UDC 004.056+681.518.5

AL-SUDANI MUSTAFA QAHTAN ABDULMUNEM,
V. S. KHARCHENKO, D. D. UZUN

National Aerospace University "KhAI" Kharkiv, Ukraine

VULNERABILITY ANALYSIS OF WIRELESS NETWORKS: CASE FOR SMART BUILDING AUTOMATION SYSTEM

Wireless communication has become very popular in industry, business, commerce, and in everyday life. Wireless technology spans from user applications, such as personal area networks, ambient intelligence, and wireless local area networks, to real-time application. The given paper shows the analysis of wireless network security and availability, and helps to develop safe and effective system usable for future design. Smart building automation system is one of work areas of embedded wireless network in system design. Technique of criticality matrix based security assessment is described and illustrated for smart BAS.

Keywords: *Wi-Fi, WLAN, Smart Building, Building Automation System, vulnerability, security, criticality matrix.*

1. Introduction

1.1. Motivation

Motivation to analyze wireless network vulnerabilities is to reduce risk of attacks and to provide a solution for solving security problems. Wireless network brings a new meaning to network security using different important sensitive high quality for reliability and availability of wireless network. Communication takes place "through the air" using radio frequencies that is why the risk of interception is greater than via wired networks. If the message is not encrypted or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality.

Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks:

- preserving confidentiality,
- ensuring integrity,
- maintaining availability of the information,
- encryption technology for system information.

The given paper analysis threats of WLAN security. This analysis gives imagination about attacks and weak points in system design; such details help to design a protected system.

1.2. Work Related Analysis

Wang, Srinivasan and Bhattacharjee [1] proposed a 3-way handshake model instead of the usual 4-way handshake method for the 802.11i protocol. It is shown how the alternative method can effectively prevent denial of service (DoS) attacks including deauthentication, disassociation and memory/CPU DoS attacks. Wireless security is analyzed in the same way like wired security in [2], the authors tried to explain important part of security and aimed to develop knowledge of administration for networking to avoid attack and have perfect system. In [3] current threats in wireless networks and some academia research reviews regarding the matters are discussed. Significant and persistent threats discussed are sniffing, Man in the Middle Attack (MITM), Rogue Access Points (RAP), Denial of Services (DoS) and social engineering attacks.

In [4] wireless local area network standards and characteristic analysis are explained. Analyzing vulnerability for each standard helps to list attacks and tries to make a solution for attacks. In [5] vulnerability of wireless network is shown from the view point of the vulnerability of wired and wireless network analysis. The known attacks and the way how they find a target are investigated.

In [6] a new idea for wireless network security is presented using firewall as a type of defense to minimize the risk of attack on wireless network by analyzing threats of different layers. Swatie and Shilpi [7], provide a comparative study between three major security protocols (WEP, WPA, WPA2), their work discusses encryption/decryption process, limitations and the vulnerability of each protocol to various attacks.

Using FMEA and Criticality matrix [12], a methodology to identify and analyze potential failure modes of the various parts of a system and the effects these failures may influence the system in general.

1.3. Goal

The given paper helps to understand threats and attacks on wireless network, and to manage network in different application fields that require high security. Building automation system (BAS) is one of the fields of wireless network application which requires high level of security. The paper analyzes communication system for BAS, and helps to understand the threats which can affect a system by describing and investigating vulnerability of two important components in BAS-communication system (Wi-Fi, ZigBee). The goal of this paper is to show vulnerability of wireless network and to apply this analysis in BAS.

2. Analysis of Wireless Network Security

Wireless networks consist of four basic components: transmission of data using radio frequencies; access points that provide connection to the organizational network, end devices and users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

Wireless local area network (WLAN), Wi-Fi 802.11 standard is declared through several specifications of wireless network, it defines an over-the-air interface between two points. WLAN topology is defined as three types: point–to-point, multipoint-to- point, multipoint-to-multipoint. Characteristics of WLAN [8] make it the most popular technology used in communication design of building automation system.

