International Journal of Academic Multidisciplinary Research (IJAMR)
ISSN: 2000-006X
Vol. 2 Issue 4, April – 2018, Pages: 19-27

Wireless Network Security: Challenges, Threats and Solutions. A Critical Review

[1]Lusekelo Kibona, [2]Hassana Ganame

[1]Department of Computer Science, Ruaha Catholic University (RUCU), Tanzania,
lusekelo2012@gmail.com
[2]Department of Information and Telecommunication, School of Engineering of Bamako, Mali
ganame_hassana@yahoo.fr

Abstract: *Wireless security is the avoidance of unlawful access or impairment to computers using wireless networks. Securing wireless network has been a research in the past two decades without coming up with prior solution to which security method should be employed to prevent unlawful access of data. The aim of this study was to review some literatures on wireless security in the areas of attacks, threats, vulnerabilities and some solutions to deal with those problems. It was found that attackers (hackers) have different mechanisms to attack the networks through bypassing the security trap developed by organizations and they may use one weak pint to attack the whole network of an organization. However the author suggested using firewall in each wireless access point as the counter measure to protect data of the whole organization not to be attacked.*

Keywords - Wireless network, network security, WAP2, WEP, hackers, Firewall

1. INTRODUCTION

Wireless network is a network set up by using radio signal frequency to communicate among computers and other network devices, sometimes it is referred as Wi-Fi network or WLAN and it is getting popular nowadays due to easy setup feature and no cabling involved [1]. Wireless Internet access technology is being gradually arrayed in both office and public surroundings, as well as by the Internet users at home.

With continual advances in technology, coupled with increasing price/performance advantages, wireless accessibility is being deployed increasingly in office and public environments. This new era of technological flexibility can also provide an open invitation for network security threats not only in the corporate world, but also the privacy of users at home.

When the decision is made to move from a physically connected architecture to wireless LAN technology, component accessibility and signal propagation provided convenient opportunities for unauthorized users to introduce malicious activities, intercept data transmission, or passively eavesdrop upon the infrastructure of a system

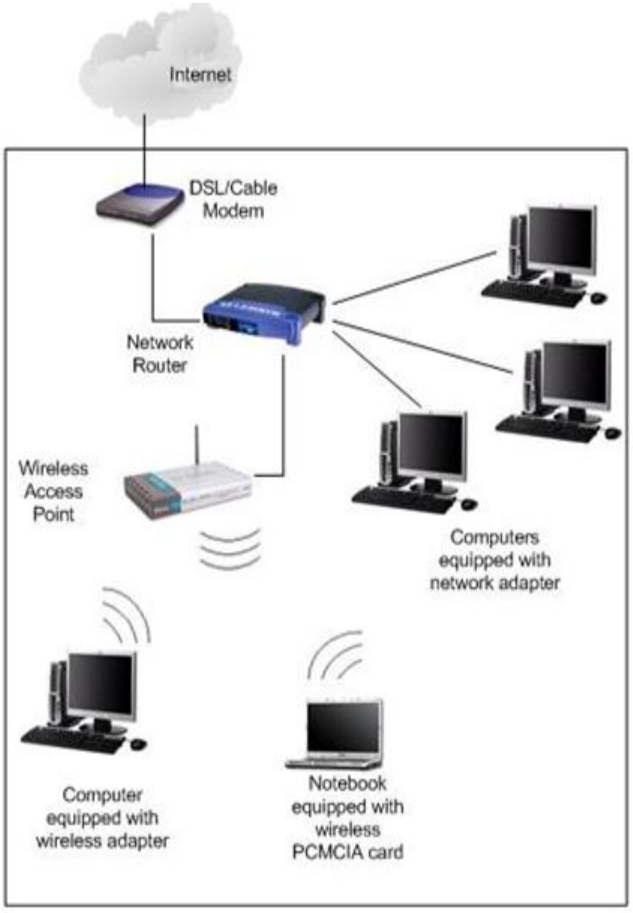

Figure 1: Showing the architecture of wired network and wireless network (for devices accessing Wireless Access Point) [1].

