Quantification of the Different Security Algorithms in Wireless Network

Abdalla Gheryani[†] and Mladen Veinović [††]

Singidunum University, Beograd - Serbia

Summary
This paper studies and measures the effect of different security algorithms on the performance of a wireless LAN. Real experiments were performed on a wireless LAN and the data obtained was analyzed for throughput, jitter and delay under different security scenarios. Both TCP and UDP traffic streams were analyzed at three different data rates. The effect of congestion is also measured. The results tell that no important degradation in performance occurs by enabling security algorithms in a wireless LAN. In low bit rate, it shows there is no important degradation, but in case of high rate more than channel rate, it shows there is influence.

Key words:
Wireless LAN, TCP, UDP, WPA, WEP.

1. Introduction

Wireless networks have extended marvelous acceptance in marketable, military, educational and research in last few years. Mobility support is another salient feature of wireless networks which grants the users not only "anytime, anywhere" network access, but also the freedom of roaming while networking. The main contributors to this acceptance are flexibility and mobility offered by these networks. The significant dependence on wireless networks in all walks of life has created a tremendous need for increasing the reliability and security of these networks. The security risks in wireless networks are more than those of wired networks due to open access of the shared wireless medium [2]. Besides security, performance is another major issue in wireless networks. These issues have been exclusively studied in an extensive manner. However, little work exists in the area of understanding the relationship between these two issues. The aim of our study is to understand and quantify the relationship between security and performance in wireless LANs (Local Area Networks). To carry out this study, we performed experiments on a wireless LAN by enabling security protocols like WEP and WPA for TCP and UDP traffic at data rates of 1 Mbps, 5Mbps and 14 Mbps. To see the impact of these security protocols, experiments were performed in unencrypted case as well. The data obtained from these experiments is compared for performance metrics like throughput, jitter and delay.

Manuscript received June 5, 2012
Manuscript revised June 20, 2012

2. Network Layout and Procedure

In our scenario, we have used wired node N0 (Dell with Pentium Dual-Core 2.2 GHz, Marvell Yukon Fast Ethernet Controller and Windows 7 Ultimate with service pack1) as the sender and wireless node N1 (Compaq with Pentium Core Duo 1.83 GHz, Broadcom Wireless LAN and Windows 7 Ultimate with service pack1) as the receiver. In the topology R1 (Cisco 2100 Cable Modem) act as Cisco Modem while R2 (Linksys E1500 Wireless-N Router with SpeedBoost) is Cisco Access Point. Ethernet node N0 connects with R1 through a 100 Mbps link. The link bandwidth between R1 and R2 is set to 100 Mbps while the wireless link between R2 and N1 operates at a nominal data rate 11 Mbps.

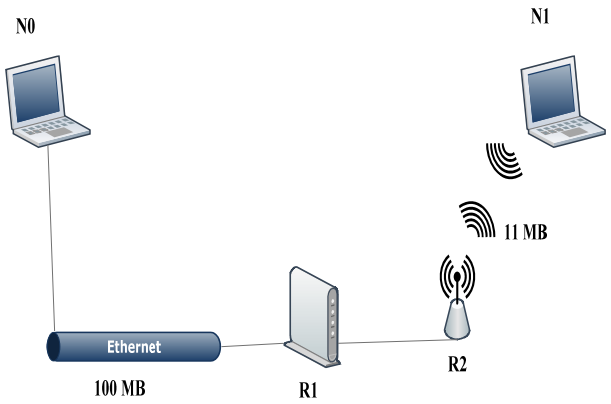

Fig. 1 Layout of the Network

The experiments were conducted on wireless test for different security scenarios and traffic streams in the infrastructure mode of wireless LANs. A brief discussion of different aspects of these experiments is given below.

2.1 Security Scenarios

The experiments were carried out for following scenarios:-

- **No Security:** In this scenario the entities communicate over wireless link without any authentication and encryption. The results obtained are used as a reference for comparison with security enabled cases.

• **WEP enabled:** In this scenario WEP encryption is enabled. The experiments were performed for 64 bit and 128 bit key sizes.
• **WPA enabled:** In this scenario experiments were performed using TKIP and AES mode supported by the access point.

2.2 Traffic Stream

TCP and UDP traffic streams were chosen for experiments. The traffic was generated and received using pathtest tool, installed on both communicating objects.