2.1. Vulnerability of Wireless Local Area Network

WLAN network uses radio as transmission medium and this displays all the information at risk from attacker. Another affection of wireless transmission can be Invasion & Resource Stealing, Denial of Service and Rogue Access Points. The list of WLAN intrusion methods:

- lack of Physical Security: a signal of wireless network is broadcasting among communication nodes, unlike in wired network hacker can interrupt a broadcasting signal path, it can be for the purpose of surveillance, stealing information, sabotage;

- invasion& Resource Stealing: an attacker can use for monitoring or for physical/logical attack in network any source of building automation system (servers, camera, and data store);

- traffic Redirection: an intruder can change the route of the traffic, and it can cause problems in communication between parts of the system and the delay in sending and receiving information.

2.2. Wireless Local Area Network Threats

A number of security threats in 802.11areexploited by malicious hacker. The threats to the WLAN include relatively harmless free Internet access as well as malicious intrusion, snooping, interference, destruction of data, and a virus attack. Attacks to which the WLAN can be subjected are divided into two large categories: passive and active [9]. (Fig.1) shows a general taxonomy of security attacks.

1. Passive Attack is an attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below:

- eavesdropping means that the attacker monitors transmissions of message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station;

- traffic analysis means that the attacker gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

2. Active Attack is an attack when an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below:

- masquerading means that the attacker impersonates an authorized user and thereby gains certain unauthorized privileges;

- replay is when the attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user;

- message modification means that the attacker alters a legitimate message by deleting, adding to, changing, or reordering it;

- denial-of- service is when the attacker prevents or prohibits the normal use or management of communications facilities.

2.3. Attacks on Wireless local area network

1. Denial-of-service attack (DoS) generally consists of temporarily or indefinitely interrupts or suspends services of a host connected to the Internet DoS is an attempt to make a network resource unavailable to its authorized users.

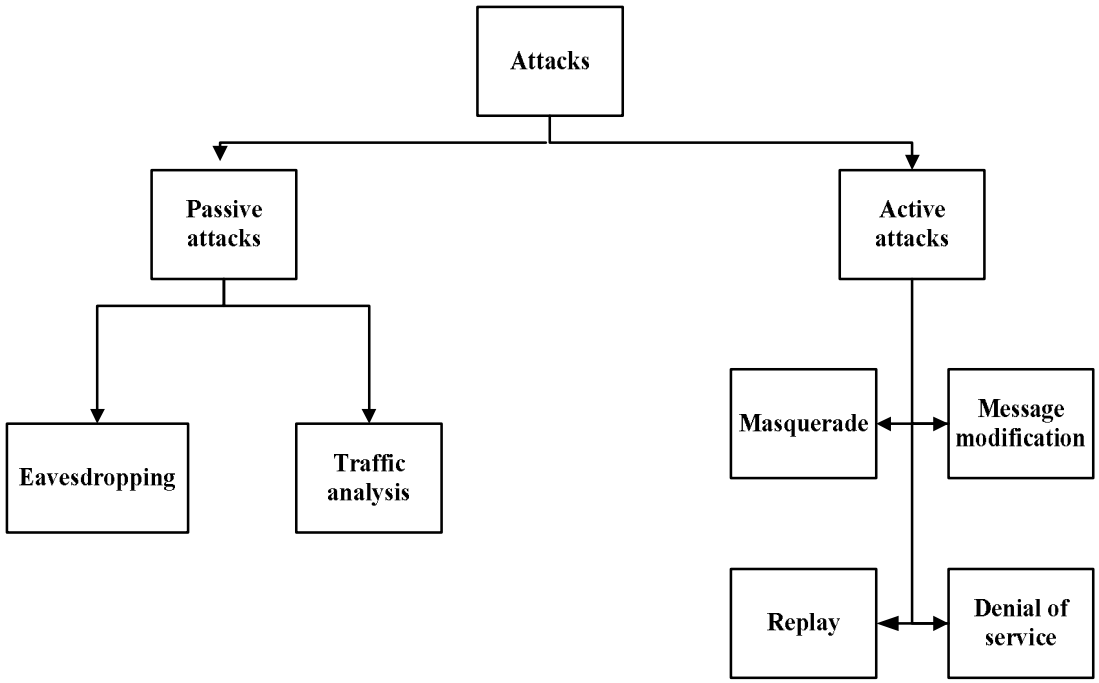

Fig. 1. Taxonomy of Security Attacks [9]

