Impact of Wireless Security Protocols on Data Throughput

Article · June 2018

CITATIONS
0

READS
788

1 author:

Ojo Ademola
Dominican University, Ibadan, Nigeria
30 PUBLICATIONS **65** CITATIONS

SEE PROFILE

Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 9 No. 2, June, 2018 - www.cisdijournal.org

Impact of Wireless Security Protocols on Data Throughput

Ojo Emmanuel Ademola
Professor and Chairperson
Centre for Citizenship and Leadership Galaxy
London, United Kingdom
E-mail: ojo_ademola@hotmail.co.uk

ABSTRACT

The benefits of the IEEE 802.11 Wireless LAN standard give reasons to its gaining global traction since 1997. Frequent improvement to the rule continues to permeate the wireless communication market. In this paper, a critical analysis that underscores the enterprise requirements for wireless systems, protocols information typically investigated. The recital of both IEEE 802.11b and 802.11g via the results of data throughput experiment carried-out on campus and the simulation results from a chosen article analysed. It also discusses the feebleness in WEP as the unproductive crack of the WPA and WPA2 confirmed the security vulnerabilities of WEP. The critical decisions about designing secure wireless networks could underline the global nature of WLAN standards and design. Finally, the paper discusses the comparison of results for the scenarios.

Keywords - IEEE 802.11bg, throughput analysis, WLAN.

CISDI Journal Reference Format
Ojo Emmanuel Ademola (2018): Impact of Wireless Security Protocols on Data Throughput
Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 8 No 1. Pp 1-12.
Available online at www.cisdijournal.org

1. INTRODUCTION

Models in the IEEE venture 802 focus on the physical layer (PHY) and medium access control (MAC) layer. At the point wireless local area network (WLAN) was first imagined, it appeared that it would be merely one more PHY of one of the accessibility guidelines. The primary hopeful considered for this was IEEE's most conspicuous usual 802.3 (Ethernet). Nonetheless, it before long ended up evidence that the radio medium is altogether different from the all-around carried on the wire. Because of gigantic lessening even finished short separations, collisions that exist go undetected. Henceforth, 802.3's carrier sense multiple access with collision detection (CSMA/CD) could not be connected.

The following competitor is typical to be well-thought-out as 802.4. Its organised medium access, the perfunctory transport idea, accepted to be better than 802.3's conflict-based plan. Thus, Hiertz et al. (2010) keep up that WLAN started as 802.4L. Nonetheless, since 1990, radio systems were troublesome as well as beneficial. The institutionalisation body understood that a WLAN standard would require its own MAC. At long last, on March 21, 1991, IEEE 802.11 protocol was affirmed.

The initial 802.11 standards were distributed in 1997. At the most reduced layer (PHY,) it gives three arrangements: a frequency hopping (FHSS) and a direct sequence spread spectrum (DSSS) PHY in the unlicensed 2.4 GHz band, and an infrared PHY at 316– 353 THz. Albeit every one of the three gives an essential information rate of 1 Mb/s with a discretionary 2 Mb/s mode, an infrared business user does not exist. Like 802.3, O'hara and Petrick (2005) show that essential 802.11 MAC works as indicated by a tune in before-talk plot and is known as the distributed coordination function (DCF). It actualises carrier sense multiple access with collision avoidance (CSMA/CA) instead of collision detection as in 802.3. To be sure, as collisions go undetected in the radio condition, 802.11 sits tight for a backoff interim before each casing transmission instead of after impacts. Notwithstanding DCF, the first 802.11 standard indicates a discretionary plan that relies upon a focal coordination element, thus, the point coordination function (PCF). This capacity utilises the purported point coordinator (PC), which works amid the alleged noninteroperable-free period. The last is an intermittent interim, the computer starts and outline trades using polling.

In any case, the PCF's weakened against concealed hubs that brought about unimportant reception by makers. Having distributed its initial 802.11 standards in 1997, the Working Group (WG) had the input that numerous items did not give the level of comparation clients anticipated. For instance, regularly the evasion encryption scheme, termed Wired Equivalent Privacy (WEP), would not function amongst gadgets of various merchants. This requirement for an affirmation package prompted the establishment of the Wireless Ethernet Compatibility Alliance (WECA) in 1999, retitled as Wi-Fi Alliance (WFA) in 2003. Wi-Fi affirmation has turned into an outstanding confirmation project that has noteworthy enterprise impact. The alliance introduced an interim solution WEP called Wi-Fi protected access (WPA). WAP aimed to discourse some of the susceptibilities of WEP awaiting the ratification of 802.11i. This 802.11i embraces pre-RSNA set-of-rules. At the acceptance of 802.11i, WFA released WPA2. The enormous achievement in the market and the apparent inadequacies of the base 802.11 standards gave a premise and driving force to a productive programme of changes and expansions. Indeed, this prompted variously approved modifications of the draft, inspired by an entire notion of revisions. Hiertz et al. (2010) show series of tables to delineate the complete history of this procedure.

