Annales Mathematicae et Informaticae
***42** (2013) pp. 45–55*
http://ami.ektf.hu

Performance evaluation of wireless networks speed depending on the encryption

Tamás Krausz, János Sztrik

Faculty of Informatics, University of Debrecen
krausz.tamas@inf.unideb.hu, sztrik.janos@inf.unideb.hu

Submitted September 2, 2013 — Accepted November 28, 2013

Abstract

We can use a variety of encryption standards to encrypt data traffic to ensure the safety of wireless networks. The question is to what extent the security of the network affects network performance. For answering this question, experiments were performed without data encryption, and the use of various encryption standards. IEEE 802.11g and 802.11n wireless networking standards were used in the experiment. The answer of the question is that encryption should be used because it does not cause significantly slower speed.

Keywords: Wireless networking, security, encryption, WEP, WPA/TKIP, WPA2/AES

MSC: 68M20, 68M12, 94A60

1. Introduction

Wireless networks are increasingly exposed to the risk of unauthorized access. The reason for this is that the information runs instead of cable into the air. So it is enough to be in radio signal propagation range, and eavesdropping is easy (password and file contents can be stolen). You can use other internet subscriptions, and perform various illegal activities.

Avoiding illegal access to our network, we can encrypt the data flow. We can read about various wireless security tools in books [6, 7]. Wireless network security

was examined in [2, 3, 5]. Paper [1] discovers the effects of the IEEE802.11i security specification on the performance of wireless networks. In [4], the throughput performance of IPv4 and IPv6 using UDP for wireless LAN networks with 802.11n and with and without security for two client-server networks were compared.

The question arises as to the security of wireless networks influences the speed of data transfer, that is, the network performance. To answer this question, experiments were performed without data encryption, and the use of various encryption standards.

At first, a wireless router was connected directly (USB 2.0) to hard disk and the file transfer speeds between client and disk were measured, than the file transfer speeds between two wireless clients were tested using a modern wireless router for home use.

The number of clients was increased for further examination of the network performance. In experiments, the number and type of clients were changing and the ftp service speed was measured in conjunction with encryption.

The following encryption standards were used in the experiments:

WEP (Wired Equivalent Privacy) is a security algorithm for IEEE 802.11 wireless networks. Obsolete, it is not safe in today's circumstances. Each 802.11 packet is encrypted separately with an RC4 cipher stream generated by a 64-bit RC4 key.

WPA/TKIP (Wi-Fi Protected Access, Wi-Fi Protected Access), which is similar to the WEP uses RC4 coder 128-bit key and 48-bit initialization vector, but this has been introduced in accessing the TKIP (Temporal Key Integrity Protocol, temporary secure key protocol), which continuously rotates keys used in the link.

WPA2/AES (Advanced Encryption Standard) uses a new coder instead of the old RC4.

2. The effect of encryption for the wireless network speed

During the experiments ca. 50 MB (50 298 448 bytes) transfer file was used.

2.1. First experiment

Copy to laptop from hard drive and back.

The laptop was placed close to the router, a SATA hard disk was connected to the router with USB port. We set up the router smb share. The wireless settings 2.4 GHz band and b / g / n mixed mode were used.

laptop 1: dell studio 1557 (Dell 1520 wireless N card, Core i720Qm, 8GB RAM, windows7 x64 operating system

router: TP-LINK WR2543ND wireless router (Atheros AR7242@400MHz CPU 64MB RAM)

The following speeds were measured:

	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	average
copy to laptop (sec)	17,16	16,94	16,88	16,81	17,03	16,96
copy back to USB hdd (sec)	29,05	29,12	28,97	29,67	29,93	29,35
copy to laptop (MB/sec)	2,93114	2,96921	2,97977	2,99217	2,95352	2,96501
copy back to USB hdd (MB/sec)	1,73144	1,72728	1,73623	1,69526	1,68054	1,71386

Table 1: Without encryption

	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	average
copy to laptop (sec)	27,33	25,94	26,18	25,77	26,84	26,412
copy back to USB hdd (sec)	38,06	38,74	38,11	37,92	38,55	38,276
copy to laptop (MB/sec)	1,84041	1,93903	1,92125	1,95182	1,87401	1,90438
copy back to USB hdd (MB/sec)	1,32156	1,29836	1,31982	1,32644	1,30476	1,3141

Table 2: WEP 64 bit encryption (no n)