Attackers usually target sites or services hosted on high-profile web servers such as banks, credit card and payment gateways there is one common method of attack that involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. Such attacks lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately

2. Man-in-the-middle means that an attacker tempts computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. Often the real access point is jammed or blocked while the rogue, with the same SSID, is in the clear with a strong signal.

2.4. Simulated attacks on WLAN

In this section will show simulation attack on wireless local area network and show the way to access this network without Authorization. For this simulation we use Kali Linux [10], which analyzes the nearby wireless networks. We will list the step of attack simulations follows:

1. After running the program we can see all the nearby networks to find out the details about network, name of wireless network, security protocol, channel broadcasting and amount of data is used in this network

2. After choosing the target network, a hacker starts to access this network by sending different and long duration requests to join this network using dictionary. This Dictionary is used to generate different kinds of password to enter the network. Having different dictionaries help to have more chances to break the network.

3. To have a successful attack time and patience are needed to get the Result and invade the network.

In (fig.2) simulation windows of attacker containing all the necessary information are shown. They facilitate choosing a target network In (fig.2) network address are shown where it is possible to see a type of security protocol used in the network to secure information as well as bandwidth of channel and name of network, all this information and details is used by an attacker to carefully choose his target.

2.5. Wireless local area network security protocol

Security is the main weakness in WLAN, wireless medium shared among the user and open access for any malicious attacks.

That is why wireless security needs to use three different types of protocol help in network security in general and WLAN in particular.

- WEP protocol is the first security protocol for WLAN that was designed as a part of the original 802.11 standard. Its purpose was to provide security to