2.3 Bandwidth

The Access Point used in the experiments can support data rates up to 54 Mbps. The data rate of Access Point (transmission rate of the wireless channel) was fixed at 11 Mbps. The data generation rate for the source was chosen at different transmission rate. These values are labeled as outgoing bandwidth. Since the data rate of Access Point was fixed at 11 Mbps so the generation rate less than 11 Mbps simulates the behavior of an uncongested network, whereas more than 11 Mbps generation rate represents a congested network.
Table 1, shows brief description of different security scenarios:

Table 1: Margin specifications

Security Scenario	***Label***	***Explanation***
No Security	S1	No Encryption
WEP-64	S2	WEP Protocol with 64 bit key
WEP-128	S3	WEP Protocol with 128 bit key
WPA-TKIP	S4	TKIP is used for data encryption
WPA-AES	S5	AES is used for data encryption

2.4 Data Collection

For data collection following points were considered.
• To allow the test to be stabilize, first two readings were unwanted.
• Each experiment was carried out 5 times for reliability of data.
• The readings were noted down when we were sure that.
• For each experiment mean of the readings taken was computed.

3. Experiment Result

We present the results obtained from experiments. The experimental data for average throughput of TCP and UDP, delay of TCP and UDP and jitter of TCP and UDP are tabulated and compared for different scenarios.

3.1 Average Throughput

Tables 2, 3 and 4 show the average throughput for different security scenarios. For comparison purposes the data is plotted using OriginPro as shown in Figures 2, 3, 4, 5, 6 and 7.
Following observations are made:-
• There is no major degradation in average throughput by enabling security policies like WEP-64, WEP-128, WPA-TKIP and WPA-AES.
• For 1and 5 Mbps traffic, the average throughput is near to the source data rates. However, for 12 Mbps case, the average throughput is less than the source data rate. This is due to congestion as the bandwidth of wireless channel is fixed at 12 Mbps.