In Figure 1, both wired network and wireless network get data to be communicated among the laptops/computers or any mobile devices from the router, for wireless network the wireless access point provide data access for laptops but for wired network the router provides data access to laptops/computers. Both (wired network and wireless network) require resolute confidentiality with no violations to system integrity, while continuing to sustain access to information and related systems for authorized users.

The pervasive availability and wide usage of wireless networks with different kinds of topologies, techniques and protocol suites have brought with them a need to improve security mechanisms [2].

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) [3]. It requires different thinking from wired network security as it gives hackers or attackers an easy transport medium access and this access increases the threat that any security architecture must deal with.

Wireless security on the IEEE 802.11 standard has received a lot of critics, because it is has got several design errors and security problems.

In dealing with wireless network security availability, authenticity, integrity, confidentiality and non-repudiation are very important aspects to deal with because any effective wireless network security must make sure [4]:

Availability: guarantees that the desired network services are available whenever they are expected, in spite of attacks. Systems that ensure availability seek to combat denial of service and energy starvation attacks.

Authenticity: guarantees communication from one node to another is genuine. It ensures that a malicious node cannot masquerade as a trusted network node.

Confidentiality: is a core security primitive for ad hoc networks, It guarantees that a given message cannot be understood by anyone else than its (their) desired recipient(s).

Integrity: denotes the authenticity of data sent from one node to another. That is, it guarantees that a message sent from node A to node B was not modified by a malicious node, C, during transmission.

Non-repudiation: guarantees that the origin of the message is legitimate. i.e when one node receives a false message from another, nonrepudiation allows the former to accuse the later of sending the false message and enables all other nodes to know about it.

According to the above security problems, the main objective of this research was to identify principle elements related to wireless network security and provide an overview of potential threats, vulnerabilities, and countermeasures (solutions) associated with wireless network security.

2. BACKGROUND AND LITERATURE SURVEY

a) NETWORK SECURITY CHALLENGES, ATTACKS AND THREATS

According to [1], the threats in the network were not known to public people till prices of wireless equipment went down around 2000, before that date, the military was the number one client for wireless security products especially during the cold war but now days every person, company and even military are very much aware of network security.

In his paper titled "*What is computer security?* " [2], asked several questions, such as what exactly the network infrastructure is, what threats it must be secured against, and how protection can be provided on a cost-effective basis, but underlying all these questions is how to define a secure system.

As per [3], Denial of Service (DoS) attack is the most severe security threat among various security risks, because DoS can compromise the availability and integrity of broadband wireless network.

[4], discussed about computing as the most new technology adopted in the wireless network today in the case of shift of information technology but security and privacy are perceived as primary obstacles to its wide adoption in modern technological information.

[5], examined the challenges of providing intrusion detection in wireless ad-hoc networks, they reviewed current efforts to detect attacks against the ad-hoc routing infrastructure, as well as detecting attacks directed against the mobile nodes, they also examined the intrusion detection architectures that may be deployed for different wireless ad-hoc network infrastructures, as well as proposed methods of intrusion response.

Using wireless mesh networks (WMNs) to offer Internet connectivity had become a popular choice for wireless Internet service providers as it allows fast, easy, and inexpensive network deployment, but [6, 7], found that, security in WMNs was still in its infancy as very little attention has been devoted thus far to this topic by the research community.

[8], came out with the applicability and limitations of existing Internet protocols and security architectures in the context of the Internet of Things by giving an overview of the deployment model and general security needed and then challenges and requirements for IP-based security solutions and highlighted specific technical limitations of standard IP security protocols.

In their paper titled '*A Secure and Lightweight Approach for Routing Optimization in Mobile IPv6, [9]*, found out security weakness in mobility support that has a direct consequence on the security of users because it obscures the distinction between devices and users and they went further by finding that, a malicious and unauthenticated message in mobility support may open a security hole for intruders by supplying an easy mean to launch an attack that hijacks an ongoing session to a location chosen by the intruder, so

they come up with the solution on how to thwart such a session hijacking attack by authenticating a suspicious message.

