Internet of Things Security Using Proactive WPA/WPA2

Mustafa Kamoona and Mohamed El-Sharkawy
Purdue School of Engineering and Technology, IUPUI

***Abstract*—**The Internet of Things (IoT) is a natural evolution of the Internet and is becoming more ubiquitous in our everyday home, business, health, education, and many other aspects. The data gathered and processed by IoT networks might be sensitive whichcallsforfeasibleandadequatesecuritymeasures.This paper describes the use of the Wi-Fi technology in the IoT connectivity, then proposes a new approach, the Proactive Wire- less Protected Access (PWPA), to protect the access networks. Then a new end to end (e2e) IoT security model is suggested to include the PWPA scheme. To evaluate the solution's security and performance, firstly, the cybersecurity triad: confidentiality, integrity, and availability aspects were discussed, secondly, the solution's performance was compared to a counterpart e2e security solution, the Secure Socket Layer security. A small IoT network was set up to simulate a real environment that uses HTTP protocol. Packets were then collected and analyzed. Data analysis showed a bandwidth efficiency increase by 2% (Internet links) and 12% (access network), and by 344% (Internet links) and 373% (access network) when using persistent and non- persistent HTTP respectively. On the other hand, the analysis showed a reduction in the average request-response delay of 25% and 53% when using persistent and non-persistent HTTP respectively. This scheme is possibly a simple and feasible solution that improves the IoT network security performance by reducing the redundancy in the TCP/IP layers security implementation.

Index Terms*—IoT, security, cyber security, Wi-Fi, Internet of Things, performance.*

*****

I. INTRODUCTION

Although the IoT networks are now ubiquitous in networking environments, in literature, the term Internet of Things or Internet of Everything (IoE) is still ambiguous. There isno unified definition of what IoT really is, however, we can define the IoT by stating what it can provide. The IoT is the next evolution of the Internet [1] as it provides a networking infrastructure allowing trillions of devices to collect data and communicate with each other to make processed smart decisions. In other words, IoT will be a network of the currently existing powerful Internet devices like smart phones, personal computers, and servers with addition of new less complex devices like heart or brain activity monitoring sensors, auto- mobile motion or brake sensors, or any environmentalsensors. A typical IoT home environment is shown in Fig.1

The before mentioned examples show that an IoT device does not have to be as complex as the current Internet devices. Thus there is a wider range of devices that can be connected to the IoT networks than that of the Internet. Whether it is home, business, health, or educational IoT environment, the IoT might be thought of as the point in time where more things or object are connected to Internet than people.

Fig. 1. Typical IoT Enabled Home [2].

An explosive growth of tablets and smart devices happened to increase the number of connected devices from around 500 million connected devices in 2003 while the humanpopulation was around 6.3 Billion to 25 Billion connected devices when the population was 7.2 in 2015. According to [1], the point in time when the number of connected devices surpassed the human population was in 2010.

Although the IoT roots can be tracked back to Massachusetts Institute of Technology (MIT) laboratories back in 1999 [1], the idea of low power communication sensor networks goes back way further in time. The emergence of the distributed low power sensor networks goes back to as early as the year 1967 [4]. Then a series of intermittent events led to the idea of wireless sensor networks (WSN) which in turn led to the concept of smart dust networks. Standards started to emerge for such

networks in 2003/2004, whenfirstly the 802.15.4 standard and secondly the ZigBee standard were released. The emergence of those standards facilitated the development of the idea of the IoT.

From those events, one can see that there are three basic requirements for IoT Networks:

- Low energy communication. As their battery life will have to be long for the IoT applications to be practical, as charging or changing the batteries for a huge number of devices would not be a simple process[4].
- Reliable Internetworking enabled communication stack. The IoT devices should beagle to communicate with each other and with other devices on other Internet devices[4].
- Light Secure End to End environment. Those networks might communicate sensitive information, so a light secure end to end communication is a necessity.

Fig. 2. Different Wireless Area Networks [5].

The IoT connectivity solutions range from the IPv6 Low Power Wireless Personal Area Networks (6LoWPAN) to the Bluetooth Low Energy (BLE) to the ZigBee then to the dominant Wi-Fi technology and more. The dominance of the Wi-Fidue to the fact that Wi-Fi networks are already deployed as part of the buildings infrastructures. A natural evolution of the Wi-Fi is to be an integral part of the IoT connectivity. Each of the above solutions has its own advantages and disadvantages depending on the range required, circumstances, and environment conditions. Fig. 2 shows multiple wireless area networks and their scopes [5].

Naturally, the TCP/IP implementation of theWi-Fisoftwareis complicated and large for the simple design of the IoT and requires much memory and processing. But Latest silicon advancements made embedded Wi-Fi modules solutions possible by reducing the large amount of the overhead from the micro processing units to allow the smallest micro controlling units to deploy the Wi-Fi connectivity, and in most cases the IoT devices will use only a fraction of the Wi-Fi bandwidth and draw intermittent small currents. Some currently available products claim to maintain operation using two AA batteries for more than twelve months. All that makes the Wi-Fi technology a very promising connectivity solution that helps the advancement of the IoT rapid development [5].