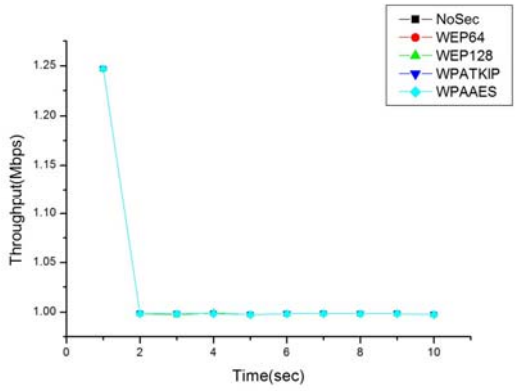

Fig. 2 Average Throughput of TCP in 1 Mbps

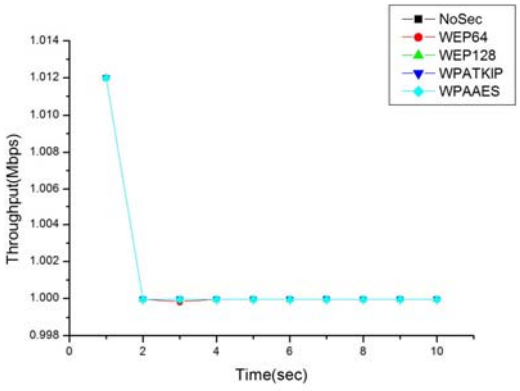

Fig. 3 Average Throughput of UDP in Mbps 1

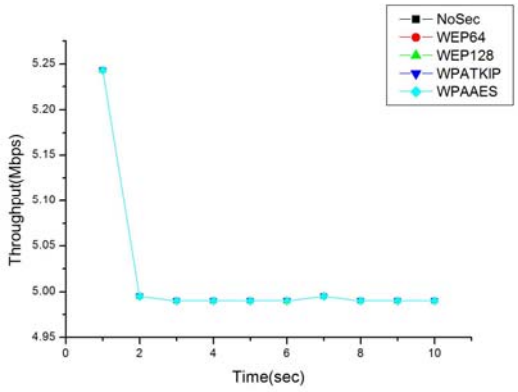

Fig. 4 Average Throughput of TCP in 5 Mbps

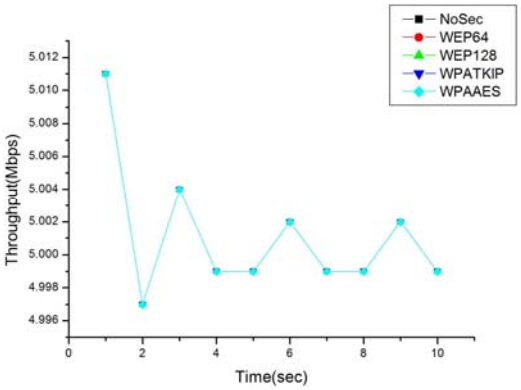

Fig. 5 Average Throughput of UDP in 5 Mbps

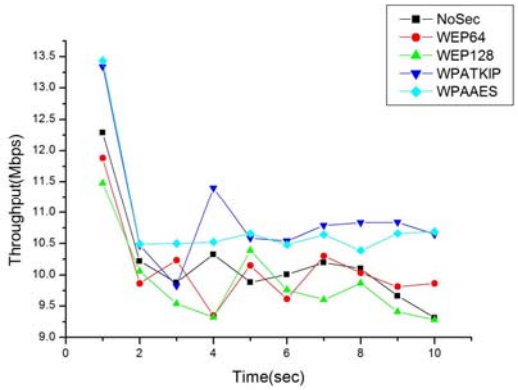

Fig. 6 Average Throughput of TCP in 14 Mbps

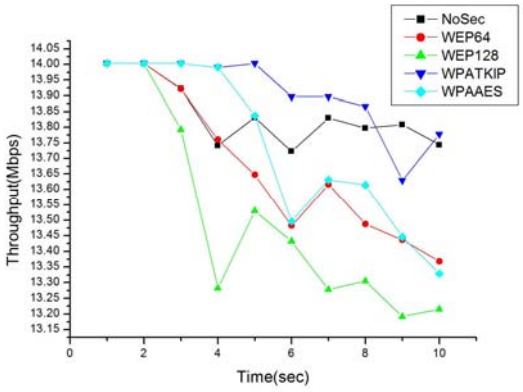

Fig. 7 Average Throughput of UDP in 14 Mbps

The above figures show the achieved throughput for the two transport protocols, TCP and UDP as a function of the transmission rate. It can be seen that TCP and UDP achieve the same throughput for a send rate of 1 Mbps to 5 Mbps.

For transmission rates, beyond 12 Mbps to 14 Mbps, TCP achieved 9.5 Mbps to 13.5 Mbps, whereas UDP achieved 13.2 Mbps to 14.01Mbps.

Experiments show that there is no significant decrease in average throughput for various security scenarios. For 1 and 5 Mbps cases, no effect of congestion was seen as the average throughput is almost same as the data transmission rate at the source. The results obtained for 14 Mbps case show that the average throughput is less than the transmission rate. This is attributed to the congestion caused in the network by high generation rate.

3.2 Jitter

The jitter performance for each of the two transport protocols is shown in Table 5, 6 and 7.

For comparison purposes the data is plotted using OriginPro as shown in Figures 8, 9, 10, 11, 12 and 13.