In a paper '*Analysis of Security Threats in Wireless Sensor Network' by [10],* investigated the security related issues in wireless sensor networks because wireless communication technology incurs various types of security threats due to unattended installation of sensor nodes as sensor networks may interact with sensitive data and /or operate in hostile unattended environments.

[11], explained Internet of Things (IoT) as a three layer perspective: perception layer, transportation layer and application layer, they analyzed the security problems of each layer separately and tried to find new problems and solutions, they also analyzed the cross-layer heterogeneous integration issues and security issues in detail and discussed the security issues of IoT as a whole and tried to find solutions to them.

As discussed by [12], some current solutions data security and privacy protection issues associated with cloud computing across all stages of data life cycle.

Even though security issues have received great considerations in cloud computing and vehicular networks, [13] identified security challenges that are specific to vehicular clouds (VCs), e.g., challenges of authentication of high-mobility vehicles, scalability and single interface, tangled identities and locations, and the complexity of establishing trust relationships among multiple players caused by intermittent short-range communications and finally they provided a security scheme that addresses several of the challenges discussed.

The paper titled '*Survey on VANET security challenges and possible cryptographic solutions*' by [14], presented the communication architecture of VANETs and outlined the privacy and security challenges that needed to be overcame to make such networks safety usable in practice they then identified all existing security problems in VANETs and classified them from a cryptographic point of view [15].

In their research paper, [16], improved the security of the 3G protocols in a network access by providing strong periodically mutual authentication, strong key agreement, and non-repudiation service in a simple and elegant way.

[17], found out the security challenges such as identity theft, international credit card fraud, communications fraud and corporate fraud are some of the main barriers preventing wireless technologies from growing and over taking the wired technology position, so they explored the security vulnerabilities of the 802.11b wireless LAN and presented solutions for some of its major vulnerabilities.

As per [18], the wormhole attack forms a stern threat in wireless networks, specifically against many ad hoc network routing protocols and location-based wireless security systems taking an example on present ad hoc network routing protocols, in which without some ways to defend against the wormhole attack, they will be unable to find routes longer than one or two hops, and thus severely disrupting communication.

According to [19] ,the loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications as unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

As per [20], they researchers focused on routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication. On the basis of the nature of attack interaction, the attacks against MANET were classified into active and passive attacks. Attackers against a network can be classified into two groups: insider and outsider. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs.

[21], presented the *rushing attack*, a new attack that results in denial-of-service when used against *all* previous on-demand ad-hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack, the attack is also damaging because it can be performed by a relatively weak attacker. They analyzed why previous protocols failed under this attack and then developed *Rushing Attack Prevention (RAP),* a generic defense against the rushing attack for on-demand protocols. RAP incurs *no cost* unless the underlying protocol fails to find a working route, and it provides provable security properties even against the strongest rushing attackers.

According to [22], current wireless technologies in use allow hackers to monitor and even change the integrity of transmitted data so the lack of rigid security standards has caused companies to invest millions on securing their wireless networks which is very expensive.

b) OSI MODEL IN NETWORK SECURITY

To adequately secure the integrity of a network, administrators require standards of the framework to implement various protocols. In order to replace TCP/IP and satisfy this prerequisite, the Open System Interconnection (OSI) model was introduced as network reference model for analyzing data communication between hardware and software in a seven layer system.

While carrying out very unique tasks, each layer is also assigned to support the layer above and offer service to the one below it respectively.

According to [23], OSI layers are categorized into two group layers depending on the functionalities, and those layers are layers 1-4 which are assigned the lower layers of the

protocol stacks and media layers responsible for transferring and moving data and layers 5-7 which are considered to be the upper host layers of the system and are associated with application level data.

Table 1: Seven layers Architecture and their functionalities [24].