In this paper, the concert of IEEE 802.11bg at the MAC sub-layer, concerning QoS, by the results of data throughput experiment carried-out on campus and the simulation results from a chosen article analysed. It also discusses the weaknesses in WEP as there was a crack attempt of the WPA and WPA2. The unsuccessful attempts to crack WAP and WPA2 are confirmations to underscores the security vulnerabilities of WEP. The critical decisions about designing secure wireless networks could underline the global nature of WLAN standards and design. Nonetheless, Pahlavan and Krishnamurthy (2011) argue that standardisation provides interoperability, faster product development, stability, ability to upgrade, and cost reduction. These are the benefits of IEEE 802.11 protocols that made them so globally deployable in communication markets. The analysis presents the comparison of results for the on-campus experiment results as well as the simulation results modelled by Athanasopoulos and colleagues (Athanasopoulos et al. 2006). Finally, the paper discusses the impact of security on the throughput of 802.11 standards as well as compare results extracted from research.

2. THROUGHPUT WITH/WITHOUT SECURITY EXPERIMENTS

In this section, two experiments were carried out in the research Centre to look at and analyse the information and channel bit rates of the 802.11b and 802.11g protocols. The throughputs were estimated utilising "JPERF", and "IPERF" traffics. There was as an attempt to screen the remote traffics. With WEP and WPA2 enabled, two access points and a network card that works in "promiscuous mode" were used to scan all networks and sniffed the packets. Li et al. (2018) proposed that the communication between a wireless client and an access point is represented by the stern arrangement of etiquettes that presents settled adjournments in the communication channel. This examination analysed the effect of WEP and WPA2 safety conventions on the information throughputs in IEEE 802.11b contrasted with the effect of the information throughputs in 802.11g. The examinations were performed utilising "Bi-directional Transmission Control Protocol (TCP)" Window size and "User Datagram Protocol (UDP)" IPERF traffics. It investigated information bundles and bit rates of the IEEE 802.11b and 802.11g without security as well as with the WEP and WAP2 security protocols activated.

2.1 Experiment Configuration

Figure 1 depicts the setup of the experiment. The PC setup with Linux operating systems, meaning that the investigations used the "Linux Server and Client". One server is serving two clients. The IPERF installed to measure the bandwidth and the quality of a network link; Chen and Law (2007) assert that IPERF creates traffic as well as to help investigate the communication channel frame-error-rate (FER). With FER, it becomes apparent to report datagram loss in the wireless link, a primary function used to calculate throughput performance. BThub and TPlink were interchangeably used as the access points. The respective access points were at the alternative time configured with and without security. With WEP and WPA2 set as security protocols to determine the impact of security on the 802.11b and 802.11g. Accessibility to the network through passwords encrypted using the WEP and WPA2 protection as installed penetration test tools applied to crack the passwords for unauthorised access to the system. Arkin et al. (2005) accentuate that penetration test tools are essential software applications helping to fulfil an overall enterprise functional business requirement.

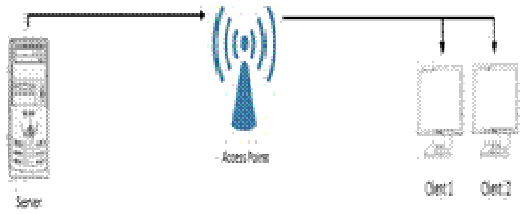

Figure 1: Experiment setup

2.2 Data Capturing

In the interest of comparation, three levels of data acquisition avail to accentuate the experiment data collection process. The data from an on-campus experiment conducted, shared data and simulation result. The holistic approach to data collection could present an opportunity for a researcher to wholly compare data from different scenarios of the same topology to critically analyse the performance of both protocols.

2.2.1 Experiment Data Collection

The experiment was conducted five times using the Bi-Directional traffic with and without WEP and WPA2 security. The data collection columns are the data transfer in Mbytes and data rate in Mbps, and the average subsequently calculated. Tables 1 and 2 show that the experiment performed five times for the UDP and TCP traffics generated by IPERF and standards took respectively.

Table 1: Average IEEE 802.11b for TCP/UDP Traffic On-Campus Experiment

Protocol	Item Description	No Security	WEP	WPA2
802.11b	Average TCP	4.4	3.78	5
	Average UDP	9.27	9.23	9.42

Table 2: Average IEEE 802.11g for TCP/UDP Traffic On-Campus Experiment

Protocol	Item Description	No Security	WEP	WPA2
802.11g	Average TCP	12.9	5.84	12.8
	Average UDP	10	8.66	10

2.2.2 Shared Data

Following the same process in 2.2.1, consent of the original data collector sought and gotten. Tables 3 and 4 show a similar acquisition to Tables 1 and 2.

Table 3: Aberage IEEE 802.11b for TCP/UDP Traffic and Impact of Security

Protocol	Item Description	No Security	WEP	WPA2
802.11b	Average TCP	3.98	3.41	3.03
	Average UDP	7.53	8.01	9.35
	Dropped TCP%	0%	14.32%	23.87%
	Dropped UDP%	0%	-6.37%	-24.17%

Table 4: Aberage IEEE 802.11g for TCP/UDP Traffic and Impact of Security

Protocol	Item Description	No Security	WEP	WPA2
802.11g	Average TCP	12.6	4.71	2.4
	Average UDP	10	5.06	6.18
	Dropped TCP%	0%	62.62%	80.95%
	Dropped UDP%	0%	49.40%	38.20%

Table 4: Average IEEE 802.11g for TCP/UDP for Traffic and impact of security

2.2.3 Simulation Result

Athanasopoulos et al. (2005) use the C++ wireless simulator and OPNET v.11.0 for valuation of the performance of IEEE 802.11b and IEEE 802.11g protocols. The simulation result of their work noted and used in this paper for contrast purposes. Figures 2 to 5 depict corresponding contributions of various input to the throughput calculation and analysis.

