substantial extent. In this paper an effort has been made to analyze the performance of wireless LANs in terms of throughput and end-to-end delay for different security protocols that are in practice these days. Here we have implemented different security protocols of WEP and its various variants namely WEP-40, WEP-104 and WEP-BGS along with WPA through NS2 in simulated wireless LANs comprising different number of nodes and have analyzed the simulated results. A comparative analysis of various security protocols with different number of nodes in a WLAN has also been carried out on the basis of these two parameters.

## II. WIRELESS SECURITY PROTOCOLS

### A. *Wired Equivalent Privacy*

The WEP standard was developed in 1997 by the 802.11b task force, to protect 802.11 networks from wireless threats with an objective to bridge the breach between wireless usage and the security offered by wireless LAN [1]. WEP uses a key having a 40-bit pre-shared key and a 24-bit initialization vector thus making the total key length of 64 bits. The expansion of the key into a sequence is accomplished using a pseudo random number generator. The sequence thus obtained is used to encrypt the plain text. RC4 is used for the encryption and CRC-32 is employed for the Integrity Check. Before transmission the initialization vector is concatenated with the encrypted key [2]. Although WEP is vulnerable to various types of attacks [3-6], owing to its easy implementation characteristic, WEP continues to be used in residential as well as commercial networks, despite its vulnerable nature [7]. Although, number of variants have been 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], [8-13]. Due to the problems being associated with WEP, IEEE recommended both manufacturers and users to prefer WPA for its being stronger and with resilient encryption. In this paper we have employed three variants of WEP in simulated WLANs viz. WEP-40 the original WEP, WEP-104 with key length increased to 104 bits and WEP-BGS, a WEP based algorithm where we have chosen key length matching with another protocol called WPA. Since throughput and delay are important parameters [14-16] which affect the performance of a WLAN, these are computed for each of the variant of WEP that would help in further analyzing the effect of key length on throughput as well as EED.

#### 1) *Algorithm of WEP*

$c\_sum \rightarrow C(m)$

$p\_text \rightarrow Cn(m, c\_sum)$

$k\_strm \rightarrow Cn(k, iv)$   
 $c\_text \rightarrow Xr(p\_text, k\_strm)$   
 $t\_text \rightarrow Cn(c\_text, iv)$

2) **Notations used**

$C()$  represents operation of CRC-32 algorithm

$Cn()$  represents concatenation

$Xr()$  represents XOR operation

$m$  represents message

$k$  represents secret key

$p\_text$  represents plain text

$c\_text$  represents cipher text

$iv$  represents initialization vector

$t\_text$  represents transmitted text

**B. Wi-Fi protected Access**

There are a number of security flaws that have been detected in WEP [3] on account of which the Wi-Fi Alliance discovered another security protocol known as Wi-Fi Protected Access (WPA). WPA is based on another much complex encryption technology called Temporal Key Integrity Protocol (TKIP) as has been shown in Fig. 1.

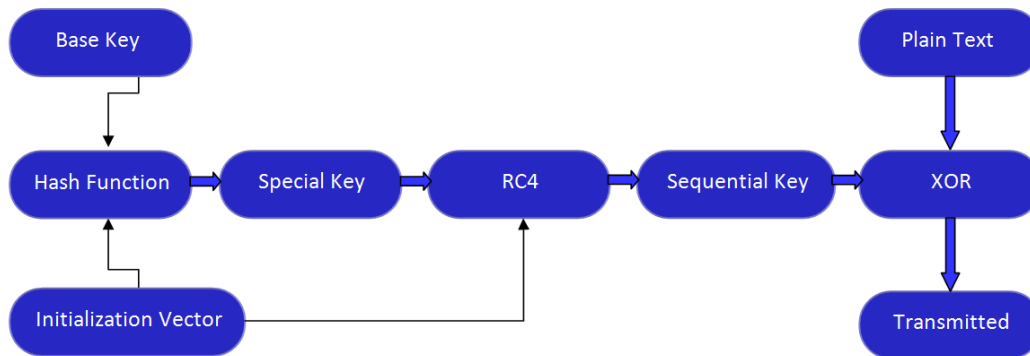


Fig. 1. **Encryption algorithm of WPA (TKIP)**

It is observed that TKIP uses RC4 like in WEP and also a hash function before the expansion of the key given by RC4 algorithm. The RC4 stream cipher used by WPA is a 128-bit per-packet key that dynamically generates a new key for each packet. In this process a duplicate initialization vector is first created so that one copy is hashed with the base key and the other one is used in the next step. The result produced by the hash function is then employed to generate a key which is concatenated to the copy of the initialization vector that forms the input to the RC4 algorithm. This results in formulation of a sequential key at the output of the RC4. In next step, sequential key is XORed with the plain text that generates the cipher text

which is finally transmitted. At the receiver, decryption process is just reverse of the above stated encryption process. WPA is also available in two modes: personal and enterprise. The personal WPA or WPA-PSK (Pre-Shared Key) is targeted for domestic use. Since both the client and the AP already possess this key, WPA provides mutual authentication, and the key is never transmitted over the air. The Enterprise mode uses Remote Authentication Dial In User Service (RADIUS) for authentication [5]. Since WPA is the successor of WEP and is used nowadays, variations of throughput and EED and their values for WPA enabled WLANs need to be evaluated so that performance of WPA can further be compared with other security algorithms.