The flow of this paper is as follows: Section I is an introduction to the IoT. Section II is an introduction to IoT security. Section III states the problem and the aim of the work of this paper. Section IV illustrates the proposed scheme architecture.SectionVdetailstheworkresults.Finally,section VII states the conclusion.

II. INTRODUCTION TO THE IOT SECURITY

Secure network communication is defined as the secure exchange of messages between two entities over an insecure medium [7]. Regular networks have many security requirements, yet, IoT networks and because of their intrinsic critical nature mandate even higher security measures. The IoT is an immense network of interconnected networks and includes devices that are resource constrained thus entails low power computations. Such networks face numerousattacksrangingfrom physical attacks to sophisticated cryptanalysis attacks.

Cybersecurity has three services that the network administrator should keep in mind to protect the network from exploited vulnerabilities. Sensitive IoT networks should provide the below security pillar services.

Confidentiality: The contents of the messages between the two host devices (client and server) should only be read by the authenticated devices and no other intermediate adversary should be able to sniff and then read those sensitive contents. This is done by devices authentication and messages encryption.

Integrity: The exchanged messages should not be tampered by intermediate entities with or without purpose. Integrity helps in preventing the man-in-the-middle attacks where a middle device would inject packets into the network masquerading a legit host. An example is a replay attacks where the attacker records a transaction and then replays it at a later time.

Availability: The data that is supposed to be available to authenticated devices should be available to those devices at all times. This prevents denial of service attacks (DoS) where the attacker targets the availability of the provided services to the authentic users.

Those services are provided by different devices and layers in the network with the aid of symmetric key cryptography, public key cryptography, and hash functions [7].

A. *Transport LayerSecurity*

Transport layer security (TLS) and its predecessor secure socket layer (SSL) are enhancements to the transmission control protocol (TCP) implemented in the application layer. From development point of view, the TLS/SSL resides in the transport layer. SSL enhances the TCP by providing the security services confidentiality, integrity, and client and server authentication. It is usually used for HTTP application layer messages which made it a good candidate TCP/IP IoT networks. SSL starts with a simple TCP 3-way handshake and then proceeds to the SSL handshake where the two entities exchange their supported lists of cryptographic algorithms and hash functions and agree upon which ones to be used for the session, then they proceed to deriving the session master key from the server public key.

The actual data stream that is passed from the application layer to the SSL socket is divided into chunks called records. A message authentication code (MAC) is then added to each record for message integrity check. This MAC is generated by a hash function that takes the data record and a key as its input. The sender then encrypts the data plus the MAC using an encryption key and an additional header at the beginning of the encrypted part to form the whole record format.

B. *Network Layer Security(IPsec)*

Internet Protocol security (IPsec), on the other hand, targets the network layer security. The IPsec does that by providing network layer confidentiality, that is encrypting the payload of the network layer packets and that leads to building a virtual private network (VPN) on top of a public network.

Fig. 3. R1 to R2 SA (unidirectional) [7].

There are basically two IPsec protocols. The Authentication Header (AH) and the Encapsulation Security Protocol (ESP). The ESP is more widely used since it provides both the authentication and integrity services that AH provides plus data payload encryption (confidentiality) [7].

The IPsec uses virtual connections between two entities. The virtual connections are called security associations (SA) and the entities can be any network layer device or router. A security association is a unidirectional connection, so 2 SAs are required for a bi-directional IPsec communication.

When a packet is sent from a host in one side of the VPN to a host in the other side of the VPN, the ESP protocol performs multiple steps to convert the traditional IPv4 packet to an IPsec packet. First an ESP trailer is appended at the end of the IPv4 packet and then the whole combination is encrypted, an ESP header is then appended at the beginning of the outcome and an overall MAC is added to the end for message integrity, the result is the payload of the new IPsec datagram. At last, a new normal IPv4 header is added to the beginning with the new IP source and destination addresses. The source and destination IP addresses are the IP addresses of R1 and R2 interfaces that are connected to the public networks respectively.

III. PROBLEMSTATEMENT

IoT networks are currently being implemented in many enterprise and home environments. The opinions about its burst are vacillating and there is still no confidence in the available security solutions (see [14]). Some surveys like [15] show multiple security flaws that are deleterious to the development of the IoT. There are currently numerous implemented and proposed solutions to secure the IoT networks. Manyof them are rather complicated or do not provide a robust solution for low power devices that use Wi-Fi connectivity. This IoT revolution will be hindered without finding an easy, simple, and feasible solution that facilitates the ubiquity ofsuch networks in every environment with minimum efforts.

A. *Aim ofPaper*

The aim of this paper is to propose a new feasible easy-to- implement solution that uses the current infrastructure of the Wi-Fi networks to form a paradigm that proves secure, and saves bandwidth, delay, and energy consumption which are the main pillars for IoT applications.

B. *Methodology*

The proposed solution uses a DD-WRT router to manage the PWPA and IPsec security, a Linux server machine as a cloud application, and multiple embedded systems to simulate a typical IoT scenario. The three security services: confidentiality, integrity, and availability are analyzed. The data is collected and statistically studied and compared with an end- to-end security solution, Secure Socket Layer, for bandwidth, delay, and energy consumption improvements. It is important to note that it is assumed in this work that the adversary does not have physical access to the routers in which they can login to the router or simply disconnect the connectivity or unplug it to remove the service as such actions will easily be noticed by the administrator.