	OSI Model : 7 Layers & Architecture			
	Assigned Layer Number	*Data units type*	*OSI model layer*	*Layer function*
Host Layers	7	Data	Application	• Applications interface • Interpreting program requests & info requirements.
	6	Data	Presentation	• Data compression • Data representation • Encryption.
	5	Data	Session	• Communications of interhost
Media Layers	4	Segments	Transport	• End-to-end connections • Properly sequence of packets
	3	Packets / datagram	Network	• Establish network connection • Translate network addresses • Transmitting individual packets across a network • Logical addressing: IP.
	2	Bit / frames	Data link	• Physical addressing
	1	Bits	Physical	• Physical network connection signal management • Binary bit transmission • Media

In the OSI model each layer is susceptible to numerous attacks, which standstills the performance of a network.
[25], defined vulnerability as a weakness in security system and a certain system may be susceptible to unlawful data operation because the system does not authenticate a user's distinctiveness before permitting data access thus MANET is more vulnerable than wired network.
The following is the description of the attacks, threats and vulnerabilities of various OSI layers [26]

***Physical Layer Vulnerabilities includes*:** Loss of Power, Loss of Environmental Control, Physical Theft of Data and Hardware, Physical Damage or Destruction of Data and Hardware, Unauthorized changes to the functional environment (data connections, removable media, adding/removing resources), Disconnection of Physical Data Links, Undetectable Interception of Data and Keystroke & Other Input Logging.
Link Layer Vulnerability includes: MAC Address Spoofing (station claims the identity of another), VLAN circumvention (station may force direct communication with other stations, bypassing logical controls such as subnets and firewalls.), Spanning Tree errors may be accidentally or purposefully introduced, causing the layer two environment to transmit packets in infinite loops, In wireless media situations, layer two protocols may allow free connection to the network by unauthorized entities, or weak authentication and encryption may allow a false sense of security, Switches may be forced to flood traffic to all VLAN ports rather than selectively forwarding to the appropriate ports, allowing interception of data by any device connected to a VLAN.
Network Layer Vulnerabilities includes: Route spoofing - propagation of false network topology, IP Address Spoofing-false source addressing on malicious packets, Identity & Resource ID Vulnerability - Reliance on addressing to identify resources and peers can be brittle and vulnerable.

Transport Layer Vulnerabilities includes: Mishandling of undefined, poorly defined, or "illegal" conditions, Differences in transport protocol implementation allow "fingerprinting' and other enumeration of host information, Overloading of transport-layer mechanisms such as port numbers limit the ability to effectively filter and qualify traffic, Transmission mechanisms can be subject to spoofing and attack based on crafted packets and the educated guessing of flow and transmission values, allowing the disruption or seizure of control of communications.
Session Layer Vulnerabilities includes: Weak or non-existent authentication mechanisms, Passing of session credentials such as user ID and password in the clear, allowing intercept and unauthorized use, Session identification may be subject to spoofing and hijack, Leakage of information based on failed authentication attempts, Unlimited failed sessions allow brute-force attacks on access credentials.
Presentation Layer Vulnerabilities includes: Poor handling of unexpected input can lead to application crashes or surrender of control to execute arbitrary instructions, Unintentional or ill-advised use of externally supplied input in control contexts may allow remote manipulation or information leakage, Cryptographic flaws may be exploited to circumvent privacy protections.
Application Layer Vulnerabilities includes: Open design issues allow free use of application resources by unintended parties, Backdoors and application design flaws bypass standard security controls, Inadequate security controls force "all-or-nothing" approach, resulting in either excessive or insufficient access, Overly complex application security controls tend to be bypassed or poorly understood and implemented, Program logic flaws may be accidentally or purposely used to crash programs or cause undesired behavior.
The following figure shows the exact classification of security attacks for MANETS for different layers of the OSI model