### III. SIMULATION RESULTS

This section deals with the results being obtained when different security algorithm employing different numbers of nodes are used in WLANs. The results so obtained are plotted through X-graph utility in NS2. Since majority of WLAN users employ either WEP or WPA [14], analysis of performance of these security protocols needs to be explored. Although majority of researchers have performed the analysis using a test-bed approach which is limited to only a few number of nodes (usually two or three nodes) in a WLAN, but, practically, as WLAN comprises much larger number of nodes, an attempt has been made to analyze the security algorithms through a simulation approach, so that an extensive analysis of such security algorithms can be carried out and that too for varying number of nodes from 10 to 80. Since throughput and end-to-end delay are important performance metrics which have been used by number of researchers [17-20], they have been employed in this piece of research too. Thus for each of the four algorithms, viz., WEP-40, WEP-104, WEP-BGS and WPA we have simulated 8 WLANs having number of nodes 10, 20, 30, 40, 50, 60, 70 and 80. Further, the simulation might have been performed with some other software too but on account of various advantages of NS-2, viz., flexibility, scalability and faster in reflecting latest technologies, NS-2 has been found to be quite appropriate. However, implementing using NS-2 has been a great challenge for NS-2 being open source software and having been lack of formal documentation.

#### A. *Simulation Results for WEP-40*

Firstly, the case of a standard WEP called WEP-40 is considered. Here throughput and end-to-end delay have been considered as performance metrics. For simulation through NS-2, the time for all the simulations has been set as 50 seconds. Eight WLANs have been simulated with different sizes in terms of number of nodes and eight different variation graphs have been plotted using Xgraph utility of NS2.

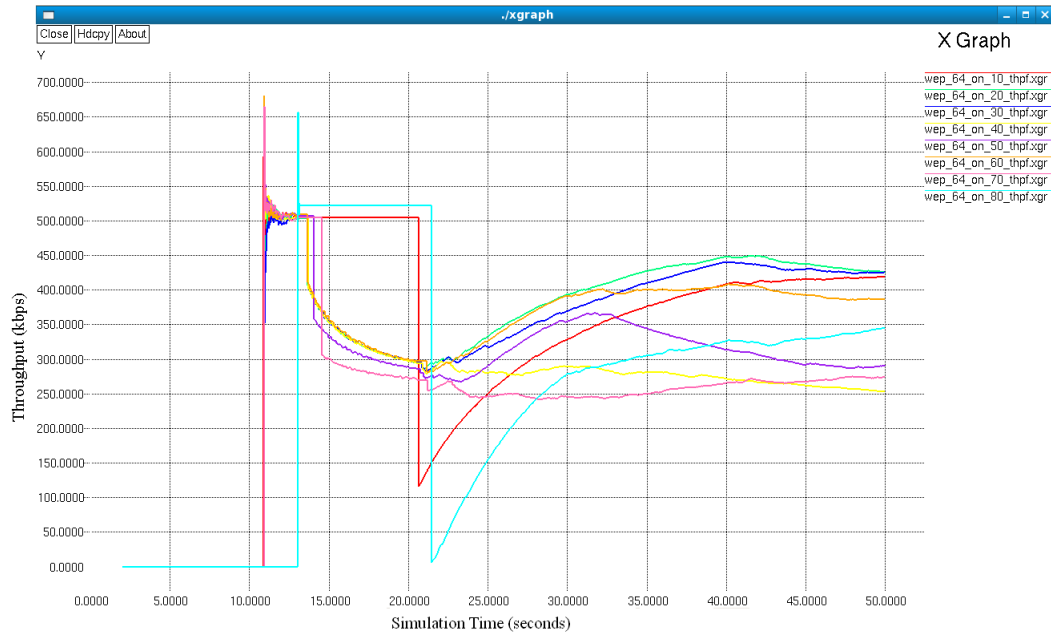


Fig. 2. **Xgraph for throughput variation for WEP-40 for different nodes**

For the sake of comparison, throughputs of WEP-40 for all combinations of nodes have been computed and plotted through Xgraph as shown in Fig. 2. It is observed that WLAN sets-up between initial 10 to 15 seconds, while during 15 to 25 seconds there is an abrupt change in the values of instantaneous throughput which may be accounted for initial connection-set up phase of the network. Beyond 25 seconds, the data packets are being transferred over the WLAN and thus the variations in the throughput attain a saturated value. Although after 25 seconds, the throughput is constant for a given number of nodes, there is difference in the saturated values for WLANs having different number of nodes. It is further observed that towards the end of simulation, the instantaneous throughput ranges from 250 to 450 kbps. When number of nodes is less, packets are expected to travel freely in the medium in comparison with the case when the number of nodes is 70 or 80 where the channel gets congested with the transfer of large number of data packets. Hence it can be concluded that WLANs, having lesser number of nodes have greater throughput. The average value of throughput for WLAN having 10, 20, 30, 40, 50, 60, 70 and 80 nodes in the network is found to be approx. 352.3 kbps.

In this part of the section, with the help of Xgraphs, end-to-end delay as a function of simulation time (seconds) has been studied for various number of nodes for WEP-40. The individual behavior of variation of EED for number of nodes being set as 10, 20, 30, 40, 50, 60, 70, 80 has been computed and plotted through NS-2 and has been depicted in Fig 3. The average EED for WEP-40 employing 10 nodes comes out to be approx. 42.469 ms; 40.417 ms for 20 nodes; 25.271 ms for 30 nodes; 57.094 ms for 40 nodes; 55.757 ms for 50 nodes; 54.0177 ms for 60 nodes; 61.111 ms for 70

nodes; 2067.125 ms for 80 nodes. The variations depict a common finding that EED increases stutteringly throughout the simulation for WLANs having different number of nodes. Since with increase in size of the WLAN (in terms of number of nodes) the network complexity in terms of data traffic increases, therefore for a large network the EED is higher.