2.3 Throughput Analysis

In Figure 2, the experiment depicts that the transfer rate of 802.11g tends to be higher than that of the 802.11b. An exception exists when the protocols are using the UDP traffic and secured with WEP, where the 802.11b protocol has the faster transfer rate, 9.23 Mbits/Second in comparison to the 802.11g's 8.66 Mbits/Second.

The fastest rate of data transfer for the 802.11g occurs when no security is applied to the standard at 12.9 Mbits/Second, while the quickest rate of transmission for the 802.11b wireless protocol occurs when the WPA2 security used and the UDP traffic in play, at 9.42 Mbits/Second. Some corresponding changes noted in throughput performance appreciably indicates compatibility that exists between IEEE 802.11b and IEEE 802.11g.

The slowest rate of transfer for the 802.11g protocol occurs when WEP security is applied, and the TCP transfer protocol used, the speed recorded at 5.84 Mbits/Second. Similarly, for the 802.11b protocol, the slowest speed occurs in the same conditions for the 802.11g's standard, at rates of 3.78 Mbits/Second.

Notably, another pattern that shows the TCP traffic, the rate of transfer tends to have slower compared to the UDP traffic in WLAN. This outcome allows for the comparisons that may exist between theoretical throughputs and experimental throughputs obtained when security is enabled or not. Whatever it is, it has been argued, (Barka and Boulmalf 2007; see also Chen and Law 2007), that throughput can be improved and predicted when security policies are enabled and sufficiently defined irrespective of the vulnerabilities associated with the IEEE 802.11 protocols.

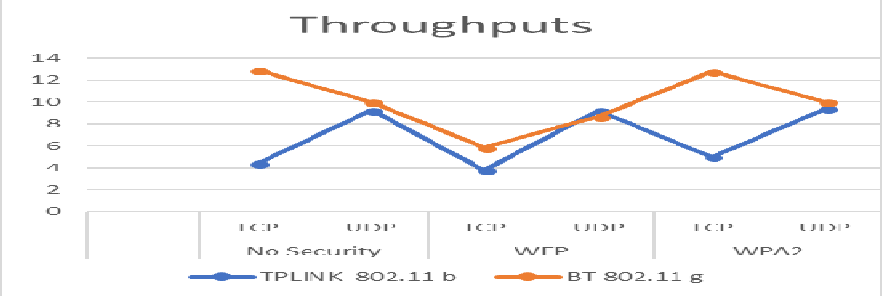

Figure 2: IEEE 802.11b Versus 802.11g

Figures 2 and 3 show that variations in throughput performance for most IEEE 802.11 protocols could be higher when security policies are allowed. Agarwal and Wang (2005) demonstrate that depending on the TCP/UDP traffic streams, the throughput performance of IEEE 802.11 protocols could improve when outcome relate effectively to QoS.

Agarwal and Wang, notwithstanding, contended that "No Security" scenarios causes analysts to contrast the overhead and other security benefits regarding end-to-end reaction time, throughput and other conventional issues. It is a view supported by the outcome of this investigation. Similarly, the results presented in Table 3 shows the throughput performance when observed at security enabled scenarios. Figure 3 depicts that with IEEE 802.11b for the TCP traffic, the throughput ached a decrease of 14.32% when WEP enabled and a 23.87% when WPA2 used as the encryption algorithm. It also illustrates that for UDP traffic, the throughput in contrast improved with a 6.37%; a further increase of 24.17% noted when WPA2 enabled.

Likewise, Figure 4 shows that IEEE 802.11g the TCP traffic for throughput had suffered a decrease of 62.62% when WEP enabled and a further 80.95% when WPA2 enabled. The result depicts that for UDP traffic the performance started a decline from 49.4% to 38.20% when WEP WPA2 respectively enabled. Figure 5, however, shows a throughput pattern for TCP and UDP traffics for both protocols; with an opened security, WEP and WPA2 enabled. Reasons for such throughput behaviour could provide evidence for why these variants of 802.11 suffered security distrust in the market between 2000 and 2002.