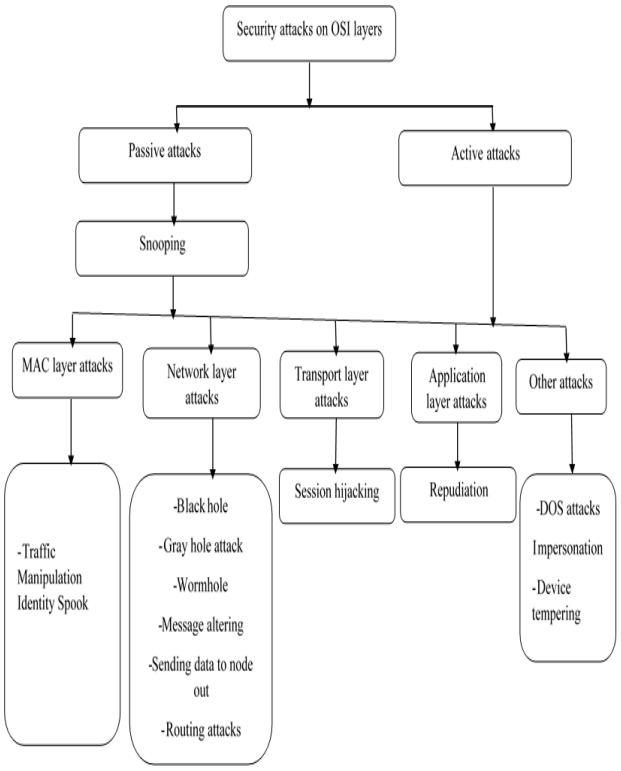

Figure 1: Classification of Security Attacks for different layers in MANETS [27].

Some attacks are non-cryptography related, and others are cryptographic primitive attacks. Table 2 below shows cryptographic primitive attacks and the examples[28].

Table 2. Cryptographic Primitive Attacks

Cryptographic Primitive Attacks	**Examples**
Pseudorandom number attack	Nonce, timestamp, initialization vector (IV)
Digital signature attack	RSA signature, ElGamal signature, digital signature standard (DSS)
Hash collision attack	SHA-0, MD4, MD5, HAVAL-128, RIPEMD

c) SOME NETWORK SECURITY SOLUTIONS

[29], suggested a new routing technique called Security-Aware ad hoc Routing (SAR) that includes security attributes as parameters into ad hoc route discovery thus SAR allows the use of security as a negotiable metric to improve the significance of the routes exposed by ad hoc routing protocols, they then developed a two-tier classification of routing protocol security metrics, and proposed a framework to measure and enforce security attributes on ad hoc routing paths.

According to [30], suggested to defend routing against denial-of-service attacks by taking advantages of the inherent redundancy in ad-hoc networks multiple routes between nodes, they also used replication and fresh cryptographic schemes, such as threshold cryptography, to build a highly secure and highly accessible key management service.

[18], presented a general mechanism, called packet leashes, for spotting and, thus protecting against wormhole attacks, and then presented a specific protocol, called TIK, that implements leashes.

A modest solution to protect VANETs as suggested by [31], is the use of cryptographic algorithms and approaches that are already widely deployed to protect against traditional threats in computer networks.

[28], suggested cryptography as an imperative and dominant security tool that offers security services, such as authentication, confidentiality, integrity, and non-repudiation but In all possibility, there exist attacks on many cryptographic primitives that have not yet been revealed even though Cryptographic primitives are considered to be secure, however, lately some problems which were discovered, such as collision attacks on hash function, e.g. SHA-1, Pseudorandom number attacks, digital signature attacks, and hash collision attacks which are very difficult to be secured.

In their paper titled '*Secure aggregation for wireless networks'* [32], presented a protocol that provided a secure aggregation mechanism for wireless networks that is strong to both intruder devices and single device key concessions, their protocol was envisioned to work within the computation, memory and power consumption limits of low-cost sensor devices, but takes benefit of the properties of wireless networking, as well as the power irregularity between the devices and the base station.

According to [33] a new and efficient wireless authentication protocol providing user secrecy was presented and was based on the hash function and smart cards, and mobile users only do symmetric encryption and decryption, in their protocol, it takes only one round of message exchange between the mobile user and the visited network, and one round of message exchange between the visited network and the corresponding home network.

[34], came up with the description that when either firewalls or VPN gateways are used in security of wireless local area networks, centralized server based solutions can be used for authentication, as in Remote Authentication Dial-In User Service RADIUS server (RADIUS), their architecture (as in figure 2 below) differ from others because they use location information together with user privileges in access control and they have chosen to determine location of the client from IP subnet information, which is considerably simpler compared to other studies which utilized GPS technology for a similar purpose.