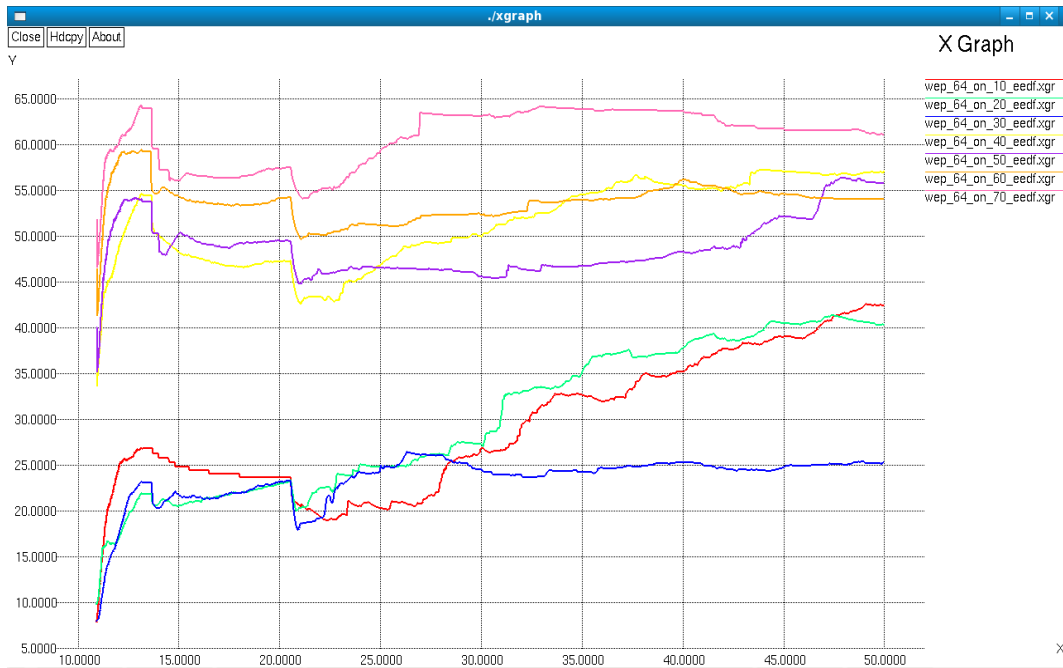


Fig. 3. Xgraph for EED variation for WEP-40 for different nodes

It is also reinforced from the Fig. 3 that there is marked difference in EED for small WLANs i.e 10, 20 or 30 nodes as their EED is less as compared to EED variations for larger WLANs. The mean EED for WEP-40 WLANs having 10, 20, 30, 40, 50, 60, 70 and 80 nodes in the network comes out to be approx. 300.408 ms.

#### B. Simulation Results for WEP-104

WEP-104 is another algorithm based on WEP that uses RC4 for encryption and CRC-32 for integrity check but with an increased key length of 104 bits instead of 40 bits as it was in case of WEP-40. The Initialization Vector is still of 24-bits, making the total key length of 128 bits. In Fig. 4, Xgraph showing throughput variations of WEP-104 for different number of nodes are plotted simultaneously.

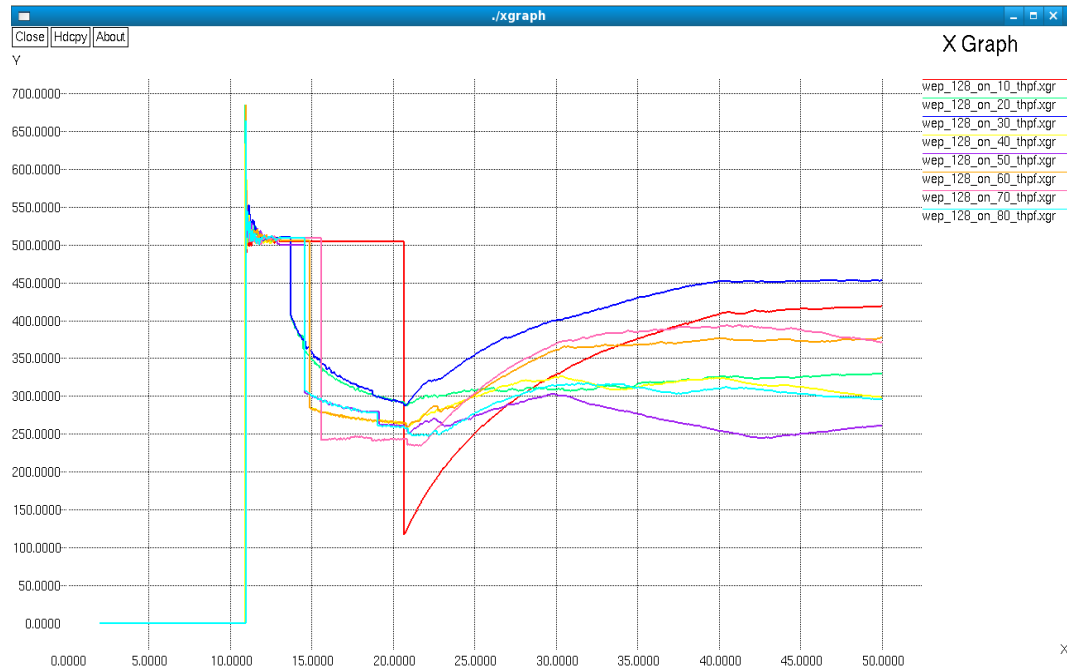


Fig. 4. **Xgraph for throughput variation for WEP-104 for various nodes**

The figure depicts that initial connection set-up occurs during the simulation time of  $t = 10$  s to  $t = 20$  s after which there is a steady rise in the throughput. Also it is noticed that instantaneous throughput ranges from 250 to 450 kbps towards the end of simulation. It is further noted that when the number of nodes is less for example, 10 or 30 throughput is more compared to large WLANs having 70 or 80 nodes. The mean throughput value for WEP-104 WLANs having 10, 20, 30, 40, 50, 60, 70 and 80 nodes in the network comes out to be approx. 350.45 kbps.