IV. PROPOSED SCHEMEARCHITECTURE

A. Introduction to Wi-Fi Wireless Networks

Local Area Network (LAN) is a group of computingdevices communicating with each other through a communicationlink. This LAN's shared communication channel can be anything from a simple coaxial cable to a wireless channel that devices can connect to through a wireless access point. While a wireless communication link offers easier installation and more flexibility, but without proper considerations it can be much more susceptible to attacks and security breaches.

The Wi-Fi is one of the many wireless LAN (WLAN) products and it follows the Institute of Electrical and Electronics (IEEE) standards to allow computing devices to communicate. It utilizes the 2.4 GHz and 5 GHz frequency bands.

These devices can get access to the WLAN by connectingto a wireless access point and upon authenticating, they can get access to the network resources whether it is a simple device in the network as a printer or a scanner or this resource can be any host that is connected to the Internet if this access point routes the traffic to the Internet. Usually wireless access points have an indoor range of about twenty five meters and a much larger range in the outdoors where there are less obstacles to attenuate the signal. The access point can cover a limited area of a single room, floor, or a building depending on the strength of signal and how much blocking the walls impose, whereas if multiple access points with overlapping coverage are used, a range of many miles could be achieved. Since the wired LANs require their signals to be transmitted via wires between the network elements, then they provide more security than the wireless networks where the signal is transmitted as radio waves in the shared medium (air) and any adversary with a network interface card (NIC) can receive the wireless signal. So within this network, and hence the wireless access points usually operate up to the network layer only, unless the communicating devices are using some kind of transport layer encryption like secure socket layer (SSL) for instance then the data is as secured as the network layer security used.

Since the 802.11 standard emerged, it used many security schemes. Starting with the Wired Equivalent Privacy (WEP) that uses an RC4 algorithm to encrypt the messages exchanged. The size of the seed plus the incorrect implementation of the cipher were the security weak link which made the WEP unreliable to secure the wireless traffic. Later, the 802.11i standard brought into light the Wi-Fi Protected Access (WPA) and then the second version (WPA2). Those schemes basically have two modes of operation. First, the Enterprise model which demands a data base and an authentication server (AS) that usually uses 802.1x RADIUS or DIEMETERprotocolstobe setup and maintain which is a task that is usually costly and requires some expertise. The AS does the authentication with the wireless devices by sharing a Master Key (MK) and then independently they derive a Pair wise Temporal Key(PTK)that both the access point (AP) and the wireless device will use for further messages encryption and authentication (integrity).The second model is the WPA Personal model that uses a Pre-Shared Key (PSK) for authentication. This key uses an8-63 character phrase to crate the symmetric keys that are going to be used for further encryption. Depending on the strength of the password, it is possible that the key can be broken in a matter of hours by the use of offline brute force dictionary attacks after sniffing the messages exchanged betweentheAPand the client when the client gets de-authenticated and then tries to get re-authenticated. Several software utilities such as Aircracking and CainandAbel, AirSnort, and Wifite can be used for such purpose. The efficiency of such utilities are bounded to the strength of the passcode used by theWPA personal model as the stronger the passcode the more time it takes to hack the net work. Now, one issue with the WPA personal model is that the symmetric key administration and its generation, renewal, and distribution in case ofanetworksecurity breach cumbersome and is not easy to performed specially if the setup is of more than a couple of devices connected to the network. So a new improvement needs to be implemented to solve this problem.

This work proposes and implements a new algorithm that solves, in a seamless way, the problem of WLAN WPA/WPA2 pre-shared key generation, distribution, and administration by changing the passkey proactively and automatically with the trusted clients without any required intervention fromtheusersusing only the same DD-WRT access point that is used to provide the connectivity in the first place.

B. Key Administration and Management Problem

Since the security of the Wi-Fi WPA personal security model is as powerful as the strength of the symmetric pre-shared key used, hence, there are some scenarios where an adversary with modest resources can use offline dictionary attacks to recover the key and attack the wireless network.One possible solution is for the administrator to manually log in to the router when a suspicious activity occurs in the networkand changes the password to a relatively long and hard password, then manually distributes the new pre-shared key with all the trusteddevices.

This manual hideous process takes a lot of time and needs to be done again whenever another suspicious activity

ISSN: 2321-8169
23 – 32

occurs. This solution is obviously time and resources consuming and leaves the wireless network open for attackers.

Even if a new password is generated, during the process of distributing the new key to all the trusted users and with the current implementations like QR codes, a mouthword, or paper-printed passwords can easily be misused and hence defeats the whole goal of changing the passkey in the first place as the network supervisor will have to re-do the process all over and that can be frustrating.

C. Related ProjectWork

Many of the current works target the alleviation of the wireless Wi-Fi network management and key administration problembutlesssuccesshasbeenachievedtodate.Maybeone of the best work is the WPS (Wi-Fi Protected Setup) which was introduced in 2006 as a simple Wi-Fi configuration setup. This scheme allows key distribution to simple users who do not know much about security approaches and get annoyed by entering long strong passkeys by using a pin, push button, near field communication (NFC), or the USB methods. This implementation is vulnerable to multiple offline and online brute force attacks where the PIN and hence the encryption key can be cracked. While the WPS helps a little with the key distribution, it does not by any means solve the trigger for key generation and change in which the case all the users will have to go physically to the AP to get the new code.