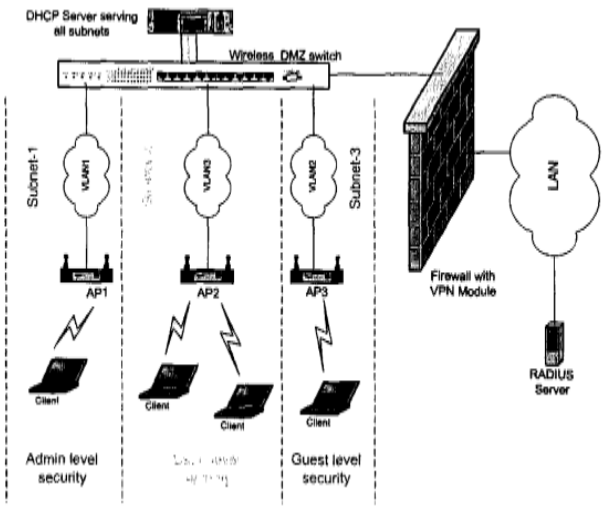

Figure 2: Proposed security architecture using RADIUS [34].

[35], concluded that Wi-Fi Protected Access repairs all known susceptibilities in Wi-Fi network security and greatly improves data security and access control on current and future Wi-Fi wireless LANs and it also delivers an instant, strong, standards-based, interoperable security solution that addresses all known errors in the original WEP-based security.

Ping Guo *et* al [36], proposed a novel design prototype in the direction of lightweight and tolerant authentication for service-oriented WMNs, named Variable Threshold-value Authentication (VTA) architecture in which VTA's intrusion-tolerant ability was guaranteed to design a series of node stimulated mechanisms to remain threshold values t and n of system private key unchanged the analysis and simulation results show that VTA can not only overcome the disadvantage of those static threshold value schemes, but also mostly increase system cost relating to the schemes not equipped with threshold mechanism for WMNs.

d) WPA AND WPA2 TECHNOLOGIES

The acronyms WEP, WPA, and WPA2 refer to different wireless encryption protocols that are anticipated to protect the information you send and receive over a wireless network and the first protocol the Wi-Fi Alliance created was WEP (Wired Equivalent Privacy), introduced in the late 1990s. WEP, however, had serious security weaknesses and has been superseded by WPA (Wi-Fi Protected Access). [37].

Table 3: Showing comparison between WEP and WAP [35].

	WEP	**WPA**
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1X and EAP

Just as WPA substituted WEP, WPA2 (second version of Wireless Protected Access (WPA) has substituted WPA as the most current security protocol because WPA2 implements the latest security standards, including "government-grade" data encryption and since 2006, all Wi-Fi certified products started to use WPA2 security and was an optional feature on some products before that so it was designed to improve the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires [38].

According to [39], WEP and WPA use RC4 (RC4 [40], is a stream cipher algorithm, which "takes one character and replaces it with another character, the output of which is known as a key stream), a software stream cipher algorithm that is susceptible to attack,

WPA is still vulnerable to attacks because it is grounded on the RC4 stream cipher.

The main difference between WEP and WPA is that WPA adds an extra security protocol to the RC4 cipher known as TKIP (Temporal Key Integrity Protocol) but WPA2 makes use of Advanced

Encryption Standard (AES and it is so secure that it could potentially take millions of years for a supercomputers' brute-force attack to crack its encryption even though, there is speculation, partially based on Edward Snowden's leaked National Security Agency (NSA) documents, that AES does have at least one weakness which is a backdoor that might

have been purposely built into its design.) and CCMP, a TKIP replacement.

The following table gives brief comparisons between WAP and WAP2.

Table4: Comparison between WAP and WAP2 [39].

	WPA	**WPA2**
Abbreviation stands for	Wi-Fi Protected Access	Wi-Fi Protected Access 2
Definition	A security protocol developed by the Wi-Fi Alliance in 2003 for use in securing wireless networks; designed to replace the WEP protocol	A security protocol developed by the Wi-Fi Alliance in 2004 for use in securing wireless networks; designed to replace the WEP and WPA protocols.
Methodology	As a temporary solution to WEP's problems, WPA still uses WEP's insecure RC4 stream cipher but provides extra security through TKIP.	Unlike WEP and WPA, WPA2 uses the AES standard instead of the RC4 stream cipher. CCMP substituted WPA's TKIP.
Security and Recommendations	Somewhat. Superior to WEP, inferior to WPA2.	Yes, though more secure when Wi-Fi Protected Setup (WPS) is disabled.