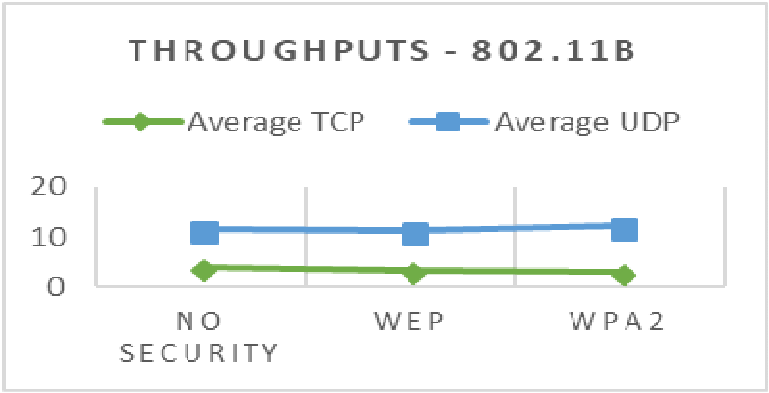

Figure 3: IEEE 802.11b

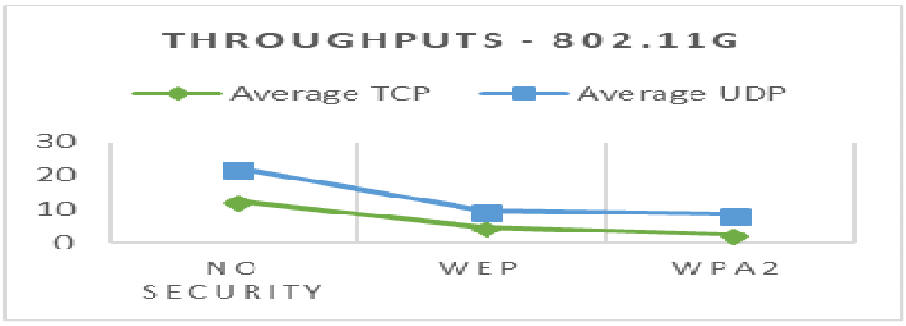

Figure 4: IEEE 802.11g

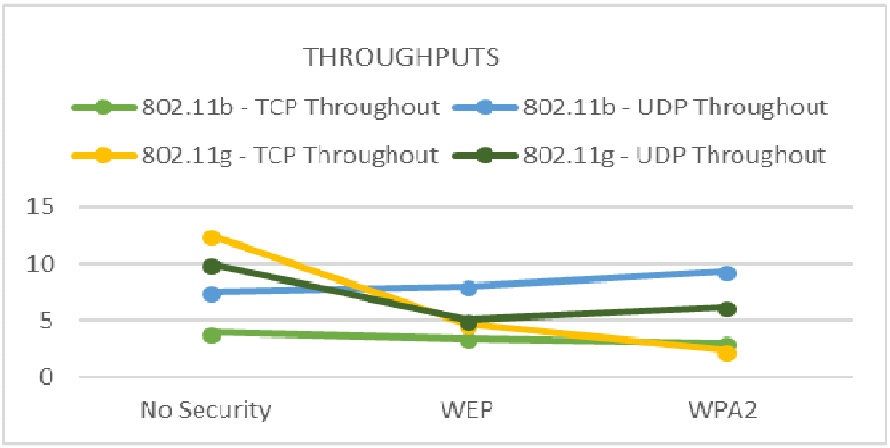

Figure 5: Throughput for IEEE 802.11b/g combined

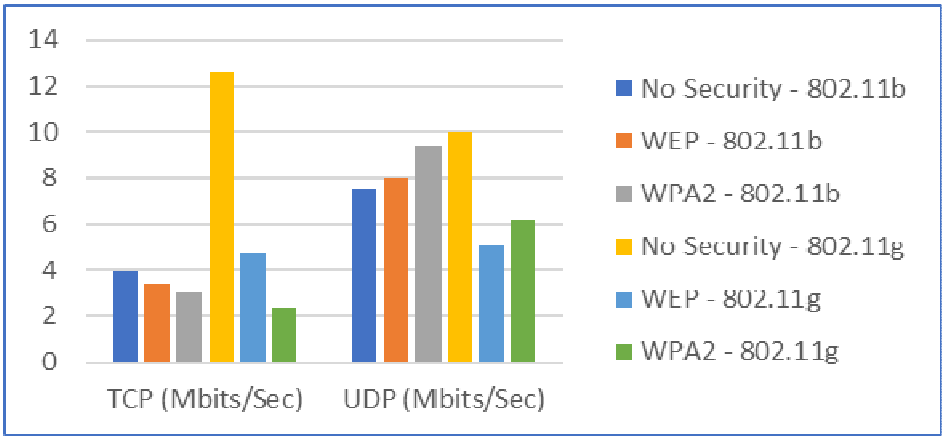

Figure 6: Throughput graphical analysis

As shown in Figure 6, there exists a link between IEEE 802.11bg when the open network, WEP and WPA2 enabled. It becomes apparent as well as allowed for further analysis regarding security.

Nonetheless, further analysis of the simulation results of Athanasopoulos et al. (2005), provide an opportunity for comparation. The 802.11b appears to have a similar execution with topology and activity situations, while the 802.11g seems to perform inadequately when concealed hubs are in use within the topology situation. This perception matches with the desires that emerge from the possible piece of throughput execution and the portrayals of the MAC layer security components. In this manner, 802.11b protocols would have steadier throughput performance and QoS qualities. Considering the autonomous of contracts topology and information activity, while 802.11g standards appear to be vulnerable when presented to shrouded hub issue, 802.11b retains it QoS and negate security vulnerability that is apparent.