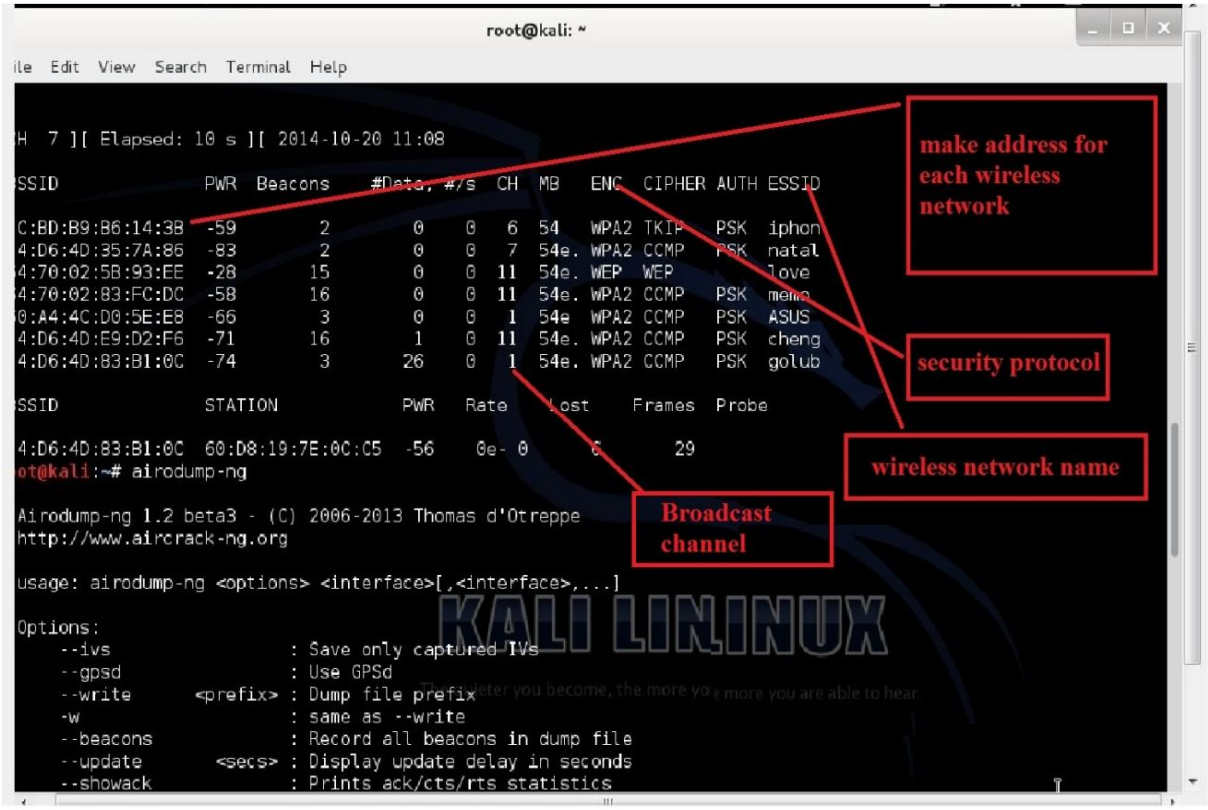

Fig. 2. Wireless monitoring using Kali Linux

WLAN equivalent to the security existing in the wired network. WEP uses RC4 stream cipher for confidentiality and CRC-32 for integrity. In this paper, we used 128-bit WEP protocol with 104-bit key and 24-bit initialization vector [11];

- WPA1 was designed to overcome the limitations and insecurity of WEP protocol. WPA1 implements most of the IEEE 802.11i standard;

- Key Integrity Protocol (TKIP)uses a per-packet key. Hence, unlike WEP, a new 128-bit key is dynamically generated for each packet. Consequently, this prevents most of the type of attacks that compromised WEP. WPA1 replaced the insecure CRC used in WEP with a stronger message integrity check. Despite the fact that WPA1 addressed most of the problems that exists in WEP, it continues to show some limitations such as relying on stream cipher and cryptographically weak integrity (Michael algorithm) [11];

- WPA2 also referred to as IEEE 802.11i replaces WPA1 and implements the mandatory elements of IEEE802.11i standard. It uses a new AES-based encryption mode CCMP that is highly secure. This resolved the security issue with TKIP in WPA [11].

2.6. ZigBee Analysis

ZigBee is expected to provide low cost and low power connectivity for equipment that needs battery life as long as several months to several years but does not require data transfer rates as high as those enabled by Bluetooth. ZigBee can be implemented in mesh networks larger than is possible with Bluetooth.

ZigBee compliant wireless devices are expected to transmit 10-75 meters, depending on the RF environment and the power output consumption required for a given application, and will operate in the unlicensed RF worldwide (2.4GHz global, 915MHz Americas or868 MHz Europe). The data rate is 250kbps at 2.4GHz, 40kbps at 915MHz and 20kbps at 868MHz. IEEE and ZigBee Alliance have been working closely to specify the entire protocol stack. IEEE 802.15.4 focuses on the specification of the lower two layers of the protocol (physical and data link layer) standard.

On the other hand, ZigBee Alliance aims to provide the upper layers of the protocol stack (from network to the application layer) for interoperable data networking, security services and a range of wireless home and building control solutions, provide interoperability compliance testing, marketing of the standard, advanced engineering for the evolution of the standard.

This will assure consumers to buy products from different manufacturers with confidence that the products will work together.

ZigBee is applied for the second part of the connection area in building automation system. Considering the Characteristics of ZigBee, small area needs high performance and low cost with long life of power.