One firewall may be the solution to some extent but the problem appears to the costs to be incurred as each wireless access point must be secured with firewall in order to make stubbornness for attackers to attack the whole system. So computers connected to one access point may be attacked but not all access points or even the server can be attacked by the same attacker using the gateway of access point 1because all other access points are secured separately from access point 1 that's why it brings stubborn to attacker as the attacker is required to visit each access point which is time consuming and it may be easy to detect him/it.

To be able to attack say computers (C) protected by firewall 1 which protects computers connected to access point (1) one, so the computers in that access points may be vulnerable to attacks but all other computers connected to other access points can be attacked as the firewall 1 cannot allow access to wireless switch which links to other access points.

The following figure explains very well the scenario described above in which the attacker may

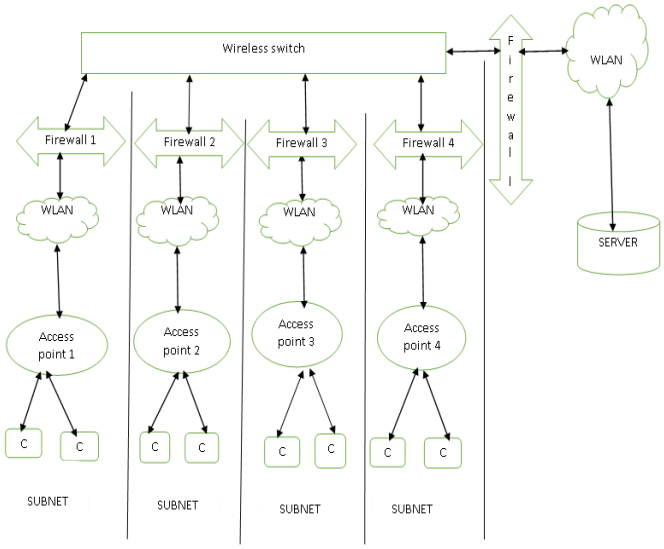

Figure 3: Suggested solution for small organization wireless network

In figure 3, firewall 1 deals with protecting computers in access point 1 against attacks from computers from other access points, the same applies for firewalls 2, 3 and 4.

3. CONCLUSION

According to visited literature reviews which bring about the secondary data sources and some few primary data sources, it seems that there are still difficulties in totally securing the wireless network against attacks, threats and vulnerabilities. The purpose of this study was to visit different literature in wireless network security and propose some network security solutions which will be more capable of securing wireless network compared to the existing solutions. .Most of the literatures indicated that securing totally wireless network is not an easy job but some parts of that network can be secured but not the whole network. So figure 3 is suggested in this study even though it is expensive but it may secure some network portion as it brings challenge for the attacker to visit every node in order to access the whole network which may lead for an attacker to be detected.

4. RECOMMENDATION AND FUTURE WORK

In the future, strong network security using firewall must be designed in order to avoid expenses of installing firewall in each WLAN as suggested in this study.
The authors recommends the protection of data to be done in the media gateway even though it will be very difficult to monitor the whole network but some security mechanisms in the gateway may somehow reduce the expenses which many organizations are incurring now days.

References

[1] W. A. Arbaugh, *Real 802.11 security: Wi-Fi protected access and 802.11 i*: Addison-Wesley Longman Publishing Co., Inc., 2003.

[2] M. Bishop, "What is computer security?," *IEEE Security & Privacy*, vol. 99, pp. 67-69, 2003.

[3] S. Khan, K.-K. Loo, T. Naeem, and M. A. Khan, "Denial of service attacks and challenges in broadband wireless networks," *8; 7*, 2008.

[4] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, pp. 69-73, 2012.

[5] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," in *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, 2003, pp. 368-373.

[6] N. B. Salem and J.-P. Hubaux, "Securing wireless mesh networks," *IEEE Wireless Communications*, vol. 13, pp. 50-55, 2006.