Overall, with IEEE 802.11bg, theoretically and practically, WLAN users will notice that average actual data throughput (27 Mbps for IEEE 802.11b and 20-25 Mbps for IEEE 802.11g), as shown via the clients on a WLAN only approaches half of this esteem and unfluctuating less. Clients mostly attribute this drop to failing of protocols to meet expectations. However, this is typically not the situation. The lower throughput rate is primarily because of the MAC layer overheads in the 802.11 design and is in this manner purposeful. It is an outcome that agreed with El Hajjar (2018) that, correspondence between a wireless client and an access point usually governed by a firm procedure of conventions that presents settled delays in the correspondence channel. The adjournments do not change fundamentally regardless of quicker channel bit rates. Thus, both protocols are compatible, though the maximum users per access point vary; 32 users for IEEE 802.11b and 64 users for IEEE 802.11g. Could this dictate the cost? IEEE 802.11g is more expensive than IEEE 802.11b, a fact for the market popularity of IEEE 802.11b (Wi-Fi).

3. WEP ALGORITHM AND SECURITY EXPERIMENT ANALYSIS

Figure 7 shows that the WEP key was 100% decrypted correctly. The researcher succeeded in WEP cracked project because of the vulnerability noted with the WEP algorithm. To clarify these vulnerabilities with the Wired Equivalent Privacy (WEP) algorithm, which is part of the 802.11 protocol, the exposure of various security flaws became essential. The vulnerabilities related with WEP algorithm opens its application to different security assaults. The attacks include (1) potential attacks to unscramble traffic considering numerical scrutiny. (2) active attacks to inoculate new truck from unapproved portable stations based on acknowledged plain-text. (3) dynamic assaults to decode activity, because of deceiving the access point. (4) a dictionary-building attack that, after examination of about multi-day of operation could permit continuous mechanised decoding of all traffic.

Attacks conceivable with WEP algorithm are viable to mount just reasonable off-the-rack gear. Accordingly, anybody utilising 802.11 protocols must not depend on WEP for security but should employ other safety efforts to protect their WLAN. The outcome indicates that the attacks underscored could apply to both 40-bit and the supposed 128-piece forms of WEP. They likewise apply to systems that utilise 802.11b as an augmentation to 802.11 conventions to improve throughputs; consequently, it leaves the WEP algorithm unaltered.

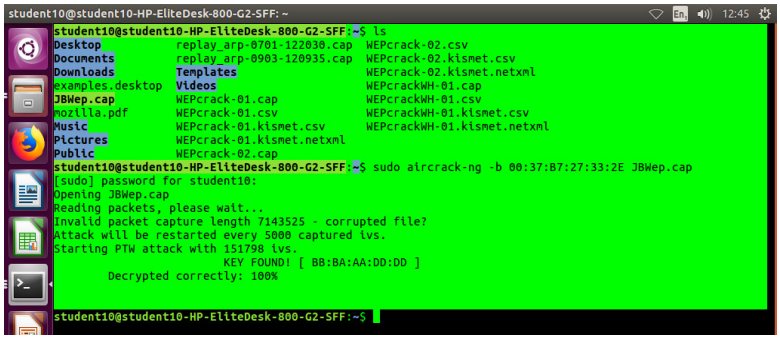

Figure 7: A WEP Cracked

3.1 WEP Setup

Considering the WEP configuration, the 802.11 typically portrays the correspondence that happens in WLANs. The WEP algorithm designs to shield wireless communication from eavesdropping. An optional capacity to avoid unapproved access to a WLAN. This capacity is not a clear objective in the 802.11 standards. However, it is regularly thought to be an element of WEP. WEP depends on a mystery key that is shared between a versatile station (e.g. a workstation with a remote ethernet card) and a passage (i.e. a base station). The secret key is utilised to encrypt packs before they are communicated, and integrity check is used to guarantee that parcels are not altered in travel. The standard does not talk about how the mutual key is set up. Practically speaking, most establishments utilise a single core that is shared between every only portable station and access points. More complex key administration strategies can be used to help shield from the assaults depicted in this paper; notwithstanding, no business framework noted has components to improve such methods.

3.2 WEP security problem

The successful cracking of WEP is a confirmation of vulnerabilities identified with it. The algorithm utilises the RC4 encryption, which is known as a stream cipher. A stream cipher works by extending a short key into an endless crucial pseudo-arbitrary stream. With the plaintext, the sender XORs the key stream to make ciphertext. The receiver has a duplicate of an exact key and uses it to produce the same keystream. XORing the keystream with the ciphertext yields the first plaintext. The method makes stream ciphers helpless against a few assaults. On the off chance that an aggressor flips a bit in the ciphertext, at that point upon decryption, the comparing bit in the plaintext will be flipped. Additionally, Zahur and Yang (2004) suggest that if a spy blocks two ciphertexts encrypted with a similar crucial stream, it is conceivable to get the XOR of the two plaintexts. It is a view shared by El Hajjar (2018), that the learning of this XOR can enable statistical attacks to recuperate the plaintexts. The statistical attacks are experimentally on the increase as more ciphertexts utilise a similar keystream is known. Agarwal and Wang (2005) note that when one of the plaintexts winds up is known, it is insignificant to recoup all the others.

Notably, WEP has guarded against the two assaults. To guarantee that a packet has not been adjusted in travel, it utilises an Integrity Check (IC) field in the bundle. An Initialisation Vector (IV) is employed to augment the shared secret key and deliver an alternative to abstain from encoding two ciphertexts with a similar keystream. It is an RC4 key for every packet. The IV is likewise incorporated into the bundle. Several researchers, for example, (Vibhuti 2005; see also Miller 2003), that in any case, the two measures are executed mistakenly, bringing about inadequate security.