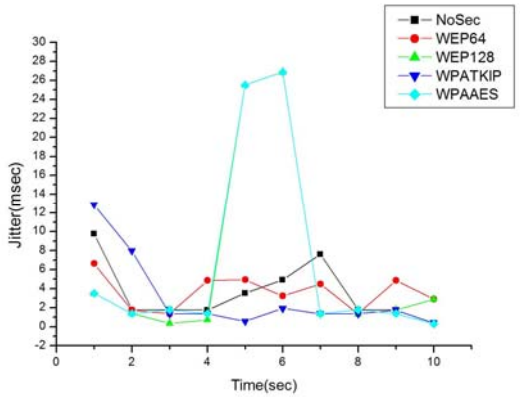

Fig. 8 Jitter of TCP in 1 Mbps

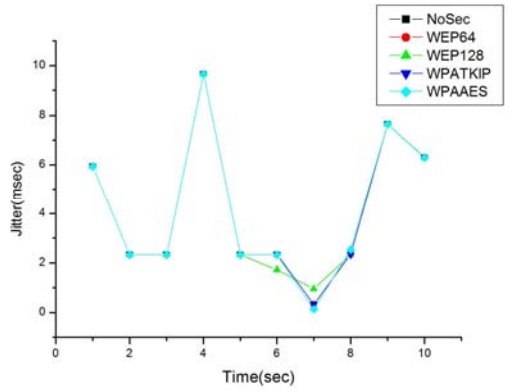

Fig. 9 Jitter of UDP in 1 Mbps

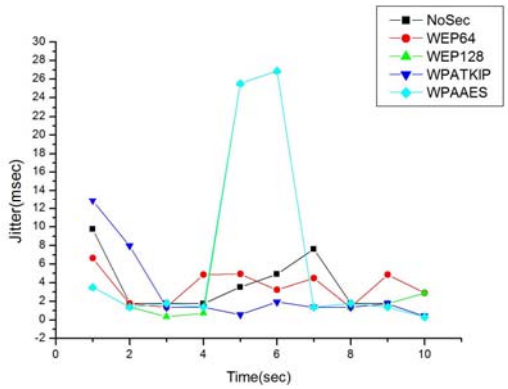

Fig. 10 Jitter of TCP in 5 Mbps

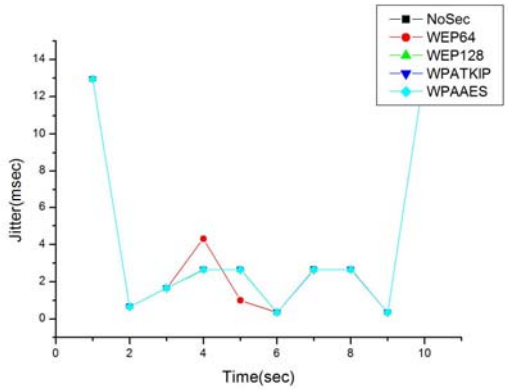

Fig. 11 Jitter of UDP in 5 Mbps

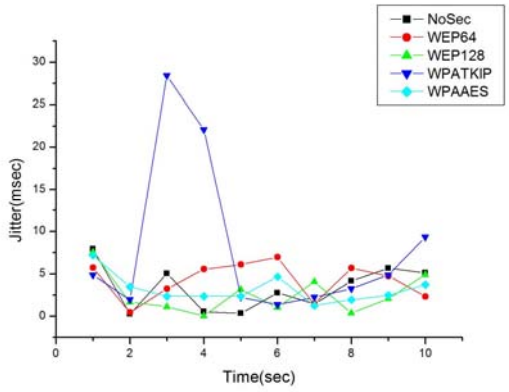

Fig. 12 Jitter of TCP in 14 Mbps

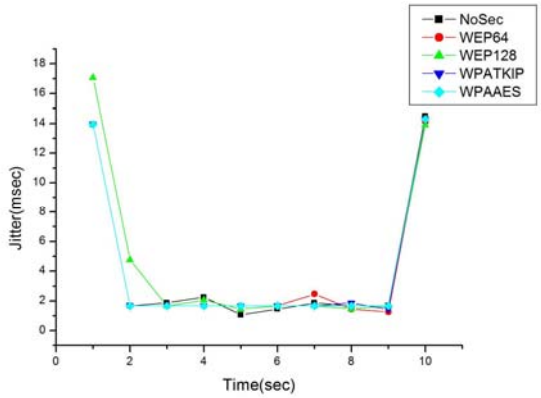

Fig. 13 Jitter of UDP in 14 Mbps

The jitter performance for both protocols is depicted in the above tables and the data is plotted using OriginPro as shown in the above figures.

It is observed that for TCP, jitter values range from 0.0562 ms to 28.42 ms as the transmission rate varies from 1 to 14 Mbps with difference security scenario. For UDP, the jitter values lie in the range from 0.144 ms to 17.064 ms. It can be noticed that with AES algorithm exhibit better performance in comparison with other security scenario.

As transmission rate increases, for TCP, we can noticed that the jitter value has taken different values depends on the security algorithm that has been used and for UDP, we can notice that the jitter values increase.

3.3 Delay

Delay refers to the time taken for a packet to be transmitted across a network from source to destination. Tables 8, 9 and 10 show the delay performance for each of TCP and UDP protocols.

For comparison purposes the data is plotted using OriginPro as shown in figures 14, 15, 16, 17, 18 and 19.