[7] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications magazine*, vol. 43, pp. S23-S30, 2005.

[8] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security Challenges in the IP-based Internet of Things," *Wireless Personal Communications*, vol. 61, pp. 527-542, 2011.

[9] S. Song, H.-K. Choi, and J.-Y. Kim, "A secure and lightweight approach for routing optimization in mobile IPv6," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 957690, 2009.

[10] S. Alam and D. De, "Analysis of security threats in wireless sensor network," *arXiv preprint arXiv:1406.0298*, 2014.

[11] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," *Wireless Networks*, vol. 20, pp. 2481-2501, 2014.

[12] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 2012, pp. 647-651.

[13] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, pp. 284-294, 2013.

[14] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, pp. 53-66, 2014.

[15] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *International Journal of Network Security & Its Applications*, vol. 5, p. 95, 2013.

[16] L. Harn and W.-J. Hsin, "On the security of wireless network access with enhancements," in *Proceedings of the 2nd ACM workshop on Wireless security*, 2003, pp. 88-95.

[17] H. Boland and H. Mousavi, "Security issues of the IEEE 802.11 b wireless LAN," in *Electrical and Computer Engineering, 2004. Canadian Conference on*, 2004, pp. 333-336.

[18] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE journal on selected areas in communications*, vol. 24, pp. 370-380, 2006.

[19] T. Karygiannis and L. Owens, "Wireless Network Security 802.11 Bluetooth and Handheld Devices. National Institute of Standards and Technology Special Publication, 800-48," ed, 2002.

[20] P. Kumar, "Analysis of different security attacks in MANETs on protocol stack A-review," in *In International Journal of Engineering and Technology (IJEAT), ISSN: 2249-8958, Volume-1, Issue-5, 2012*, 2012.

[21] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the 2nd ACM workshop on Wireless security*, 2003, pp. 30-40.

[22] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i)," in *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, 2009, pp. 48-52.

[23] V. Beal, "The 7 layers of the osi model," ed: Webopedia, 2015.

[24] A. Kavianpour and M. C. Anderson, "An Overview of Wireless Network Security," in *Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on*, 2017, pp. 306-309.

[25] P. Goyal, V. Parmar, and R. Rishi, "Manet: vulnerabilities, challenges, attacks, application," *IJCEM International Journal of Computational Engineering & Management*, vol. 11, pp. 32-37, 2011.

[26] D. Reed, "Applying the OSI seven layer network model to information security," *SANS GIAC GSEC Practical Assignment Version 1.4 b Option One*, p. 8, 2003.

[27] G. Mamatha and D. S. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS-A Survey," *International Journal of Computer Applications*, vol. 9, 2010.

[28] X. S. Yang Xiao and D.-Z. Du, "Wireless network security," ed, 2013.

[29] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, 2001, pp. 299-302.

[30] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE network*, vol. 13, pp. 24-30, 1999.

[31] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET communications*, vol. 4, pp. 894-903, 2010.

[32] L. Hu and D. Evans, "Secure aggregation for wireless networks," in *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, 2003, pp. 384-391.

[33] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, pp. 231-235, 2004.

[34] Y. M. Erten and E. Tomur, "A layered security architecture for corporate 802.11 wireless networks," in *Wireless Telecommunications Symposium, 2004*, 2004, pp. 123-128.

[35] W.-F. Alliance, "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks," *White paper, University of Cape Town*, pp. 492-495, 2003.

[36] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," *網際網路技術學刊*, vol. 15, pp. 929-935, 2014.

[37] Lifewire. (2017). *What Are WEP, WPA, and WPA2? Which Is Best?* Available: https://www.lifewire.com/what-are-wep-wpa-and-wpa2-which-is-best-2377353

[38] Lifewire. (2017). *WPA2 vs. WPA for Wireless Security*. Available: https://www.lifewire.com/wpa2-vs-wpa-for-wireless-security-3971350

[39] Diffen. (2017). *WPA vs WPA2*. Available: http://www.diffen.com/difference/WPA_vs_WPA2

[40] M. Ciampa, *CWSP Guide to Wireless Security*: Nelson Education, 2006.