Table 1

Comparison of Wireless LAN Security protocol: WEP, WPA AND WPA2

	WEP	WPA	WPA2
Purpose	Provide security comparable to wired networks	Overcome the flaws of WEP without requiring new hardware, Implements majority of IEEE 802.11i standard	Implements completely IEEE 802.11i standard and an enhancement over WPA
Data Privacy (Encryption)	RivestCipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) using block cipher Advanced Encryption Standard (AES)
Authentication	WEP-Openand WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Michael (generates Message Integrity Code (MIC))	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Lack of key management	Provides robust key management and	Provides robust key management and keys are

3. Vulnerability analysis of Wireless Network Based BAS

3.1. BAS architecture

Building automation system is represented by a programmed, computerized, intelligent network that units electronic devices for monitoring and controlling all building services systems in a facility. BAS is needed in order to create an intelligent, effective building as well as to reduce energy and maintenance costs. Usually building automation systems have a primary and secondary bus containing programmable logic controllers, input/outputs and an operator interface. A typical architecture of the system is shown in (Fig. 3).

Fig. 3 shows the divided BAS architecture as three main levels (management level, communication level, automation level). The analysis of these levels gives an image about system availability and security under threat and cyber attacks.

3.2. Criticality matrix based analysis

Vulnerability analysis is the process of estimating the vulnerability to potential disaster hazards of specified elements at risk. It is applied to analyze BAS and its components: ZigBee as hardware component embed in BAS design network, SCADA as management level for system design, and FPGA as control unite in system connected end device with control unite. The review of vulnerability of component and effected on system design is given below:

1. Previously it was considered that SCADA networks were isolated from all other networks, i.e. attackers could not access the system. However with industry growth more connectivity was demanded. SCADA systems are sometimes connected to other networks like the internet. The open standards also make it very easy for attackers to gain in-depth information of SCADA networks. The use of COTS hardware and software to develop devices for operating in the SCADA network also contribute to its lack of security. Devices that are designed to operate in safety-critical environments are usually designed to failsafe, but security vulnerabilities could be exploited by an attacker to disable the fail-safe mechanisms. That is why these devices must be designed for both safety but and security.

2. ZigBee networks are the new technology in WSN. However, they still have vulnerability in key management and information transmission. The main vulnerabilities of ZigBee network are given below:

a) key distribution. Key distribution of ZigBee network is a challenging issue because it is vulnerable in transferring Master Key, Link Key, and Network Key. It should be noted that Master Key is preinstalled in each node or transferring to each node in the unsecure way;

b) number of cryptography keys in large-scale network. ZigBee network with n nodes use the symmetric key cryptosystem and it must generate and store n keys for distributing in the large scale network. Here the problem is managing and maintaining the large number of symmetric keys by ZigBee network in large scale network.

3. Field Programmable Gate Array (FPGA) is applied for implementation of user defined function due to interconnected reprogrammable functional blocks (embedded processors, clock managers, digital signal processing blocks, Ethernet controller etc). The selection of the implementation platform for cryptographic applica-

tion depends on many critical factors such as complexity of algorithm, its application, power consumption, speed, cost and desired security aspects (physical security, side channel leakage etc.)

Black Box Attack means that an attacker inputs all possible combinations, while saving the corresponding outputs. The algorithm can be obtained after the log of different combinations. A lot of processor power is required for implementation of this attack. However, this attack will be less feasible as the number of logic elements and complexity of the FPGA increases.

Through the above-mentioned vulnerability analysis of system components, we can calculate criticality matrix to describe availability of the system and security with different fault in its internal component. As show in (Fig. 3) the system is divided into three levels:

1) management level (ML), which contains controlling unite, monitoring and information storage;

2) communication level (CL), which is responsible for the link between system components;

3) automation level (AL), which presents input/output, and another end devices that provide information for management level.

Degrees of fault effect on system availability and security for each level are as follows:

1. Management level: fault and error in controlling unit and data basic lead the system to a failure or even to shut down state because this level manages all operation on the system, rank of availability and security of system depends on management level.