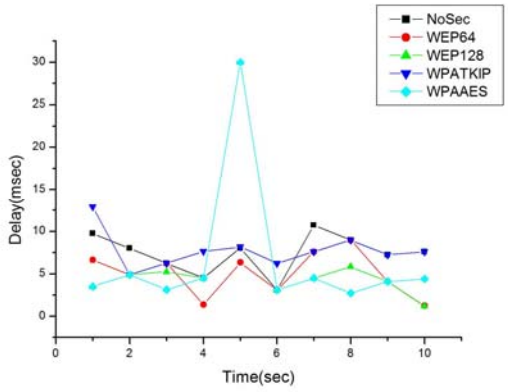

Fig. 14 Delay of TCP in 1 Mbps

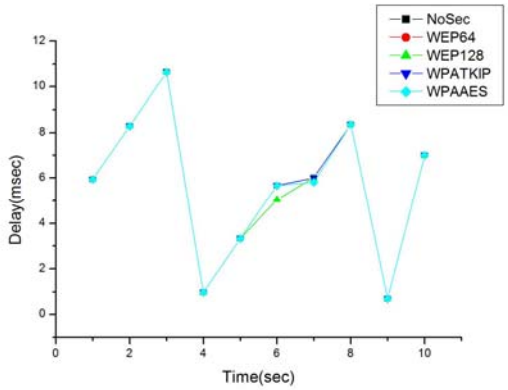

Fig. 15 Delay of UDP in 1 Mbps

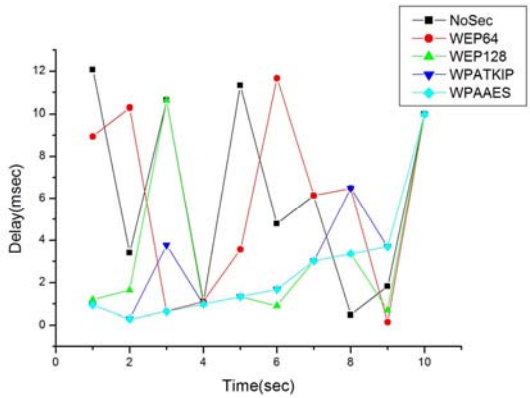

Fig. 16 Delay of TCP in 5 Mbps

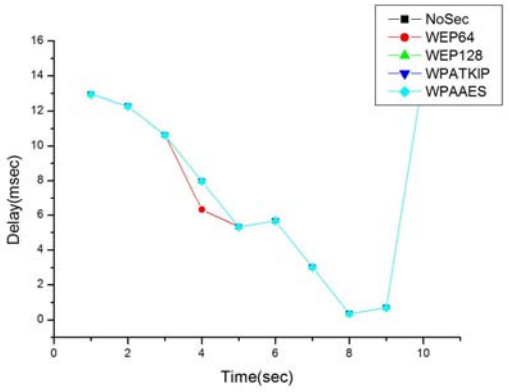

Fig. 17 Delay of UDP in 5 Mbps

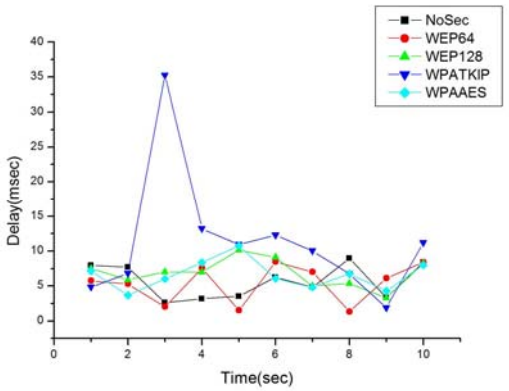

Fig. 18 Delay of TCP in 14 Mbps

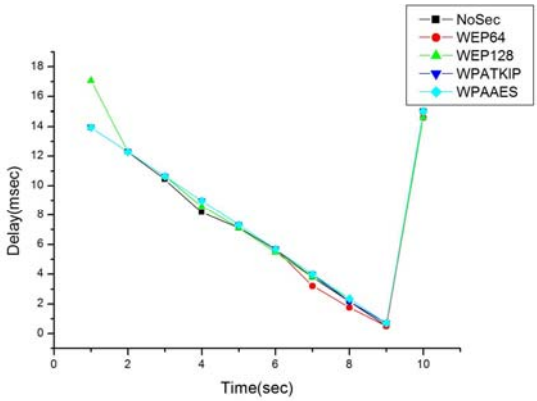

Fig. 19 Delay of UDP in 14 Mbps

The above figures show the relation between delay and transmission rate. X axis represents the time and Y axis represents to delay.

As the transmission rate is increased from 1 Mbps to 14 Mbps, delay experienced with TCP as transport protocol varies from 0.14 ms to 35.25 ms, while for UDP the delay is in the range of 0.356 ms to 17.064 ms.

We can observe that, when using the TCP protocol the delay is taken varies difference value even with using different security algorithm, but with AES algorithm is taken lower values compare with other algorithm.
In UDP, the delay is slightly same and the starting value of delay is increased with changing of transmission rate and at transmission rate of 14 Mbps, the delay is taken the highest value of 17.064 ms, because of congestion.