Another level of WEP vulnerability is the implementation of the CRC-32 checksum. It is an application to represent an integrity check field. It is a piece of the encrypted payload of the bundle depending on WEP security policies. In any case, CRC-32 is linear, which implies that it is conceivable to figure the bit contrast of two CRCs considering the bit distinction of the messages over which they are taken. Flipping bit 'n' in the word brings about a deterministic arrangement of bits in the CRC that must be turned to create a right checksum on the altered message. Since flipping bits brings through, after RC4 encryption, it enables an aggressor to flip self-assertive bits in an encoded signal. This effectively changes the checksum with the goal that the subsequent message seems legitimate.

The WEP initialisation vector (IV), a 24-bit field is sent in the cleartext fragment of a communication. The little space of IVs ensures the reuse of an exact keystream. A bustling access point, which continually transmits several byte bundles at 11Mbps, will deplete the area of IVs in succession of appropriately 18000 seconds or 5 hours. Correspondingly, the measure of time might be significantly littler since various bundles are littler than 1500 bytes. It enables an assailant to gather two ciphertexts that are scrambled with the same keystream and perform statistical attacks to recoup the plaintext. More terrible, when every single versatile station utilises an exact key, there are other odds of IV crash. For instance, a typical remote card from lucid resets the IV to 0 each time a card is instated and additions to the IV by 1 with every packet. This implies two cards embedded at generally a similar time will give a wealth of IV impacts for an attacker. More regrettably still, Hiertz et al. (2010) noted that the prior 802.11 protocol indicates that changing the IV with every packet is discretionary!

3.3 WEP Attacks and Remedies

The process that led to the WEP cracked evidence provided in Figure 7 entails a passive attack to decrypt a stream of traffic. In other words, a passive eavesdropper can intercept all wireless traffic, until an IV collision occurs. It was an approach adopted with the WEP cracked experiment carried out on campus by the researcher. Deductively, if a XORing two packets use the same IV, the attacker could obtain the XOR of the two plaintext messages. The resulting XOR can, therefore, lead to infer data about the contents of the two words. By observation, IP traffic is often very predictable and includes a lot of redundancy as depicted in the WEP cracking lab experiment. When an attacker intercepts the encrypted version of his or her message sent over 802.11 protocol, he or she could decrypt all packets that use the same IV.

Other notable attacks following the problems associated with WEP security algorithm includes an active attack to inject traffic, aggressive attack from both ends, and table-based attack. With adequate experimental monitoring, some researchers, (Barka et al. 2006; see also Barka and Boulmalf 2007), noted that attacks on WEP became possible due to the apparent vulnerabilities associated with it. The prior 802.11 protocol security's issues are a consequence of misconception of some cryptographic natives and in this manner joining them in uncertain ways. These attacks point to the significance of welcoming open audit from individuals with skill in cryptographic convention configuration; had this been done, there might not be noticeable at this level for such security issues.

4. IMPACT OF SECURITY ON THROUGHPUT OF 802.11: AN ANALYSIS

As underscored in sections 2.0 to 3.3 of this work, the underlying 802.11 standard's encryption plot WEP caused a great deal of security inconvenience in the market. Because of poor cryptographic configuration, results of various merchants were likely not to be interoperable. In this manner, numerous networks operated non-encrypted. From the get-go in 2001, Borisov et al. (2001) displayed that the reports on WEP security shortcomings happened. Also, its preshared keying idea did not take into consideration mix into big business systems, where every gadget ought to have its unique key. Subsequently, organisations required their workers to utilise IP-based virtual private networks (VPNs), and 802.11 turned into an equivalent word for frailty. Even though the foundation of 802.11i pulled in numerous security specialists, the market did not sit tight for an answer.

Consequently, WFA began its Wi-Fi Protected Access (WPA) accreditation rollout. According to Hiertz et al. (2010), the accreditation programme helps to take into consideration firmware-just, hardware-compatible updates of existing gadgets, as WPA does not depend on new encryption plans. Like WEP, the supposed Temporal Key Integrity Protocol utilises RC4 for encryption. Be that as it may, numerous points of interest of key in statement and restoration remain dynamic. WFA's WPA2 signifies the last 802.11i alteration that incorporates an extra encryption scheme planned to start with no outside help. Imperatively, the new plan depends on the Advanced Encryption Standard (AES), duly characterised and greater security accomplished. Old communication facilities, be that as it may, cannot be overhauled. The latest security-related correction was distributed in September 2009. 802.11w targets authenticated and encrypted management frames. Even though administration outlines don't convey client information, extortion may cause disengagement and opens the entryway for wireless denial of service attacks. Subsequently, 802.11w is stretching out the 802.11i structure to close the hole. Some researchers, (Kolahi et al. 2009; see also Baghaei et al. 2004), propose that the provision within 802.11n as an amendment that improves security upon the previous IEEE 802.11 protocols.