There are other recent solutions that try to assist with the network security management like the KissWiFi that manages the connected users by using MAC (Medium Access Control) access list and binds them to NFC tags and choosing the first user as an administrator. Such mechanism can lead to many flaws including the simple traffic dump then MAC address spoofing by the adversary to masquerade as a legitimate user and sometimes as an administrator.

Another recent work is the Flexi WiFi security manager[16] which uses an Android application, an Infrared (IR) transceiver, Bluetooth (BT) transceiver, and an embedded system to control a DD-WRT router to generate a new key and then distribute it to legitimate users. While it is a viable proposal for the problem solution, it still requires some user intervention and extra hardware to be added to the system.

D. Proactive WPA/WPA2 for access network

The proposed scheme is to use a proactive WPA/WPA2 approach. The DD-WRT router generates a new fixed length random password every preset time interval (two hours by default) then uses this strong password as the new pre-shared key. Before the password change occurs, every connected user will automatically open a TCP connection over the same secured Wi-Fi link and fetch the new password and the time until the new password will be applied (current password timeout). In that case, when the timeout occurs, all thewireless devices in that network will seamlessly change the password and hence no need for any user intervention. For simplicity, the first time the users get connected to the router can use either [16] or a simple NFC then after that the proactive WPA scheme will take over to change the password in the router and all the trusted already connected devices. Fig. 4 and Fig. 5 show the flowchart of the router and a trusted connected client.

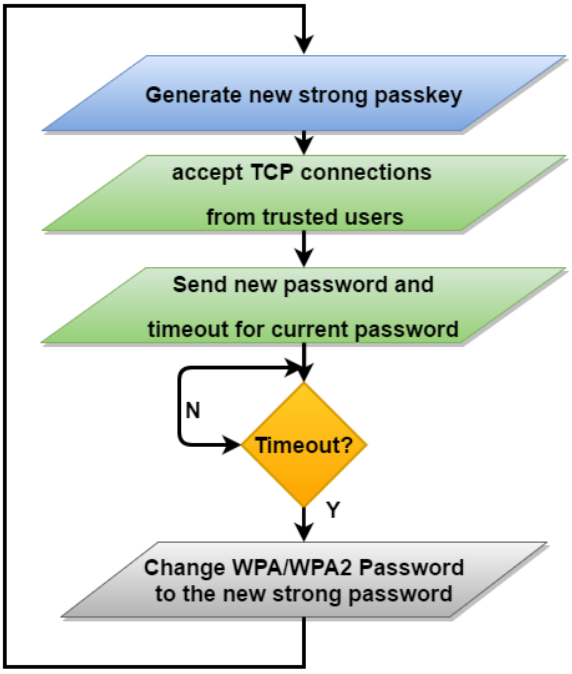

Fig. 4. DD-WRT Router Simplified Flowchart.

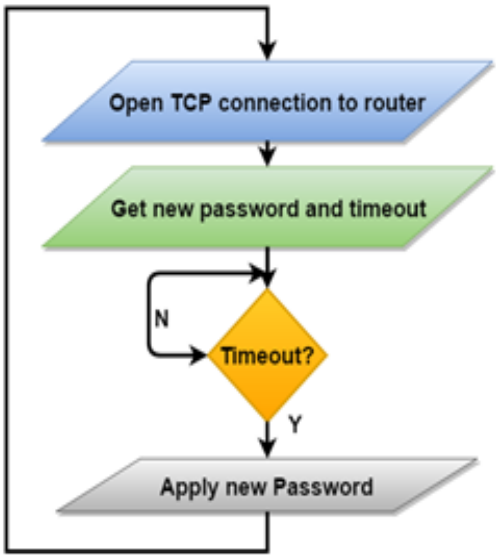

Fig. 5. Trusted Client Simplified Flowchart

E. Detailed SystemDesign

The hardware system design is very simple as no explicit extra hardware needs to be added. To get connected for the first time, users can simply enter the current password to get authenticated and connected. Then the router generates a predefined length (15 characters by default) strong random password that in corporates multiple techniques for strong pass- words generation like mandating the choice of some special characters and different upper and lower case letters. Each of the connected users then open a TCP connection to the listening server which provides the new password and a timeout for the current pass word expiration. The router can be set to accept connections to as many users in the network so that no TCP SYN connection initiation request will be rejected. The router and clients operate normally after that until the timeoutoccurs. When the timeout occurs, the DD-WRT router applies thenewdistributed password and all the clients reconnect using that password. The above explanation shows that except for the first time connection (Mandated by the WPA personal model) everything else is done automatically by the code on the DD- WRT router and the connected clients and no user intervention is required.

F. Schemes SecurityAnalysis

Since the proposed solution uses all the strength points of the WPA/WPA2 personal model and adds to that some enhancements to target its weaknesses. The proactive approach eliminates the possibility of an attacker capturing handshake messages exchange and trying to use offline dictionary attacks to get the password. Taking into account the considerable amount of resources (Including time) that requires an adversary to get the password, by then the system would have already generated and distributed a new strong passwordalong with a new timeout and thus it would be meaningless for an attacker to perform offline dictionary attacks.