Now the other performance metric i.e EED is considered for WEP-104. Again eight WLANs have been simulated with different number of nodes and the EED variations are plotted on the Xgraph shown in Fig 5.

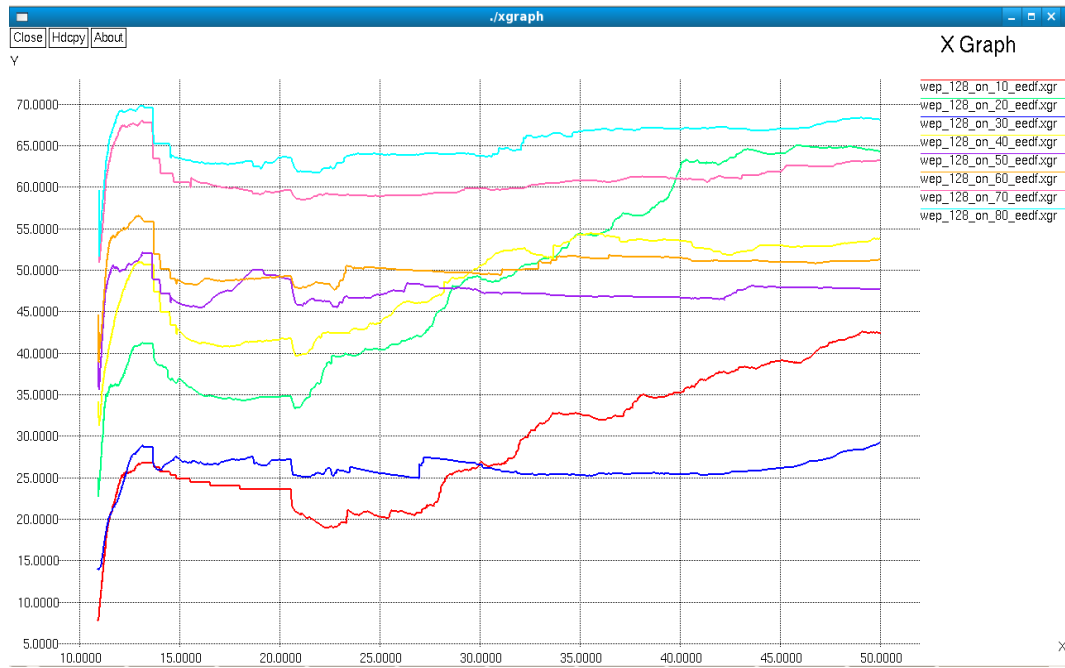


Fig. 5. Xgraph for EED variation for WEP-104 for various nodes

It is seen that the variations follow a common suit and the behavior is similar to that of WEP-40 as EED increases stutteringly throughout the simulation [Fig. 5]. Although with increase in size of the WLAN, the network complexity in terms of data traffic increases, due to which EED is expected to be higher in value for a large network. However, the size of the data packet also plays its own role. Since the size of packet is increased, the marked difference in EED between a small and a large WLAN is now reduced. It is also observed that graph for 20-node WLAN the graph intersects various other graphs, indicating that at some instances of simulation the EED for 20 nodes is equal to that of WLANs having more number of nodes. The mean EED for WEP-104 WLANs having 10, 20, 30, 40, 50, 60, 70 and 80 nodes in the network comes out to be approx. 52.495ms.

### C. Simulation Results for WEP-BGS

Here another security protocol has been suggested by the authors of this paper and have named it as WEP-BGS which is based on basic WEP algorithm and also uses RC4 for encryption and CRC-32 for integrity check except that the key length for this algorithm has been enhanced to 256 bits, contrary to 40-bits or 104-bits of WEP-40 and WEP-104, respectively. This key length matches the key length employed in another security algorithm, named Wi-Fi Protected Access (WPA).