Undoubtedly, the addition of multiple-input-multiple-output (MIMO) antennas contributes to a higher throughput performance. As the first venture whose focused information rate of estimation over the MAC layer. IEEE 802.11n gives the client the possible encounter identical to the outstanding of Fast Ethernet (802.3u). A long way past the bare necessities that were gotten from its wired paragon's most extreme information rate of 100 Mb/s, 802.11n conveys up to 600 Mb/s. Its most distinct element is MIMO capacity. An adaptable MIMO idea considers varieties of up to four reception apparatuses that empower spatial multiplexing or bar framing. Its most faced off regarding development is the use of discretionary 40 MHz channels. Even though this component was at that point being, utilised as an exclusive augmentation to 802.11a and 802.11g chipsets. It caused a full talk on neighbour well-disposed conduct. Mainly for the 2.4 GHz band, concerns were raised that 40 MHz activity would immensely influence the throughput performance of existing 802.11, Bluetooth (802.15.1), ZigBee (802.15.4), and different gadgets. The improvement of a trade-off, which prohibits 40 MHz channelisation for devices that can't identify 20 MHz-just gadgets, counteracted endorsement of 802.11n until September 2009.

Subsequently, the 20/40s MHz activity and different receiving wire designs, 802.11n characterises a sum of 76 distinctive MCSs. Since a few of them give comparable data rates, WFA's accreditation scheme chooses the MCSs at long last utilised as a part of the market. 802.11n's PHY improvements are bolstered by medium access upgrades as presented in the MAC segment. Thinking about the development of 802.11ac and 802.11ad corrections, Eastwood et al. (2008) state that the alterations accomplished through 802.11ac and 802.11ad satisfy the International Telecommunication Union's (ITU's) prerequisites on recommendations for the IMT Advanced standard. Both target more prominent than 1 Gb/s throughput.

Eastwood and colleagues underlined that while 802.11ac considers the common WLAN frequencies underneath 6 GHz, 802.11ad contends with the Wireless Personal Area Network Task Group (TG) 802.15.3c, standard ECMA 387, and the Wireless Gigabit Alliance on the 60 GHz recurrence range. Because of their awkward stage, both TGs are still during the time spent gathering info and recommendations from their individuals. Presently, related articles considering 802.11ad has just begun to characterise some additional prerequisites regarding no less than 10 m at 1 Gb/s. It is a consistent exchange of a functioning session from the 60 GHz band to the 2.4/5 GHz band and in the opposite way. In conjunction with different frameworks in the group, for example, 802.15.3c, and IEEE 802.11i, Athanasopoulos et al. (2006) consider the development as a bolster for uncompressed video necessities, and MAC expansions for better information security for improved throughput performance in security mindfulness.

5. EXPERIMENT RESULTS GAINED IN COMPARISON WITH RESEARCH

Based on the analysis of the impact of throughput of IEEE 802.11b and IEEE 802.11g discussed in the earlier section, there is a basis for comparison with research of what the conclusions might entail. Research centres on various IEEE 802.11 security vulnerabilities when using WEP and how these are both theoretically and practically managed cost-effectively. For instance, an unsuccessful attempt to crack a wireless network when WPA2 in use remains a confirmation of security mindfulness in the market communication. Some researchers, for example, (Barka and Boulmalf 2007; see also Baghaei and Hunt 2004; Kolahi et al. 2009), have agreed the various experimental results gained, accentuate IEEE 802.11 wireless security and throughput performance.

The overall observations taken from the lab experiment results compared with Barka and Boulmalf outcome on the effect of encryption on the throughput of design framework WLAN IEEE 802.11g concurred. Both works noted that: Throughput decreases when security, WEP, is enabled. It is observable that the encryption operations performed by this protocol increases the amount of data transmitted and slows down the rate of data being sent or received (see Figures 2 and 6). For WEP when the critical size builds the throughput marginally diminishes. It depicts the possibility since WEP includes the Initial Value of its symmetric encryption key to the information sent. Furthermore, it utilises whatever remains of the key bits to start a key planning algorithm that creates a stream key for the stream information to be XORed successful. The usual procedure of the RC4 encryption algorithm can force a specific measure of delay. According to El Hajjar (2018), "the lower throughput rate is primarily due to the MAC layer overheads in the 802.11 architecture and is therefore intentional." Moreover, with the communication between a wireless client and an access point, El Hajjar underscores that by governance, there exist a strict arrangement of conventions that present settled postponements in the communication channel. It slows the sending of information after encryption received then decrypted.

In the wireless to a wireless environment, Agarwal and Wang (2005) noted that "the throughput suffered more degradation than that in the wireless to the wired environment." When WEP and WPA2 enabled, for example, the remote to the remote condition, there are twofold encryptions which came about because of having two air interfaces with one access point. Nonetheless, Lopez et al. (2018) expose some of the WPA2 vulnerabilities and recommend possible remedies within the Colombian service providers. Due to the unsuccessful attempt to crack WPA2, this work considers it an area for further research notwithstanding the research outcome. Even with multiple clients, Baghaei and Hunt (2004) observe a similar WLAN security and throughput performance. Some researchers, (Xiao 2005; see also Kolahi et al. 2009) note the high possibility of enhancements for higher throughput when IEEE 802.11n enabled. Overall, throughput behaviour depends on the characteristics of the IEEE 802.11 protocol, and whether the security WEP and WPA2 in use.