4. Conclusions

We quantified the effect of implementing security on network performance in infrastructure mode wireless LAN. Experiments were performed under different security scenarios for TCP and UDP traffic streams.
The security scenarios chosen were Wired Equivalent Privacy (WEP) with key sizes of 64 and 128 bits and Wi-Fi Protected Access (WPA) using TKIP and AES algorithms. For comparison purposes experiments were also performed for unencrypted case as well. The data rate for AP (potential bandwidth of wireless channel) was selected as 11 Mbps.
The results obtained from experiments show that there is no different in average throughput for unencrypted and encrypted scenarios. UDP traffic shows there is slightly difference between unencrypted and encrypted value, because of congestion.
For jitter performance, TCP is taken different values and that happen with changing of the encrypted algorithm and in UDP the jitter value is increasing in all encrypted scenario.
For delay performance, there are varies values the delay had taken with TCP protocol in both unencrypted and encrypted algorithms, but when using UDP protocol, the delay almost same with all scenario.

Acknowledgments

The author would like to express his pleasant thanks to Dr. Mladen Veinović for his valuable advice.

References

[1] Gh. Rasool Begh Ajaz Hussain Mir, "Quantification of the Effect of Security on Performance in Wireless LANs," Third International Conference on Emerging Security Information, Systems and Technologies, 2009.
[2] H. Yang, F. Ricciato, S. Lu, and L. Zhang, "Securing a wireless world," Proc. IEEE (Special Issue on Cryptography and Security Issues), vol. 94, no. 2, February 2006.
[3] A. K. Agarwal and W. Wang, "Measuring performance impact of security protocols in Wireless Local Area Networks," The Second International Conference on Broadband Networks, Boston, USA, October 2005.
[4] M. Boulmalf, E. Barka, and A. Lakas, "Analysis of the effect of security on data and voice traffic in WLAN," Computer Communications, 30 (2007) 2468-2477.
[5] N. Baghaei, "IEEE 802.11 wireless LAN security performance using multiple clients," University of Canterbury, Christchurch, NZ.
[6] A. M. Al Naamany, A. Al Shidhani, and H. Bourdoucen, "IEEE 802.11 wireless LAN security overview," International Journal of Computer Science and Network Security, vol.6, no. 5B, May 2006.
[7] W. Stallings, Cryptography and Network Security: Principles and Practice, 4th ed., Published by Dorling Kindersley (India) Pvt. Ltd. Licensees of Pearson Education in South Asia.
[8] W. Arbaugh, N. Shankar, Y. Wan, and K. Zhang, "Your 802.11 wireless network has no clothes," IEEE Wireless Communication, vol. 9, no. 6, Dec. 2002.
[9] C. He and J. C. Mitchell, "Security analysis and improvements for IEEE 802.11i," Stanford University, Stanford CA.

Abdalla Gheryani born on February 27, 1973. Received the B.S. in Computer Science and Engineering from Engineering Academy - Tajura in 1999 and M.S. degrees in Computer Science and Engineering from Jaypee Institute of Information Technology - India in 2009. Now pursing PhD. at Singidunum University – Serbia.

Mladen Veinović was born on January 01, 1962. He received the B.Sc., M.Sc. and Ph.D. degree in 1986, 1990 and 1996, respectively, all from the Faculty of Electrical Engineering, University of Belgrade. Since 1987, he has worked at the Institute of Applied Mathematics and Electronics. Since 2005, he is professor at Singidunum University. His current research interests include computer network, databases and data security.

Table2. Average Throughput for 1 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	1.247	1.012	1.247	1.012	1.247	1.012	1.247	1.012	1.247	1.012
2	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999
3	0.9983	0.9999	0.9983	0.9998	0.9972	0.9999	0.9983	0.9999	0.9983	0.9999
4	0.9985	0.9999	0.9985	0.9999	0.9994	0.9999	0.9985	0.9999	0.9985	0.9999
5	0.9976	0.9999	0.9976	0.9999	0.9976	0.9999	0.9976	0.9999	0.9976	0.9999
6	0.9983	0.9999	0.9983	0.9999	0.9983	0.9999	0.9983	0.9999	0.9983	0.9999
7	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999
8	0.9983	0.9999	0.9983	0.9999	0.9983	0.9999	0.9983	0.9999	0.9983	0.9999
9	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999	0.9985	0.9999
10	0.9976	0.9999	0.9976	0.9999	0.9976	0.9999	0.9976	0.9999	0.9976	0.9999