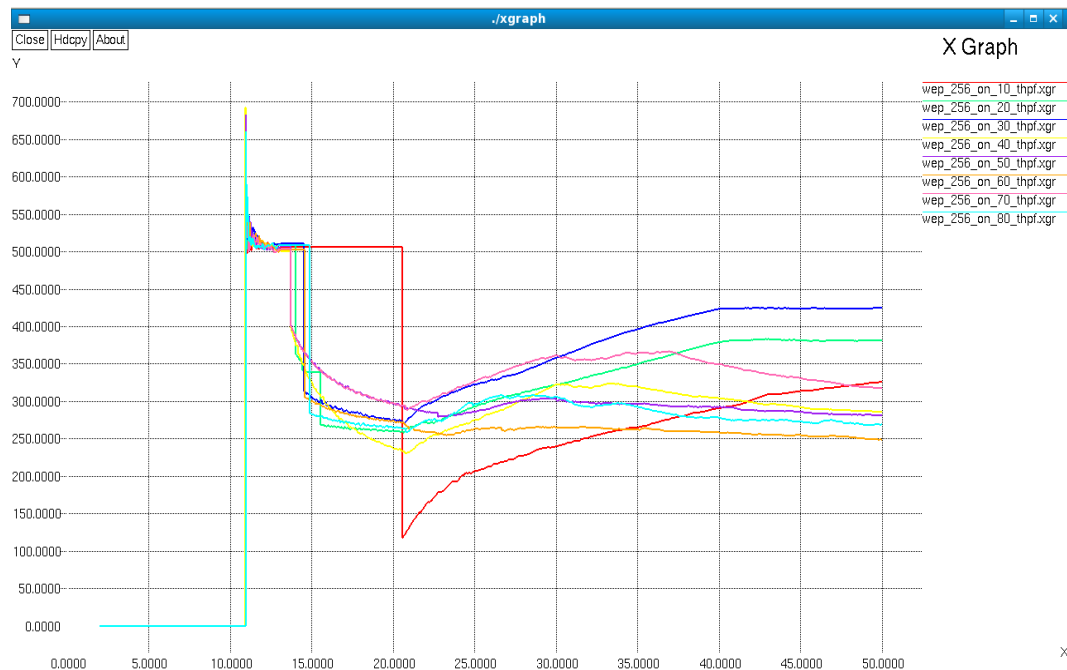


Fig. 6. **Xgraph for throughput variation for WEP-BGS for various nodes**

To study the variation in throughput in case of WEP-BGS for different number of nodes, the X-graph has been plotted [Fig. 6]. It is observed from the plot that network sets up till  $t = 20$  seconds but once it has been accomplished then all the variations have a common profile as they increase steadily after start of data transfer. The throughput variations obtained here are also similar to those obtained for WEP-40 or WEP-104 as in this case too, towards the end of simulation the instantaneous throughput ranges from 250 to 450 kbps and for 20 or 30 node-WLAN throughput is more compared to large WLANs having 70 or 80 nodes. The mean of average throughputs for WEP-BGS enabled WLAN having 10, 20, 30, 40, 50, 60, 70 and 80 nodes in the network is computed to be 316.469 kbps.

Now in Fig. 7, a Xgraph for end-to-end delay variations of WEP-BGS for different number of nodes has been plotted. Here although the variations are varying stutteringly in each case, their average values are different with corresponding values obtained for WEP-40 or WEP-104.

As it has been observed earlier, there is a marked gap in EED variations between a small and a large WLAN (in terms of number of nodes) for WEP-40 [Fig. 3]. Similarly EED variation Xgraph for WEP-104 as noticed in Fig. 5 also shows that there is a difference in small as well as large WLAN.

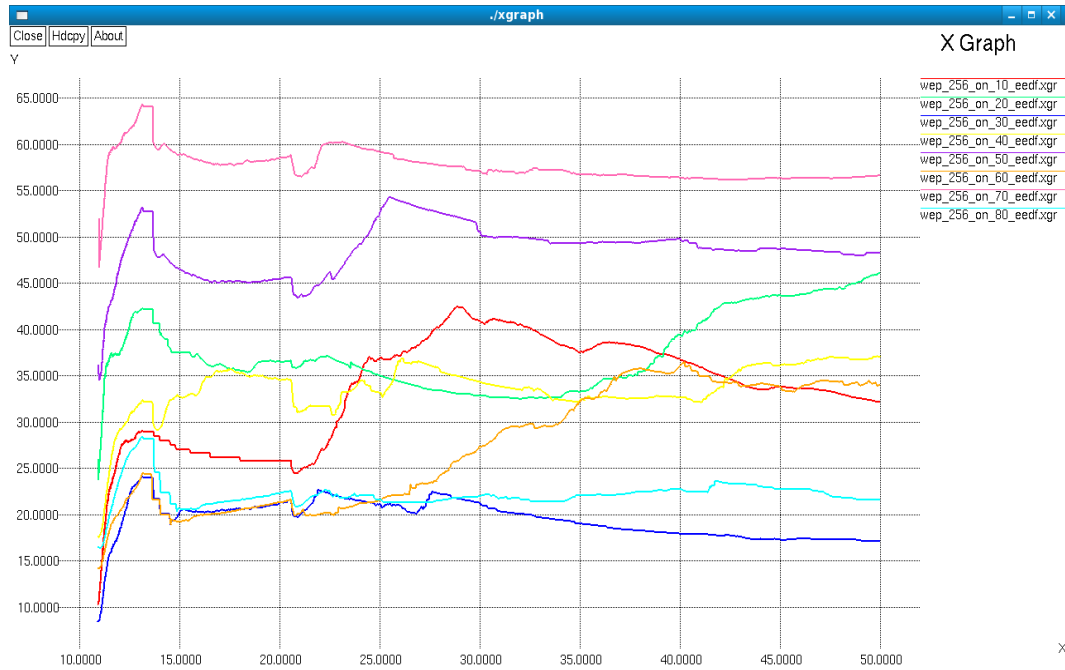


Fig. 7. **Xgraph for EED variation for WEP-BGS for various nodes**

However, in case of WEP-BGS, the difference in EED is almost negligible as has been depicted in Fig.7. Thus EED has been found to depend not only on the size of the WLAN but also on the length of the key. Moreover, as length of the key increases, its effect supersedes the effect of increase in number of nodes as depicted in Fig. 7. This accounts for the decrease in gap for small and large WLAN in case of WEP-BGS. The mean value of EED for WEP-BGS enabled WLAN having 10, 20, 30, 40, 50, 60, 70 and 80 nodes in the network has been computed as 36.63 ms.

#### IV. SIMULATION RESULTS FOR WPA

In this section, the simulations for WPA security algorithm have been carried out, employing different number of nodes. The results so obtained have been plotted through X-graph utility in NS2. The average value of throughput for WLAN enabled with WEP-BGS while having the number of nodes as 10, 20, 30, 40, 50, 60, 70 and 80 nodes in the network has been computed as 302.29 kbps and a combined Xgraph has also been plotted as shown in Fig. 8.