6. CONCLUSION

In conclusion, having considered both the theoretical and practical effect of security on the throughput execution of the IEEE 802.11b and IEEE 802.11g, the security vulnerabilities are for the most part managing the market prominence. The IEEE 802.11 standard and its changes give a rich list of capabilities to WLAN. Independent, 5, 10, 20, and 40 MHz linear transfer speed in the 2.4, 3.65, and 4.9– 5 GHz recurrence groups bolster an extensive variety of administrative spaces. Moreover, the 802.11 MAC has ended up being sufficiently adaptable to extend from its hereditary market portions. While IEEE 802.11n and work systems expand plainly understood applications, full range IEEE 802.11 standard and vehicular correspondence options open new situations for WLAN. In any case, the expanding measure of alterations additionally makes it harder to keep up a reliable standard. Work on the most recent changes tends to take longer than those before. In any case, there is no apparent alternative to the famous, shabby, and adaptable 802.11 innovation is noticeable yet. An incredible opposite, driven by clients' complex needs, the 802.11 universe keeps on growing. Thus, the need for further research to enhance throughput performance with strict security policies in protocols enabled is ever on the alert theoretically and practically.

REFERENCES

1. Agarwal, A.K. and Wang, W., 2005, October. Measuring the performance impact of security protocols in wireless local area networks. In Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on (pp. 581-590). IEEE.
2. Arkin, B., Stender, S. and McGraw, G., 2005. Software penetration testing. IEEE Security & Privacy, 3(1), pp.84-87.
3. Athanasopoulos, A., Topalis, E., Antonopoulos, C. and Koubias, S., 2006, April. Evaluation Analysis of the Performance of IEEE 802.11 b and IEEE 802.11 g Standards. In null (p. 141). IEEE.
4. Baghaei, N. and Hunt, R., 2004, November. IEEE 802.11 wireless LAN security performance using multiple clients. In Networks, 2004.(ICON 2004). Proceedings. 12th IEEE International Conference on (Vol. 1, pp. 299-303). IEEE
5. Barka, E. and Boulmalf, M., 2007, March. Impact of encryption on the throughput of infrastructure WLAN IEEE 802.11 g. In Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE (pp. 2691-2697). IEEE.
6. Barka, E., Boulmalf, M., Alteniji, A., Al Suwaidi, H., Khazaimy, H. and Al Mansouri, M., 2006, November. Impact of Security on the Performance of Wireless-Local Area Networks. In Innovations in Information Technology, 2006 (pp. 1-5). IEEE.
7. Borisov, N., Goldberg, I. and Wagner, D., 2001, July. Intercepting mobile communications: the insecurity of 802.11. In Proceedings of the 7th annual international conference on Mobile computing and networking (pp. 180-189). ACM.
8. Chen, C. and Law, C.L., 2007, December. Throughput performance analysis and experimental evaluation of IEEE 802.11 b radio link. In Information, Communications & Signal Processing, 2007 6th International Conference on (pp. 1-5). IEEE.
9. Eastwood, L., Migaldi, S., Xie, Q. and Gupta, V., 2008. Mobility using IEEE 802.21 in a heterogeneous IEEE 802.16/802.11-based, IMT-advanced (4G) network. IEEE Wireless Communications, 15(2).
10. El Hajjar, A. 2018. COURSEWORK Assignment Specification. [online] Northumbria University Newcastle. Available at: https://elp.northumbria.ac.uk/bbcswebdav/pid-5202619-dt-content-rid-16297506_2/courses/2017S03_LD7008FVZ31/Assignment%20-%20Jan%2018-PT.pdf [Accessed 10 Jul. 2018].
11. Hiertz, G.R., Denteneer, D., Stibor, L., Zang, Y., Costa, X.P. and Walke, B., 2010. The IEEE 802. 11 universe. IEEE Communications Magazine, 48(1), pp.62-70.
12. Kolahi, S.S., Qu, Z., Soorty, B.K. and Chand, N., 2009, December. The Impact of Security on the Performance of IPv4 and IPv6 Using 802.11 n Wireless LAN. In NTMS (pp. 1-4).
13. Li, Y, El-Hajjar, M, & Hanzo, L 2018, 'Joint Space-Time Block-Coding and Beamforming for the Multiuser Radio Over Plastic Fiber Downlink', IEEE Transactions on Vehicular Technology, vol. 67, no. 3, pp. 2781-2786. Available from: 10.1109/TVT.2017.2723876. [4 July 2018].
14. López, A.A., Monroy, E.Y.M. and Murcia, P.A.L., 2018. Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools. Facultad de Ingeniería, 27(47), pp.71-78.
15. Miller, S.S., 2003. Wi-Fi Security (Vol. 101). New York: McGraw-Hill.
16. O'hara, B. and Petrick, A., 2005. IEEE 802.11 handbook: a designer's companion. IEEE Standards Association.
17. Pahlavan, K. and Krishnamurthy, P., 2011. Principles of wireless networks: A unified approach. Prentice Hall PTR.
18. Vibhuti, S., 2005. IEEE 802.11 WEP (Wired Equivalent Privacy) concepts and vulnerability. San Jose State University, CA, USA, CS265 Spring.
19. Zahur, Y. and Yang, T.A., 2004. Wireless LAN security and laboratory designs. Journal of Computing Sciences in Colleges, 19(3), pp.44-60.