Our scheme uses the already secured WPA/WPA2 connection to distribute the key and its timeout over the TCP connection. This approach eliminates the need for public key cryptography protocols like Diffie-Hellman for insecure channel secret key exchange and thus simplify the overall system design. Compared to the other related works, this approach can treat the weaknesses of the WPA/WPA2personal model instead of partially increasing the security level that is done by simpler defense techniques like MAC address filtering and hidden SSID. While this design is way simpler than the FlexiWiFi manager [16] in the sense that it does not require any extra hardware, the two systems can actually work together to form a whole administration system for the WPA/WPA2 WLANs by using the IR commands to trigger manual password changes while the automatic proactive approach continues in the background. Nevertheless, this scheme can be used as a standalone solution for secure Wi-Fi networks.

G. Proactive WPA/WPA2 Plus IPsec for the IoTSecurity

To provide an end to end IoT security, an additional component which is IPsec is added. The proactive Wi-Fi Protected Access (PWPA) was suggested as a counter measure to the weaknesses of the 802.11i standard to protect the wireless access network, which means that the data on the rest of the public Internet is still vulnerable. The Internet protocol security (IPsec) should be implemented between the two access routers (sensors' router and the cloud server router) toachieve end to end security. Depending on the application and the available bandwidth in the end to end network, either the encapsulation security protocol (ESP) transport or tunneling mode can beimplemented to provide end-routers datasecurity.

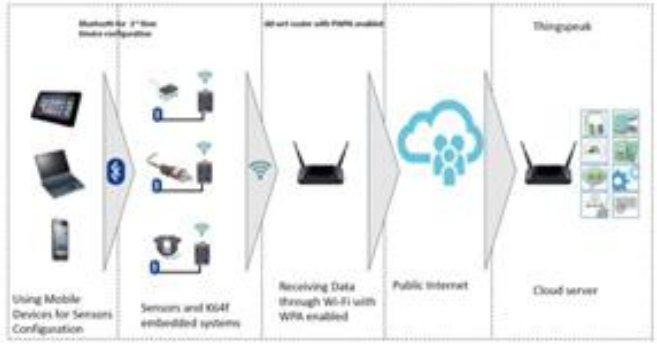

Fig. 6. PWPA Solution IoT Connectivity.

V. RESULTS ANDDISCUSSION

In order to demonstrate the efficiency of the solution, this section illustrates the solution connectivity, configuration, test parameters, and the process by which the data was collected and processed to show the results.

VI. PWPA CONNECTIVITY ANDCONFIGURATION

Fig. 6 shows the PWPA IoT solution connectivity and its components

To setup the IoT sensors and embedded systems for the first time, an Android application was developed and used to fetch the current WPA password and install it in the embedded system using the IR and BT interfaces (see [16]). The security control is passed to the PWPA solution where the password change will take place between the AP and the connected devices using the WPA2 security model. Table I shows the solution configuration and the test parameters used and Fig. 7 and Fig. 8 show the embedded system setup and the Android application interfaces, respectively.

 ISSN: 2321-8169
23 – 32

TABLE I SOLUTION TEST MATERIALS and PARAMETERS.

Item	Value
Router	BUFFALO AirStation AC 1750
Router	GL.iNET
Router	dd-wrt
IoT sensors	Temperature
IoT sensors	Pressure
IoT sensors	Current
IoT	Freescale K64f
Configurati	Bluetooth HC HC-05
Data Link	802.11
Transport	Transmission Control Protocol (TCP)
application	HTTP (Persistent and Non-persistent)
Access link	Proactive WPA2
Password	120 minutes
Internet	IPsec
Cloud	Thingspeak
Packet	Wireshark

To showcase the solution, the test was run in two scenarios. The first scenario used SSL end to end security where a separate SSL session is initiated between each device and the cloud application. The second scenario used PWPA and IPsec to provide end to end security.The two scenarios were tested with both persistent and non-persistent HTTP as some IoT servers do not support persistent HTTP protocol.

The test was run until the amount of about 5000 HTTP request/response pairs were collected and then processed and analyzed. For simplicity, the ddwrt router management was handled via a Telnet session by a separate entity (RaspberryPi) that is connected via an Ethernet cable, however, in practical situations, all the management can be done internally within the ddwrt router itself.

Fig. 7. Freescale K64f Embedded System with Portable Battery.

Fig. 8. Android Application Used for First Time Configuration.

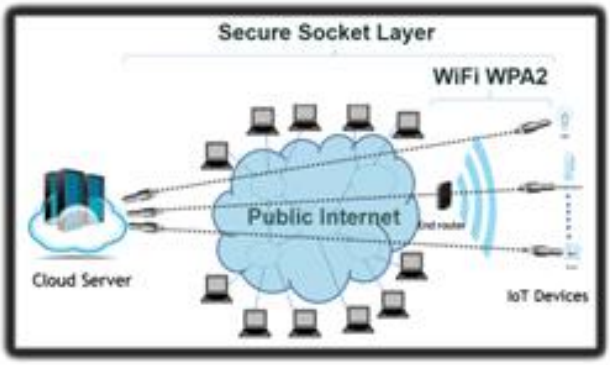

Fig. 9. Scenario One Using End to End SSL Security.