2. Communication level: there are two main kinds of attacks able to affect on this level. The first is when an attacker has access to the communication area and his aim is monitoring information between levels, this type of attack effects security field in system because data will be shown to the attacker, and as for availability the system will work as required during the period of a mission. The second type is when the attacker's aim is to disconnect communication between levels.

In order to analyze these two attacks and to understand effects on communication level we used the critical matrix to show probability and security of communication level. The criticality matrix gives understanding of the importance of this system level, as it is shown in table 2. The representation of the first attack is the symbol = A, and of the second attack is the symbol = B.

3. Automation level: mostly faults at this level do not damage the system work lot, input/output device mostly have hardware fault and it can be fixed or re placed without interruption of the system work.

We can build a criticality matrix of these levels as shown in table 3. Management level has high effect for system failure and security as well and it can lead system to shut down. Communication level effects security of system rather greatly and it has medium effect on system failure. Automation level has low effect on security and failure.

Table 2

Criticality matrix of communication system

		Probability of failure		
Security information		Low	Mean	High
	High	A		
	Mean			
	Low			B

Table 3

Criticality matrix for system

Probability of failure					
Severity of consequences		Lowest	low	Mean	High
	Lowest	AL			
	Low				
	Mean				
	High		CL		ML

4. Conclusion

One who connected to the network he/she think to protect only their information from hacker but the thing to stop the hackers hacking the network. We have proposed a system to protect the infrastructure of the network and this paper mainly concentrate on issues to identify the footprints of the attackers.

The hacker will not leave any type of evidence to find him so there are the certain steps to identify those hackers, setting a wireless network is easier but to protect the infrastructure of the created one is find to be little difficult from vulnerabilities of outsiders. The attackers enter through the weak holes present in the wireless environment and make the disturbance to the environment and to the authorized users. We can prevent it the network from those attackers by applying few methodologies provide in this paper.

We also used some tools to hack the WLAN infrastructure so that we are able to find the hackers idea on attacking the network. This paper also provides the technique to restrict the hackers from future threatens.

Future work includes two steps:

1. Development of the algorithms for data encoding when it is sent through air.

2. Protection of transmission between sender and receiver. Increasing security takes into account cost, reliability and effectiveness while designing the system.