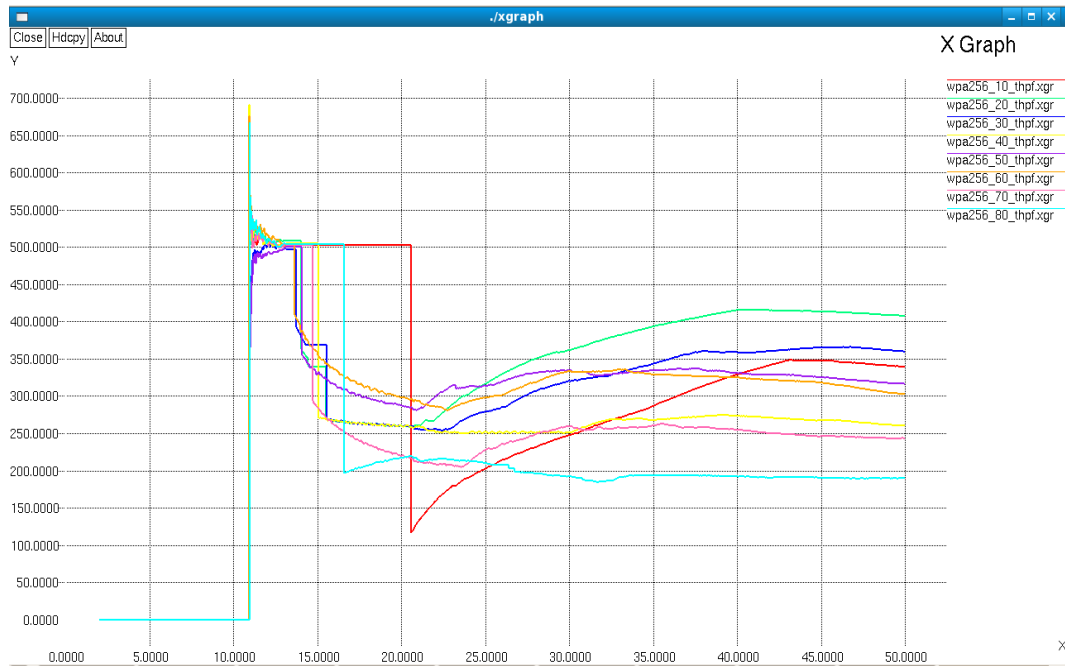


Fig. 8. **Xgraph for throughput variation for WPA for different nodes**

It is observed that WLAN sets-up during initial 10 to 15 seconds, while during 15 to 25 seconds; there is an abrupt change in the values of instantaneous throughput which may be accounted for initial connection-set up phase of the network. Beyond 25 seconds, the data packets are being transferred over the WLAN and thus the variations in the throughput attain a saturated value. Although after 25 seconds, the throughput tends to become constant for a given number of nodes, there is difference in the saturated values for WLANs having different number of nodes. It is further observed that towards the end of simulation, the instantaneous throughput ranges from 200 to 400 kbps. When number of nodes is less, packets are expected to travel freely in the medium in comparison with the case when the number of nodes is 70 or 80 where the channel gets congested with the transfer of large number of data packets. Hence it can be concluded that WLANs, having lesser number of nodes have greater throughput.

Now a comparison of EED variation obtained for various numbers of nodes in a WLAN is plotted through a combined Xgraph, as shown in Fig. 9. The graphs depict a common finding that EED increases stutteringly throughout the simulation for WLANs having different number of nodes. Although with increase in size of the WLAN (in terms of number of nodes) the network complexity in terms of data traffic increases, due to which EED is expected to be higher in value for a large network.

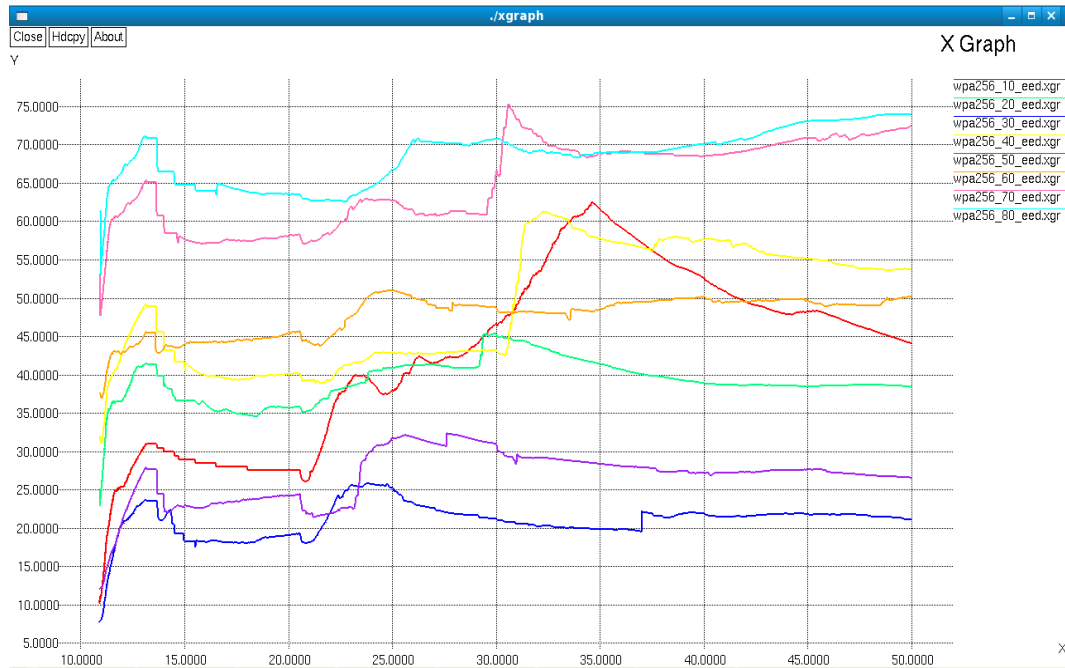


Fig. 9. **Xgraph for EED variation for WPA for different nodes**

However, the size of the data packet also plays its own role. As the size of packet is increased, the marked difference in EED between a small and a large WLAN (in terms of number of nodes) is reduced. It is also observed that various graphs intersect each other, indicating that at some instances of simulation the EED for different nodes is equal. The mean EED for WEP-104 WLANs having 10, 20, 30, 40, 50, 60, 70 and 80 nodes in the network comes out to be approx. 47.555 ms.