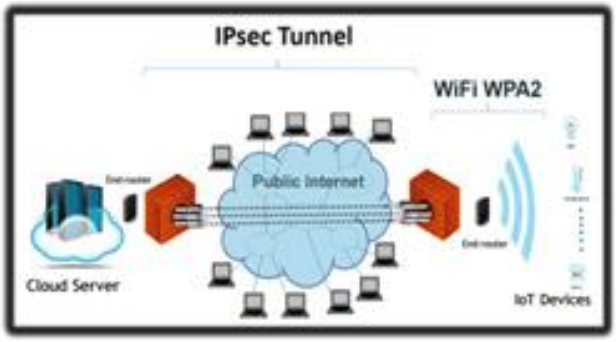

Fig. 10. Scenario 2 Uses PWPA and IPsec.

A. *Results and Discussion*

Solution Security: To prove the solution to be secure, a brief evaluation of the three cyber security pillars: confidentiality, integrity, and availability is discussed both on the PWPA side (access network) and the IPsec side (public Internet). On the PWPA side the confidentiality is achieved by either the TKIP (WPA) or AES (WPA2) encryption and pre-shared key authentication.

Integrity is achieved by using the message authentication codes to make sure that the data is not being tampered along the way. Although the availability has less consideration in WPA and WPA2 networks, some countermeasures can be taken as for WPA [12]. From the IPsec (end routers) side, the confidentiality is secured by first by mutual authentication and then messages encryption depending on the initial cipher suites negotiation. Integrity is achieved by using the ESPMAC as well. And since IPsec depends on the Internet for message transfer, an attack on availability (DoS) should be done by attacking the routers

themselves, a scenario that will not be covered in this work as mentioned in section III-B.

Network Performance Improvement - Delay: Depending on the processing power of the device, the processing time and power consumption will vary from a device to another, a multi-core processing unit will perform a function faster but will consume more energy but a device with little processing power will consume less battery life. IoT devices should have a balance between the two to perform efficiently. Accordingto the test parameters mentioned in section VI, the IoT devices used are sensors with FRDM k64f embedded systems which have moderate processing capability, the amount ofprocessing reduction when the PWPA solution is implemented will be loosely measured by the amount of delay difference the HTTP requests encounter when compared to the end to end SSL solution (instead of calculating the number of machine language instructions and multiply that number by the bus cycle duration). Although the data was gathered by initiating subsequent HTTP requests and recording their responses, Fig. 13 and Fig. 11 illustrate the average delay for both scenarios. To make the graph easier to read, each x-axis values represent a collection of 100 HTTP requests, while the corresponding y-axis values represent the average delay experienced by that request bundle. Fig. 14 and Fig. 12 illustrate the overall average delay experienced by both SSL and PWPA/IPsec scenarios.

When persistent HTTP is used, Fig.13 and Fig.14, a considerable reduction delay (including processing delay) is noticed, as an average of 23.76 milliseconds delay is experienced for each request. While in the case of non-persistent HTTP, Fig. 11 and Fig. 12, the overall average delay is decreased by 191.3 milliseconds, which is a substantial delay when sensitive IoT applications are implemented.

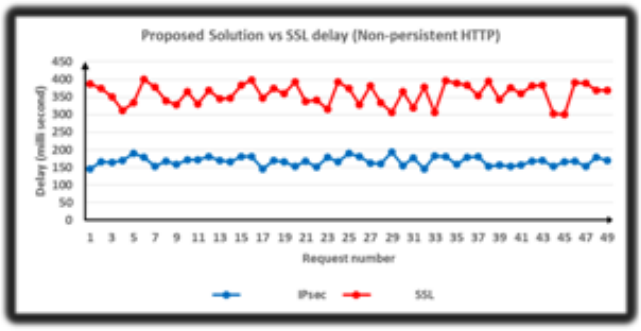

Fig. 11. SSL vs Proposed Solution (non-persistentHTTP)

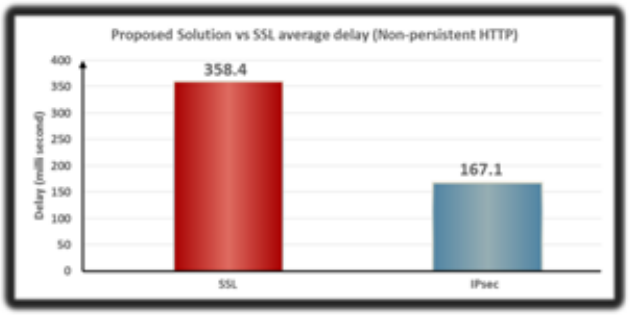

Fig. 12. SSL vs Proposed Solution Average Delay (non-persistent HTTP).