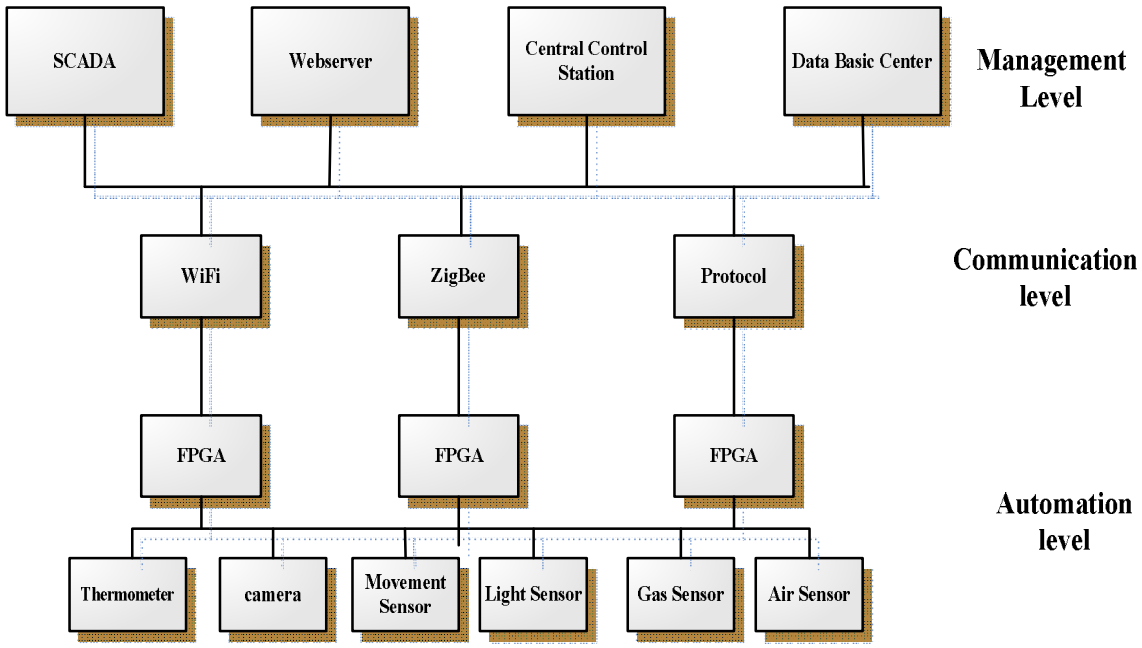

Fig. 3. Principal architecture of a building automation system

References

1. Wang, Li. Security Analysis and Improvements on WLANs [Electronic resource] / Li Wang, Bala Srinivasan,Nandita Bhattacharjee // Journal of Networks. – March 2011. – Vol. 6, NO. 3. – Melbourne, Australia. – P. 470-481. – Access mode: http://ojs.academypublisher.com/index.php/jnw/article/download/0603470481/2793. – 12.05.2015.

2. Kensby, J. Building Automation Systems Design: Guidelines for Systems with Complex Requirements [Electronic resource] / J. Kensby, R. Olsson // CHALMERS, Energy and Environment, D-2 Master's Thesis E2012:01. – Göteborg, Sweden. – 2012. – 62 p. Access mode: http://publications.lib.chalmers.se/records/fulltext/156136.pdf. – 12.05.2015.

3. Mohamad, M. Wireless Networks: Developments, Threats and Countermeasures [Electronic resource] / M. Mohamad, Wan Haslina Hassan // The Society of Digital Information and Wireless Communications (SDIWC). – 2013. – № 3(1). – P. 119-134. – Access mode: http://www.sdiwc.net/digital-library/web-admin/upload-pdf/00000595.pdf. – 12.05.2015.

4. Hatambeiki, A. Wireless Network Security (Thesis) [Electronic resource] / A. Hatambeiki. - San Francisco, California, May 2004. – 132 p. – Access mode: http://www.engpaper.net/Wireless-network-security.htm. – 12.05.2015.

*5. Dasgupta, P. Wireless Network Threats: Firewall Counter measures. Course: MSC. Computer Science (Software Engineering) [*Electronic resource*] / P. Dasgupta, E. E. Ndudi. – Faculty of Computer Science & IT, Universiti Selangor : 40000 Shah Alam, Malaysia, 2013. – 10 p.*

6. Vishali, R. Security in Wireless Local Area Networks. International Journal of Computer Science and Information Technology Research [Electronic resource] / R. Vishali. – April-June 2014. – Vol. 2, Issue 2. – P. 472-483. - Access mode: www.researchpublish.com. – 12.05.2015.

7. Granzer, W. Security in Building Automation Systems [Electronic resource] / W. Granzer, F. Praus, W. Kastner // IEEE Transactions on Industrial Electronics. – November 2010. – Vol. 57, No. 11. – P. 3622-3630. – Access mode: http://www.auto.tuwien.ac.at/~wgranzer/sebas_tie.pdf. – 12.05.2015.

8. Karygiannis, T. Network Security 802.11, Bluetooth and Handheld Devices:Recommendations of the National Institute of Standards and Technology [Electronic resource] / T. Karygiannis, Les Owens Wireless // Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. – November 2002. –Gaithersburg, MD 20899-8930. – 119 p. – Access mode: http://www.homolaicus.com/scienza/reti/wireless/nist.pdf. – 12.05.2015.

9. Mohsenian-Rad, H. Communications and Control in Smart Grid. Topic 3: Smart Grid Communications. Department of Electrical & Computer Engineering. [Electronic resource] / H. Mohsenian-Rad. – Spring 2012. – 25 p. – Access mode: http://www.ee.ucr.edu/~hamed/Smart_Grid_Overview.pdf. – 12.05.2015.