	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	average
copy to laptop (sec)	29,49	28,81	28,11	29,22	28,79	28,884
copy back to USB hdd (sec)	39,67	38,49	39,12	39,08	39,53	39,178
copy to laptop (MB/sec)	1,70561	1,74587	1,78934	1,72137	1,74708	1,74139
copy back to USB hdd (MB/sec)	1,26792	1,30679	1,28575	1,28706	1,27241	1,28384

Table 3: WPA/TKIP (no n)

	1. m.	2. m.	3. m.	4. m.	5. m.	average
copy to laptop (sec)	19,29	18,31	18,95	19,75	18,54	18,968
copy back to USB hdd (sec)	32,13	31,94	32,75	32,76	32,48	32,412
copy to laptop (MB/sec)	2,60749	2,74705	2,65427	2,54676	2,71297	2,65175
copy back to USB hdd (MB/sec)	1,56547	1,57478	1,53583	1,53536	1,5486	1,55185

Table 4: WPA2/AES

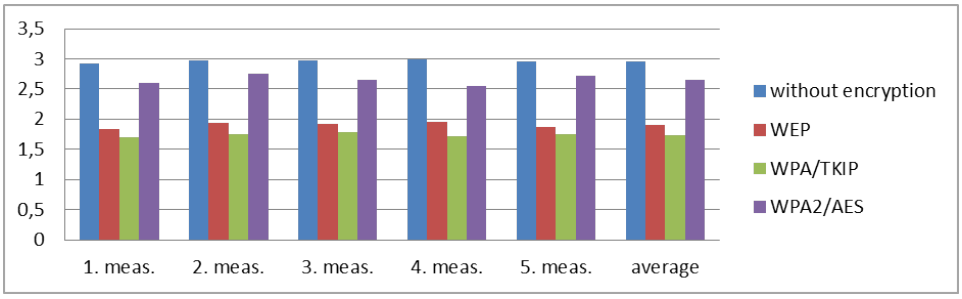

Figure 1: Copy to laptop (MB/sec)

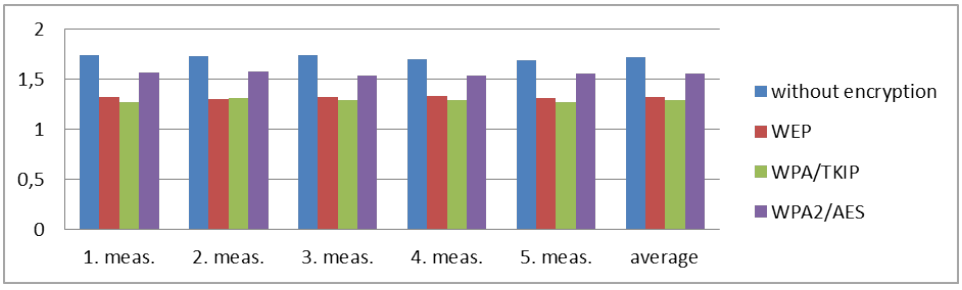

Figure 2: Copy back to USB (MB/sec)

3. Second experiment

In the second experiment, we copied the file between the two laptops using the TP-LINK WR2543ND wireless router.

laptop 1: dell studio 1557 (Dell 1520 wireless N card, Core i720Qm, 8GB RAM, window7 x64 operating system

laptop 2: fujisu amilo Pa1538 (TP-Link TL-W722N usb wireless card, AMD turion xl-50 processor 4GB RAM, windows 7 x64 operating system)

router: TP-link wr2543ND wireless router (Atheros AR7242@400MHz CPU 64MB RAM)

The following speeds were measured:

	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	average
from laptop1 to laptop2 (sec)	13,87	14,05	14,69	14,13	14,54	14,256
from laptop2 to laptop1 (sec)	17,61	17,92	16,99	17,51	17,44	17,494
from laptop1 to laptop2 (MB/sec)	3,62642	3,57996	3,42399	3,55969	3,45932	3,52823
from laptop2 to laptop1 (MB/sec)	2,85624	2,80683	2,96047	2,87256	2,88409	2,87518

Table 5: Without encryption

	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	average
from laptop1 to laptop2 (sec)	41,69	39,98	40,22	40,89	40,92	40,74
from laptop2 to laptop1 (sec)	39,5	39,88	40,13	39,64	40,02	39,834
from laptop1 to laptop2 (MB/sec)	1,20649	1,25809	1,25058	1,23009	1,22919	1,23462
from laptop2 to laptop1 (MB/sec)	1,27338	1,26124	1,25339	1,26888	1,25683	1,2627