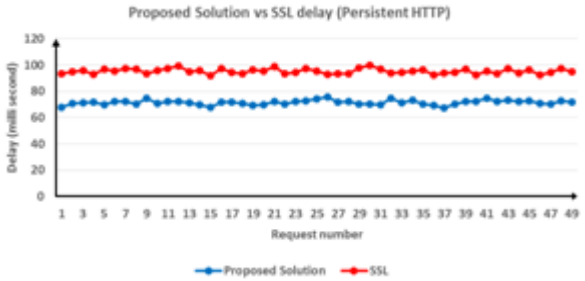

Fig. 13. SSL vs Proposed Solution Delay (persistent HTTP).

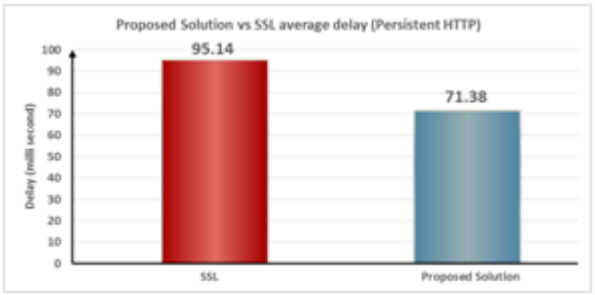

Fig. 14. SSL vs Proposed Solution Average Delay (persistent HTTP)

Network Performance Improvement - Bandwidth Efficiency: Since the end to end SSL scenario uses separate connections between each device and the cloud serve r(Things- peak),then there is a separate SSL header for each connection, and that affects the bandwidth utilization in both the access network and the Internet, while in the second scenario (proposed solution see Fig. 10), IPsec overhead only affects the Internet side and there is no extra headers in the access link side. Fig. 15 and Fig. 17, illustrate the average bandwidth efficiency for each 100 HTTP requests by calculating the actual throughput and dividing it by the bandwidth for the persistent and non-persistent HTTP respectively.

It can also be noted from Fig. 16 case, there is a 2% improvement in the Internet and an even bigger improvement, 12%, in the access link side bandwidth efficiency.

On the other hand, Fig. 18 shows that when non persistent HTTP is used, bigger enhancements are achieved when it comes to band width efficiency. This is due to the

messages exchanges that take place for each SSL connection initiation. Even though the IPsec contains a handshake and connection initiation as well, but it is only a single end router to end router connection instead of separate device to server SSL connection, the messages exchanged when an IPsec security association is initiated are shown. Fig. 18.shows that the improvement between the two scenarios, a 344% increase in the internet links bandwidth efficiency and 373% increase in the access link efficiency.

In the case of secure socket layer (SSL), the encryption occurs on top of the transport layer, so an adversary on the internet can see what is inside the transport layer and network layer headers since they are sent in the plaintext. While in the case of IPsec, the original packet is encrypted and then encapsulated in a new packet, which makes all the headers on top of the data link layer encrypted, and that is added security by the proposed solution.It is important to note here that changing the password on the device after the timeout might require a 1-5 seconds to occur, and although this situation happens once every multiple hours the data can be stored locally and then sent to the cloud after reconnecting, if the product requires real-time sensitive operation then consideration should be taken in regard of such events.

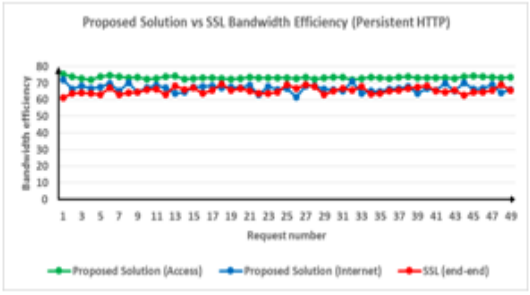

Fig. 15. SSL vs IPsec Bandwidth Efficiency (persistent HTTP).

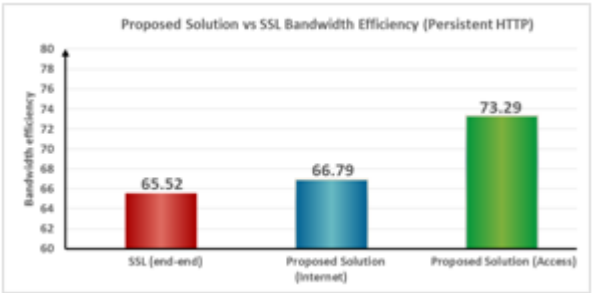

Fig. 16. Solution vs SSL Average Bandwidth Efficiency (persistent HTTP)

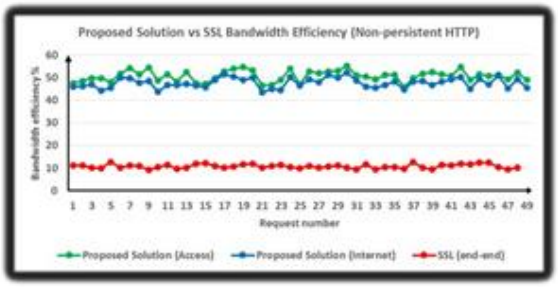

Fig. 17. Solution vs SSL Bandwidth Efficiency (non-persistent HTTP)

VII. CONCLUSION

The IoT is the natural evolution of the Internet. Its fast growing nature and being an integral part in daily sensitive services like industrial, enterprise, home networking, and education raises some security concerns. While the IoT connectivity can be any of the wired or unlicensed wireless technologies like Bluetooth, Bluetooth low energy (BLE), ZigBee, and Wi-Fi, the target of this thesis is to find a security solution for the pervasive wireless technology, theWi-Fi.