10. Jain, R. Wireless LAN Security II: WEPAttacks, WPA and WPA2 [Electronic resource] / R. Jain. – Washington University in Saint Louis. – 33 p. – Access mode: http://www.cse.wustl.edu/~jain/cse571-07/Washington University in St. Louis. – 12.05.2015.

11. Elyasi-Komari, Iraj. Analysis of Computer Network Reliability and Criticality: Technique and Features [Electronic resource] / Iraj Elyasi-Komari, A. Gorbenko, V. Kharchenko // Int. J. Communications,

Network and System Sciences. – 2011. – № 4. – P. 720-726. – DOI 10.4236/ijcns.2011.411088. – Access mode: http://www.scirp.org/journal/PaperInformation.aspx?PaperID=8252#.VXVSP1Iprgw. – 12.05.2015.

12. Mustafa Qahtan Abdulmunem Al-Sudani. Cybersecurity of FPGA-based System for Building Automation System: Problem and Solutions. [Текст] / Al-Sudani Mustafa Qahtan Abdulmunem, V. Kharchenko // Радіоелектронні і комп'ютерні системи. – 2015. – № 1 (71). – С. 39-46.

Поступила в редакцию 12.05.2015, рассмотрена на редколлегии 18.06.2015

АНАЛІЗ ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ МЕРЕЖ: ПРИКЛАД СИСТЕМИ АВТОМАТИЗАЦІЇ РОЗУМНИХ БУДИНКІВ

Аль-Судані Мустафа Кахтан Абдулмунем, В. С. Харченко, Д. Д. Узун

Бездротовий зв'язок став дуже популярним як у промисловості, бізнесі, торгівлі, так і в повсякденному житті. Бездротова технологія охоплює і користувальницькі додатки, такі як: персональні мережі, «штучний розум», бездротові локальні мережі і додатки реального часу. Дана стаття надає аналіз безпеки та доступності бездротової мережі, а також допомагає створити безпечну й ефективну систему, яку можна буде використовувати для майбутніх розробок. Система автоматизації розумних будинків є одним з напрямків застосування вбудованої бездротової мережі. Надано приклад оцінювання безпеки системи автоматизації розумного будинку з використанням матриць критичності.

Ключові слова: Wi-Fi, бездротова мережа, розумний будинок, система автоматизації будинку, вразливість, безпека, матриця критичності.

АНАЛИЗ УЯЗВИМОСТЕЙ БЕСПРОВОДНЫХ СЕТЕЙ: ПРИМЕР СИСТЕМЫ АВТОМАТИЗАЦИИ УМНОГО ДОМА

Аль-Судани Мустафа Кахтан Абдулмунем, В. С. Харченко, Д. Д. Узун

Беспроводная связь стала весьма популярной как в промышленности, бизнесе, торговле, так и в повседневной жизни. Беспроводная технология охватывает и пользовательские приложения, такие как: персональные сети, «искусственный интеллект», беспроводные локальные сети и приложения реального времени. Данная статья представляет анализ безопасности и доступности беспроводной сети, а также описывает создание безопасной и эффективной системы, которую можно будет использовать для будущих разработок. Система автоматизации умного дома является одним из направлений применения встроенной беспроводной сети. Приведен пример оценивания безопасности системы автоматизации умного дома с использованием матриц критичности.

Ключевые слова: Wi-Fi, беспроводная сеть, умный дом, система автоматизации дома, уязвимость, безопасность, матрица критичности.

Аль-Судани Мустафа Кахтан Абдулмунем – аспирант каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», г. Харьков, Украина.

Харченко Вячеслав Сергеевич – д-р техн. наук, профессор, зав. каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», г. Харьков, Украина, e-mail: v_s_kharchenko@ukr.net.

Узун Дмитрий Дмитриевич – канд. техн. наук, доцент, доцент каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», г. Харьков, Украина, e-mail: dmitriy.d.uzun@gmail.com.