## V. COMPARATIVE ANALYSIS

Finally, a comparison of various simulation results that have been computed for four different security algorithms has been computed. Firstly, the mean throughput values for different security algorithms have been computed and depicted in Fig. 10 and it is observed that the throughput values of all the WEP protocols based algorithms are comparatively much higher than the throughput value of WPA. Moreover, among all WEP-based algorithms WEP-40 is having the highest throughput value.

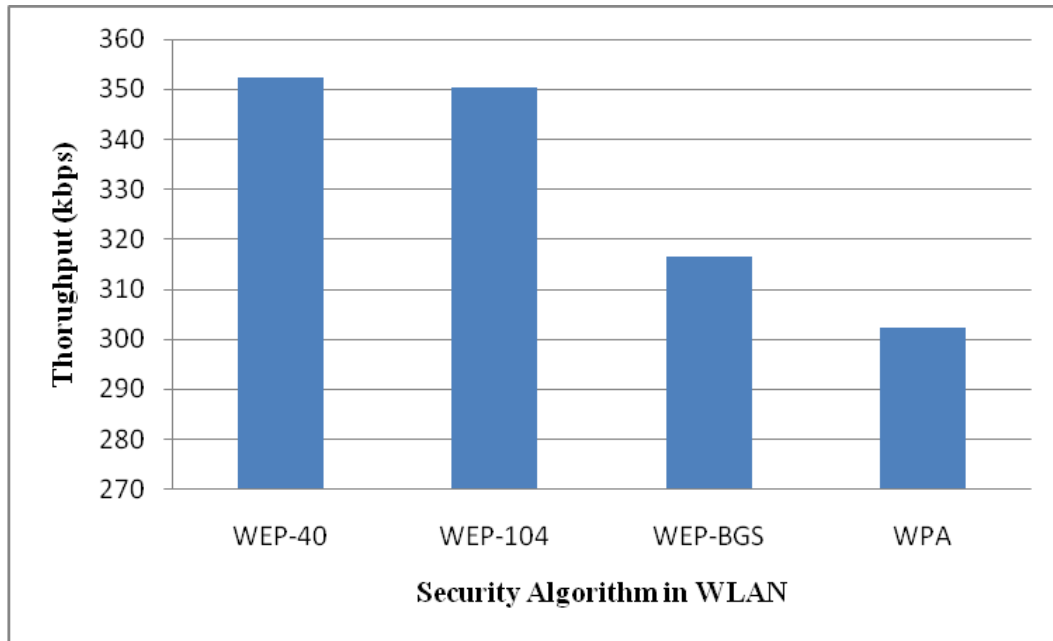


Fig. 10. **Comparison of average throughputs for WEP and WPA**

EED being another important performance metric for any communication network especially in WLAN, various values of EED for different protocols of WEP have thus been compared with WPA and have been shown in Fig. 11. It is observed that average EED (ms) is least for WEP-BGS. Taking WEP-BGS as reference, the value of EED for WEP-40 is the largest (approx. 8.2 times), for WEP-104 it is almost 1.4 times the value for WEP-BGS and for WPA, it comes out to be approx. 1.3 times in comparison with the value for WEP-BGS.

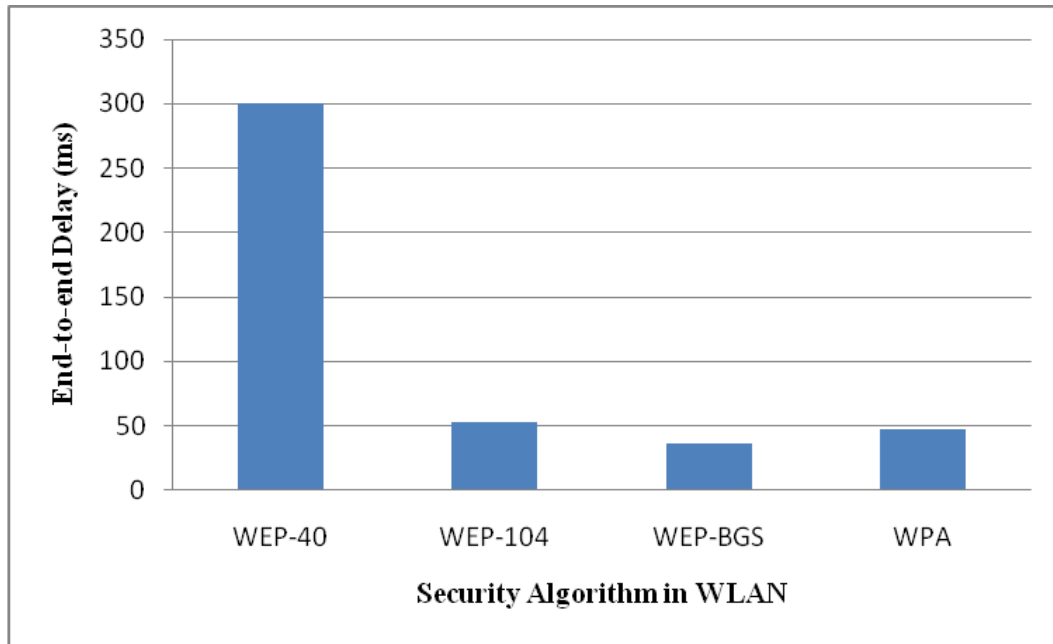


Fig. 11. Comparison of average EEDs for WEP and WPA

Thus for applications where EED parameter is of prime concern, WEP-BGS proves to be a better alternative than WEP-40, WEP-104 and even WPA despite the fact that WEP-40 (the standard WEP) and WPA are one of the most widely used security protocols.