Table3. Average Throughput for 5 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	5.243	5.011	5.243	5.011	5.243	5.011	5.243	5.011	5.243	5.011
2	4.995	4.997	4.995	4.997	4.995	4.997	4.995	4.997	4.995	4.997
3	4.99	5.004	4.99	5.004	4.99	5.004	4.99	5.004	4.99	5.004
4	4.99	4.999	4.99	4.999	4.99	4.999	4.99	4.999	4.99	4.999
5	4.99	4.999	4.99	4.999	4.99	4.999	4.99	4.999	4.99	4.999
6	4.99	5.002	4.99	5.002	4.99	5.002	4.99	5.002	4.99	5.002
7	4.995	4.999	4.995	4.999	4.995	4.999	4.995	4.999	4.995	4.999
8	4.99	4.999	4.99	4.999	4.99	4.999	4.99	4.999	4.99	4.999
9	4.99	5.002	4.99	5.002	4.99	5.002	4.99	5.002	4.99	5.002
10	4.99	4.999	4.99	4.999	4.99	4.999	4.99	4.999	4.99	4.999

Table4. Average Throughput for 14 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	12.288	14.003	11.880	14.003	11.474	14.003	13.337	14.003	13.436	14.003
2	10.219	14.003	9.8638	14.003	10.056	14.003	10.470	14.003	10.491	14.003
3	9.875	13.923	10.234	13.921	9.5412	13.791	9.8222	14.003	10.501	14.003
4	10.329	13.741	9.3486	13.760	9.326	13.282	11.397	13.991	10.527	13.991

5	9.8828	13.831	10.149	13.647	10.392	13.530	10.583	14.003	10.659	13.837
6	10.008	13.722	9.6148	13.482	9.757	13.431	10.542	13.897	10.480	13.496
7	10.198	13.83	10.302	13.615	9.6032	13.278	10.793	13.897	10.645	13.631
8	10.1	13.796	10.031	13.487	9.8688	13.305	10.835	13.866	10.391	13.614
9	9.6602	13.808	9.81	13.437	9.412	13.191	10.843	13.628	10.660	13.446
10	9.3158	13.744	9.865	13.369	9.2834	13.215	10.643	13.777	10.688	13.328

Table5. Jitter for 1 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	9.741	5.944	6.621	5.944	3.5018	5.9438	12.86	5.944	3.501	5.944
2	1.738	2.344	1.738	2.3446	1.3818	2.3448	7.978	2.344	1.381	2.344
3	1.770	2.344	1.349	2.3448	0.3492	2.3446	1.349	2.344	1.770	2.344
4	1.738	9.656	4.858	9.6556	0.7386	9.6556	1.381	9.656	1.381	9.656
5	3.534	2.344	4.941	2.3448	25.501	2.3446	0.541	2.344	25.50	2.344
6	4.923	2.344	3.210	2.3448	26.890	1.7274	1.930	2.344	26.89	2.344
7	7.621	0.344	4.501	0.3438	1.382	0.9614	1.381	0.344	1.381	0.144
8	1.770	2.344	1.349	2.3448	1.3488	2.3452	1.349	2.344	1.771	2.544
9	1.738	7.655	4.858	7.6552	1.7382	7.6554	1.738	7.655	1.381	7.655
10	0.382	6.299	2.877	6.2992	2.8978	6.2992	0.382	6.298	0.302	6.299

Table 6. Jitter for 5 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	12.06	12.94	8.943	12.945	1.183	12.944	0.943	12.94	0.943	12.94
2	8.655	0.655	1.344	0.6552	0.4644	0.6554	0.655	0.655	0.655	0.655
3	7.224	1.655	9.655	1.6558	8.9848	1.6556	3.465	1.655	0.344	1.655
4	9.535	2.655	0.464	4.3130	9.655	2.655	2.775	2.655	0.344	2.655
5	10.22	2.655	2.464	0.9979	0.3448	2.656	0.344	2.655	0.344	2.655
6	6.535	0.344	8.104	0.345	0.4156	0.3448	0.344	0.344	0.344	0.344
7	1.344	2.655	5.535	2.6556	2.1048	2.6556	1.344	2.655	1.344	2.659
8	5.655	2.655	0.344	2.656	0.345	2.6552	3.464	2.656	0.344	2.652
9	1.345	0.344	6.335	0.345	2.6552	0.3444	2.775	0.344	0.344	0.345
10	8.179	13.29	9.859	13.298	9.299	13.299	6.3	13.29	6.299	13.29