Table 6: WEP

	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	average
from laptop1 to laptop2 (sec)	46,07	45,16	45,54	45,93	46,12	45,764
from laptop2 to laptop1 (sec)	45,03	44,59	45,15	45,37	45,42	45,112
from laptop1 to laptop2 (MB/sec)	1,09178	1,11378	1,10449	1,09511	1,0906	1,09908
from laptop2 to laptop1 (MB/sec)	1,117	1,12802	1,11403	1,10863	1,10741	1,11497

Table 7: WPA/TKIP

	1. meas.	2. meas.	3. meas.	4. meas.	5. meas.	average
from laptop1 to laptop2 (sec)	15,87	16,17	16,43	16,01	16,23	16,142
from laptop2 to laptop1 (sec)	19,89	20,32	20,51	20,88	19,97	20,314
from laptop1 to laptop2 (MB/sec)	3,1694	3,1106	3,06138	3,14169	3,0991	3,116
from laptop2 to laptop1 (MB/sec)	2,52883	2,47532	2,45239	2,40893	2,5187	2,47605

Table 8: WPA2/AES

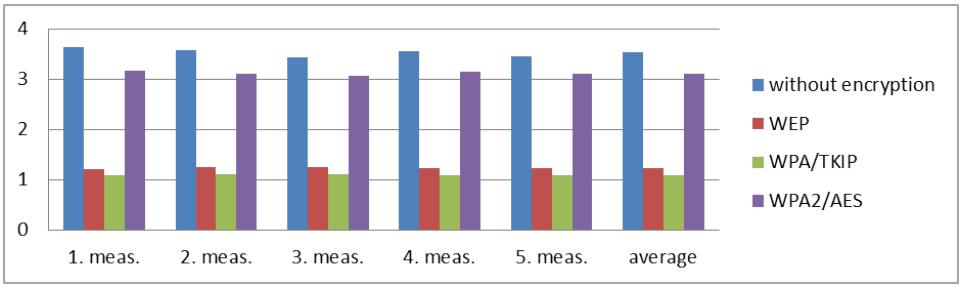

Figure 3: Copy from laptop1 to laptop2 (MB/sec)

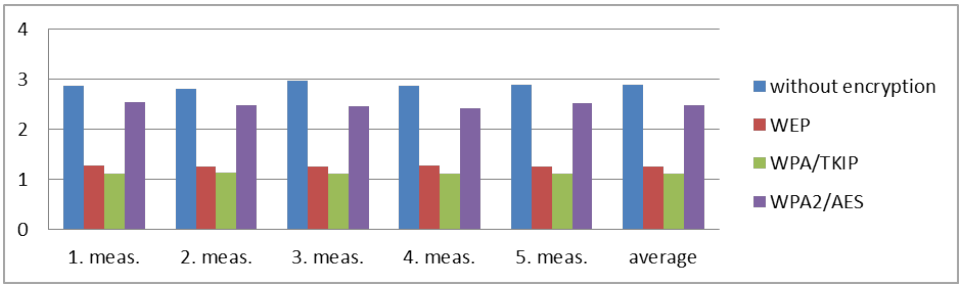

Figure 4: Copy from laptop2 to laptop1 (MB/sec)

3.1. Conclusions

Based on the first measurement, WPA2/AES causes slowdown of 10-30 percent, depending on the direction of the copy.

The 802.11n does not allow WEP and WPA/TKIP encryption, so the router will switch back to 802.11 g mode, so despite the weaker encryption much slower speeds are obtained. The WEP is no longer secure only marginally faster than the WPA/TKIP encryption.

On modern devices, WPA2/AES encryption should be used because it does not cause too significantly slower speed when transferring files.

In the second experiment, WPA2/AES encryption with the 802.11n causes 10-15 percent slowdown of copying in both directions. WPA/TKIP is 12-13 percent slower than WEP because the stronger encryption makes more load on the network card and the router.

4. FTP speed change depending on the number of clients and encryption

In these experiments, increasing the number of clients, we have examined the data traffic rate in the context of encryption. We have used TP-LINK WR2543nd router

built-in FTP server to which USB 2.0 hard drive was connected. The transfer file was approximately 100 MB (100 769 606 bytes). The wireless router setting was 2.4 GHz band and b / g / n mixed mode.