The proposed solution in this thesis is to use a proactive WPA/WPA2 approach in order to secure the access link side of the IoT. The proactiveapproach is controlled by a ddwrt router which changes the password proactively after a specific time interval after instructing the connected devices to do so as well. The solution uses an IPsec security on the end routers to ensure the data security on the public Internet side of the connection.

This simple solution allows to use a simple Wi-Fi setup or even better, to use the current Wi-Fi infrastructure which is available in almost every enterprise or home environment where the IoT is needed. A separate Wi-Fi network will be created for the IoT devices so that the current normal users experience will notchange.

The solution proved to be secure by evaluating the three security pillars: confidentiality, integrity, and availability. More even, the solution improved the overall network performance by reducing the amount of delay experienced, and increasing the bandwidth efficiency when compared to the end to end security solution usingSSL.

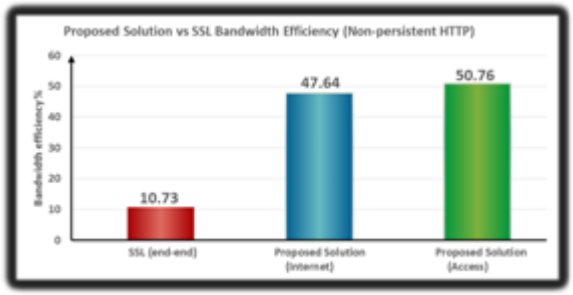

Fig. 18. Solution vs SSL Average Bandwidth Efficiency (non-persistent HTTP)

By shifting most of the encryption processing from the low power IoT devices to the router which is connected to the mains, the solution reduced the amount of processing doneby those devices and thus greatly increases their battery lifewhich is a major concern in the IoT industry.

REFERENCES

[1] Evans, Dave," The internet of things: How the next evolution of the internet is changing everything," CISCO white paper 1 (2011): 1-11.

[2] Chase, Jim," The evolution of the internet of things," Texas Instruments (2013).

[3] National Intelligence Council (US), Global trends 2025: a transformed world. National Intelligence Council, 2008.

[4] Palattella, Maria Rita, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, and Mischa Dohler," Standardized protocol stack for the internet of (important) things," Communications Surveys & Tutorials, IEEE 15, no. 3 (2013):1389-1406.

[5] Reiter, Gil,"Wireless connectivity for theInternet of Things," Europe 433(2014).

[6] Clarke, Ruthbea Yesner,"Smart cities and the internet of everything: The foundation for delivering next-generation citizen services," Alexandria, VA, Tech. Rep(2013).

[7] Kurose, James F., and Keith W. Ross, Computer networking: a top-down approach. Addison-Wesley,2007.

[8] Kahn, David. The codebreakers. Weidenfeld and Nicolson, 1974.

[9] Philip Levis," Secure internet of things project (SITP)," 2015. Online: http://iot.stanford.edu, accessed11-April-2016.

[10] Raza, Shahid. "Lightweight Security Solutions for the Internet of Things," PhD diss., Mlardalen University, Vsters, Sweden, 2013.

[11] Bontu, ChandraS., Shalini Periyalwar, and MarkPecen," Wirelesswide- area networks for internet of things: An air interface protocol for IoT and a simultaneous access channel for uplink IoT communication," Vehicular Technology Magazine, IEEE 9, no. 1 (2014): 54-63.

[12] Wikipedia, "Network performance," 2016.Online: https://en.wikipedia.org/w/index.php?title=Network performance & oldid=716348410, accessed11-April-2016.

[13] Boycottbenetton," 2016 Online: http://www.boycottbenetton.com/, accessed11-April-2016.

[14] Borgohain, Tuhin, Uday Kumar, and SugataSanyal, "Survey of Security and Privacy Issues of Internet of Things," arXivpreprint arXiv:1501.02211(2015).

[15] Kamoona, Mustafa, and Mohamed El-Sharkawy," FlexiWi-Fi Security Manager Using Freescale Embedded System," In Information Science and Security (ICISS), 2015 2nd International Conference on, pp. 1-4. IEEE, 2015.

[16] Cam-Winget, Nancy, Tim Moore, Dorothy Stanley, and Jesse Walker. "IEEE 802.11 i Overview," In NIST 802.11 Wireless LAN Security Workshop.2002.

[17] Jean Loup Gilis and MatthieuCaneill, Attacks against the Wi-Fi protocols wep and wpa," 2010. Online: https://matthieu.io/dl/wifi-attacks- wep-wpa.pdf, accessed11-April-2016.

[18] Liu, Caiming, Yan Zhang, and Huaqiang Zhang, "A novel approach to iot security based on immunology," In Computational Intelligence and Security (CIS), 2013 9th International Conference on, pp. 771-775. IEEE, 2013.

[19] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey," Computer networks 54, no. 15 (2010): 2787-2805.

[20] Li, Fagen, and Pan Xiong, Practical secure communication for integrating wireless sensor networks into the internet of things," Sensors Journal, IEEE 13, no. 10 (2013): 3677-3684.