## VI. CONCLUSION

Thus the simulation results help us to compare performance of various security enabled wireless LANs. Since the requirements of a WLAN in terms of its performance may vary from application to application, there cannot be a common performance yard stick for WLANs. The amount of security required and level of risk of the attack would be different for home or a small office, when compared with a big information industry. The analysis performed in this research work enables us to provide certain indications, so as to specify which security algorithm should be employed for a achieving a given performance metric. Since throughput is one of the prime performance parameters in a network, it has been analysed that although throughput remains constant for a given number of nodes for all security algorithms, it is lesser for a WLAN having large number of nodes in comparison with a WLAN having smaller number of nodes. Further, it has been observed that in case of WEP security algorithm, the throughput decreases with increase in the key length. In comparing any variants of WEP with WPA, it has been observed that the throughput for WPA comes out to be even lesser. Thus it may be concluded that throughput decreases in WEP on increasing the key length and, on switching from the security algorithm WEP to WPA there is a further decrease in the throughput value.

While simulating and analyzing another important parameter, EED, it was observed that there is a large percentage decrease in average EED in WPA in comparison with various WEP variants and, therefore, WPA has been found to be better than both WEP-40 and WEP-104. However, the average EED is found to be more in WPA when it is compared with WEP-BGS. Thus, in applications where EED is of prime importance, WEP-BGS proves to be a better choice than WEP-40 or WEP-104 and even WPA. It may therefore be concluded that EED reduces on increasing the key length and also the EED for WPA is quite smaller than EED values for WEP-40 and WEP-104 while more than the EED value for WEP-BGS.

When WPA is compared to WEP-BGS, it is found that WEP-BGS has greater throughput but a lower EED. Thus in terms of these two performance metrics WEP-BGS can, therefore, be considered as a better choice than WPA.

### References

- [1] K. J. Hole, E. Dyrnes, P. Thorsheim, "Securing Wi-Fi networks," *IEEE Computer journals & magazines*, doi. 10.1109/MC.2005.241, vol. 38, no. 7, pp 28 – 34, 2005.
- [2] J. S. Park, D. Dicoi, "WLAN security: current and future," *IEEE Internet Computing*, doi. 10.1109/MIC.2003.1232519, vol. 7, no. 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*, doi. 10.1109/MILCOM.2003.1290220, vol. 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*, doi. 10.1109/EUC.2008.67, vol. 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*. Doi. 10.1109/ARES.2006.42, 2006.
- [6] V. Bhatia, D. Gupta and H. P. Sinha, "Implementing comparative analysis of wireless LAN security protocols in NS2," *IASET International Journal of Electronics and Communication Engineering*, vol. 2, no. 2, ISSN 2278-9901, pp. 1-8, May 2013.
- [7] F.C.C. Osorio, "State of wireless security implementations in the United States and Europe - empirical data," *3<sup>rd</sup> IEEE International Conference on Malicious and Unwanted Software, MALWARE 2008*, doi. 10.1109/MALWARE.2008.4690863, pp 594 - 599, 2008.
- [8] 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*, doi. 10.1109/WOCN.2005.1436095, pp 92 - 97, 2005.

- [9] 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*, doi. 10.1109/ICSPS.2009.87, pp 445 - 449, 2009.
- [10] V. Bhatia, D. Gupta and H.P. Sinha, "Throughput and Vulnerability Analysis of an IEEE 802.11b Wireless LAN," *International Journal of Computer Applications*, vol. 52, no. 3, doi. 10.5120/8182-1509, Aug. 2012.
- [11] B. Potter, "Wireless security's future," *IEEE Security & Privacy*, Digital Object Identifier: 10.1109/MSECP.2003.1219074, vol. 1, no. 4, pp 68 - 72, 2003.
- [12] F. T. Sheldon, John Mark Weber, Yoo Seong-Moo, W. David Pan, "The Insecurity of Wireless Networks" *IEEE Security & Privacy*, vol. 10, no. 4, doi. 10.1109/MSP.2012.60, pp. 54-61, 2012.
- [13] A. Wool, "A note on the fragility of the "Michael" message integrity code", *IEEE Transactions on Wireless Communications*, vol. 3, no. 5 doi. 10.1109/TWC.2004.833470, pp. 1459-1462, 2004.
- [14] 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.
- [15] 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.
- [16] M. Ekpenyong, J. Isabona "Modeling Throughput Performance in 802.11 WLAN" *International Journal of Computer Science Issues*, vol. 7, no. 3, pp. 16 - 22, 2010.
- [17] R. Khalaf and I. Rubin, "Throughput and Delay Analysis in Single Hop and Multihop IEEE 802.11 Networks," *3<sup>rd</sup> International Conference on Broadband Communications, Networks and Systems, (BROADNETS)*, doi. 10.1109/BROADNETS.2006.4374367, pp. 1-9, 2006.
- [18] F. Bertocchi, P. Bergamo, G. Mazzini and M. Zorzi, "Performance comparison of routing protocols for ad hoc networks," *IEEE Global Telecommunications Conference (GLOBECOM '03)*, vol. 2, doi. 10.1109/GLOCOM.2003.1258395, 2003, pp. 1033-1037, 2003.
- [19] S. Srinivasa and M. Haenggi, "Throughput-delay-reliability tradeoffs in multihop networks with random access," *48<sup>th</sup> Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, doi. 10.1109/ALLERTON.2010.5707035, pp. 1117-1124, 2010.
- [20] R. Nath, P. K. Sehgal and A. K. Sethi, "Effect of routing misbehavior in mobile ad hoc network," *IEEE 2<sup>nd</sup> International Advance Computing Conference (IACC), 2010*, doi. 10.1109/IADCC.2010.5423008, pp. 218-222, 2010.