During the measurements, the following devices were used:

laptop 1: Lenovo R500 (Atheros AR5006X wireless a/b/g card, Core2 Dou P8400 CPU, 4GB RAM Windows7 x64 operating system)

laptop 2: Dell studio 1557 (Dell 1520 wireless N card, Core i720Qm 8GB RAM, Windows7 x64 operating system)

desktop: Pentium dual core E6500 (TL-WN721N 150 MB usb wireless card, 4GB RAM, window8 x64 operating system)

router: TP-Link WR2543ND wireless router (Atheros AR7242@400MHz CPU 64MB RAM)

The following speeds were measured:

4.1. Download

	Lenovo	Dell	deskt	Dell + desktop			all three			
				Dell	deskt	avg	Lenovo	Dell	deskt	avg
transmission time (sec)	55	27	24	40	39	39,5	73	66	65	68,0
transmission rate (KB/sec)	1832	3732	4199	2519	2584	2551	1380	1527	1550	1482

Table 9: WPA2/AES encryption

	Lenovo	Dell	deskt	Dell + desktop			all three			
				Dell	deskt	avg	Lenovo	Dell	deskt	avg
transmission time (sec)	45	23	22	38	38	38,0	69	53	54	58,7
transmission rate(KB/sec)	2239	4381	4580	2652	2652	2652	1460	1901	1866	1718

Table 10: Download without encryptions

	Lenovo	Dell	deskt	Dell + desktop			all three			
				Dell	deskt	avg	Lenovo	Dell	deskt	avg
transmission time (sec)	48	63	57	80	79	79,5	119	120	119	119,3
transmission rate(KB/sec)	2099	1600	1768	1260	1276	1268	847	840	847	844

Table 11: WEP 64 bit download

4.2. Upload

	Lenovo	Dell	deskt	Dell + desktop			all three			
				Dell	deskt	avg	Lenovo	Dell	deskt	avg
transmission time (sec)	86	68	96	115	116	115,5	178	177	178	177,7
transmission rate(KB/sec)	1172	1482	1050	876	869	872	566	569	566	567

Table 12: WPA2/AES upload

	Lenovo	Dell	deskt	Dell + desktop			all three			
				Dell	deskt	avg	Lenovo	Dell	deskt	avg
transmission time (sec)	69	65	93	109	115	112,0	176	176	175	175,7
transmission rate(KB/sec)	1460	1550	1084	924	876	900	573	573	576	574

Table 13: No encryption upload

	Lenovo	Dell	deskt	Dell + desktop			all three			
				Dell	deskt	avg	Lenovo	Dell	deskt	avg
transmission time (sec)	73	78	57	125	112	118,5	184	184	180	182,7
transmission rate(KB/sec)	1380	1292	1768	806	900	850	548	548	560	552

Table 14: WEP 64 bit upload

4.3. Download speed rates

download speed	Lenovo	Dell	desktop	Dell + desktop average	all three average
WPA2/AES	1832	3732	4199	2551	1482
no encryption	2239	4381	4580	2652	1718
WEP 64 bit	2099	1600	1768	1268	844

Table 15: Download speed rates

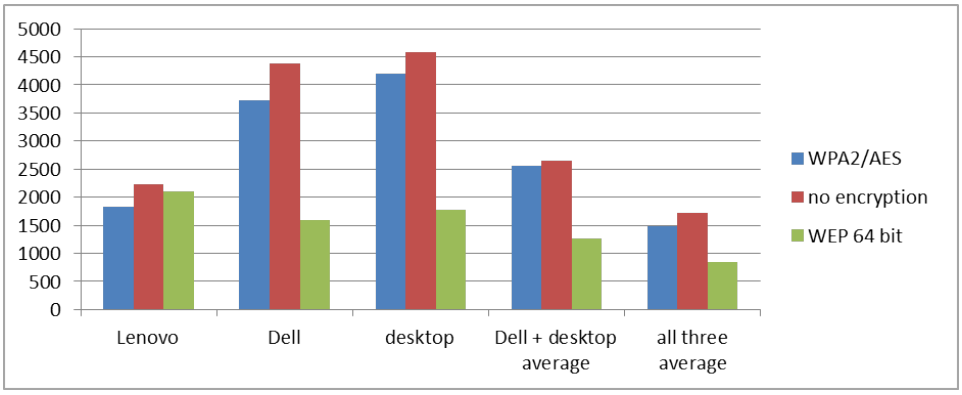

Figure 5: Download transfer speeds

Compared to the unencrypted case, the download speeds are slowed somewhat by increasing the number of clients at WPA2/AES case. The rate reduction of computers with 802.11n card is bigger if the computers are used alone compared to the case when we use them together. The three computers one-time download speed loss is similar to that of the single download.