Table 7. Jitter for 14 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	7.944	13.94	5.743	13.945	7.5438	17.06	4.864	13.94	7.144	13.94
2	0.255	1.655	0.455	1.6556	1.6548	4.7752	1.945	1.655	3.455	1.655
3	5.055	1.855	3.255	1.6552	1.1444	1.6554	28.42	1.655	2.344	1.655
4	0.544	2.255	5.545	1.6556	0.0562	2.055	22.05	1.655	2.344	1.655
5	0.344	1.055	6.056	1.6556	3.1454	1.4556	2.255	1.655	2.345	1.655
6	2.744	1.455	6.944	1.6552	1.0554	1.656	1.345	1.655	4.655	1.655
7	1.455	1.855	1.455	2.4556	4.056	1.6552	2.255	1.655	1.255	1.655
8	4.144	1.655	5.655	1.4556	0.3448	1.4552	3.256	1.855	1.945	1.655
9	5.655	1.655	4.744	1.255	2.0554	1.6556	4.855	1.455	2.455	1.655
10	5.098	14.49	2.299	14.098	4.8994	13.899	9.299	14.29	3.699	14.29

Table8. Delay for 1 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	9.741	5.944	6.621	5.944	3.5018	5.9438	12.86	5.944	3.501	5.944
2	8.003	8.289	4.883	8.2886	4.8836	8.2886	4.883	8.289	4.883	8.289
3	6.232	10.63	6.232	10.633	5.2328	10.633	6.232	10.63	3.112	10.63
4	4.494	0.977	1.374	0.9778	4.4942	0.9776	7.614	0.977	4.494	0.977
5	8.028	3.322	6.315	3.3226	29.996	3.3222	8.155	3.322	29.99	3.322
6	3.105	5.667	3.105	5.6674	3.1052	5.0496	6.225	5.667	3.105	5.667
7	10.72	6.011	7.606	6.0112	4.4872	6.011	7.606	6.011	4.487	5.811
8	8.955	8.356	8.956	8.356	5.836	8.3562	8.955	8.356	2.715	8.356
9	7.217	0.700	4.097	0.7008	4.0978	0.7008	7.217	0.701	4.097	0.701
10	7.6	7	1.22	7	1.2	7	7.6	7	4.4	7

Table9. Delay for 5 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	12.06	12.94	8.943	12.945	1.183	12.944	0.943	12.94	0.943	12.94
2	3.407	12.28	10.28	12.289	1.6474	12.288	0.287	12.28	0.287	12.28
3	10.63	10.63	0.633	10.634	10.632	10.633	3.752	10.63	0.632	10.63

4	1.097	7.978	1.097	6.3209	0.9772	7.9782	0.977	7.978	0.977	7.978
5	11.32	5.322	3.562	5.323	1.322	5.3222	1.321	5.323	1.321	5.323
6	4.786	5.667	11.66	5.668	0.9064	5.667	1.666	5.667	1.666	5.667
7	6.131	3.011	6.131	3.0124	3.0112	3.0114	3.011	3.012	3.011	3.008
8	0.475	0.356	6.475	0.3564	3.3562	0.3562	6.475	0.356	3.355	0.356
9	1.820	0.700	0.140	0.7014	0.701	0.7006	3.7	0.701	3.700	0.701
10	10	14	10	14	10	14	10	14	10	14

Table10. Delay for 14 Mbps

Time	No Security		WEP-64		WEP-128		WPA-TKIP		WPA-AES	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
1	7.944	13.94	5.743	13.945	7.5438	17.064	4.864	13.94	7.144	13.94
2	7.689	12.28	5.288	12.289	5.889	12.288	6.809	12.28	3.688	12.28
3	2.633	10.43	2.033	10.634	7.0334	10.633	35.23	10.63	6.033	10.63
4	3.178	8.178	7.578	8.9786	6.9772	8.5784	13.17	8.978	8.377	8.978
5	3.522	7.123	1.522	7.323	10.122	7.1228	10.92	7.322	10.72	7.322
6	6.267	5.667	8.466	5.6678	9.0672	5.4668	12.26	5.667	6.066	5.667
7	4.812	3.811	7.011	3.2122	5.0112	3.8116	10.01	4.012	4.811	4.011
8	8.956	2.156	1.356	1.7566	5.356	2.3564	6.756	2.156	6.756	2.356
9	3.301	0.501	6.100	0.5016	3.3006	0.7008	1.900	0.701	4.300	0.700
10	8.4	15	8.4	14.6	8.2	14.6	11.2	15	8	15