4.4. Upload speed rates

In case of 802.11n there is no significant difference among the speed of type of encryption, because the upload speed is slow. Lenovo uses 802.11g speed in the upload. WPA2/AES is 24 percent slower than unencrypted. When all three computers upload simultaneously the speed was slow and therefore it did not significantly slow down.

upload speeds	Lenovo	Dell	desktop	Dell + desktop average	all three average
WPA2/AES upload	1172	1482	1050	872	567
no encryption upload	1460	1550	1084	900	574
WEP 64 bit upload	1380	1292	1072	850	552

Table 16: Upload speed rates

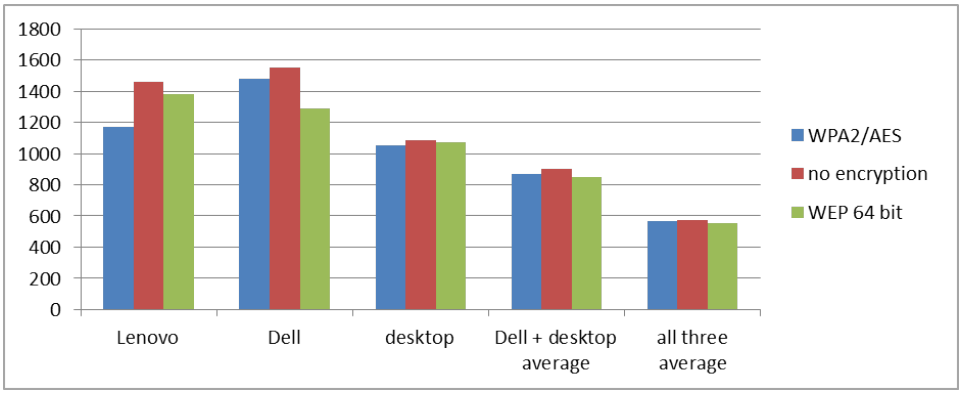

Figure 6: Upload transfer speeds

4.5. Conclusions

The WEP security is poor and 802.11n switches back to 802.11g, and therefore the speed is significantly reduced. The only exception from this is Lenovo, which originally used the 802.11g standard.

Using the FTP service when security matters, WPA2/AES encryption should always be used. If speed is more important than safety (such as anonymous FTP service), you can disable the encryption and speed of 10-20 per cent gain can be obtained.

5. Summary

We got similar result to paper [1] using more modern hardware and operating system with 802.11n wireless standard. The encryption and decryption takes time so that is the main cause of slowing down the traffic. (The packet size does not change significantly.)

In wireless networks where devices on the network are compatible and security matters, WPA2/AES encryption should always be used. The weaker encryptions switch back the more modern devices, on the older devices do not give a significantly better rate, but their security is worse. If speed is more important than safety (e.g., media playback with wireless), with disabling the encryption 10-30 percent speed gain can be obtained.

After these results we can raise the question what is more responsible for slowing down the transmission speed, either the encryption or the full bandwidth of the device.

Acknowledgment. Tamás Krausz was supported by the TÁMOP 4.2.2. C-11/1/KONV-2012-0001 project. The project has been supported by the European Union, co-financed by the European Social Fund.

The work of János Sztrik was realized in the frames of TÁMOP 4.2.4. A/2-11-1-2012-0001 National Excellence Program – Elaborating and operating an inland student and researcher personal support system. The project was subsidized by the European Union and co-financed by the European Social Fund.

References

[1] Gin, R. Hunt, Performance Analysis of Evolving wireless IEEE 802.11 Security Architectures, The International Conference on Mobile Technology, Applications and Systems, ACM, Ilan, Taiwan, 2008.

[2] P. Georgopoulos, B. McCarthy, C. Edwards, *Providing Secure and Accountable Privacy to Roaming* 802.11 Mobile, ACM, MPM'12, Bern, 2012.

[3] Bruce Potter, Wireless Hotspots: Petri Dish of Wireless Security, *Communication of the ACM*, 2006, vol. 49, no.6, pp. 51–56.

[4] Samad S. Kolahi, Zhang Qu, Burjiz K. Soorty, and N. Chand, *The Performance of IPv4 and IPv6 using UDP on IEEE 802.11n WLANs with WPA2 Security*, ACM, 2009.

[5] T. Chenoweth, R. Minch, S. Tabor, Wireless Insecurity: Examining User Behavior on Public Networks, *Communication of the ACM*, 2010, vol. 53, pp. 134–138.

[6] Vivek Ramachandran, *BackTrack 5 Wireless Penetration Testing*, PACKT Publishing, 2011.

[7] Willie Pritchett, David De Smet, *BackTrack 5 Cookbooks, Networking & Telephony, Open Source*, PACKT Publishing, 2012.