The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 6, pp.33-41, Dec. 31, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.6.33
JIIBC 2018-6-4

캠퍼스 보안을위한 IoT 및 무선 센서 네트워크 모니터링

IoT and Wireless Sensor Network Monitoring for Campus Security

아흐메드 매틴*, 칭청주후*, 살만아프리카**, 무함마드 우스만**

Ahmed Mateen*, Qingsheng Zhu*, Salman Afsar and Muhammad Usman****

요 약 스마트 캠퍼스의 플랫폼으로 사물 인터넷에 대한 아이디어가 점점 대중화되고 있다. 인터넷에 연결하기 위해 통신 네트워크, 센서 노드 및 게이트웨이로 구성된 인프라가 필요하며 각 센서 노드는 환경에서 데이터를 수집할 수 있다. 본 논문은 스마트 캠퍼스 모니터링을 적용하기 위해 인터넷에 구성한 무선 센서 네트워크를 설명한다. 무선 센서 네트워크 모니터링은 저전력 구현 및 통합 시스템을 사용하는 완벽한 솔루션이다. 그러나 제한된 컴퓨팅 범위, 제한된 컴퓨팅 성능, 네트워크 프로토콜의 가용성 부족, 프로그래밍 보안 부족 및 기밀성, 무결성 및 가용성 분야의 보안 오류로 인해 수많은 제약이 있다. WSNM 노드를 위한 새로운 보안 기술과 기능이 개발되었다. 보안 네트워크 연구 개발 및 서비스 거부 (DOS) 및 복잡성 공격 방지를 위한 시스템을 제안하였다. 이러한 시스템이 제대로 구현되면 사전 할당을 통한 에너지 효율성 메커니즘과 안전한 루틴 알고리즘을 통해 핵심 관리 모델의 새로운 키를 제공 할 수 있다.

Abstract The idea of the Internet of Things as a platform on the Smart Campus has become increasingly popular. It requires an infrastructure consisting of communication networks, sensor nodes and gateways to connect to the Internet. Each sensor node is responsible for gathering data from the environment. This document outlines a network of wireless sensors on the Internet for the application of Smart Campus monitoring. Wireless sensor network Monitoring have become a complete solution to using a low power implementation and integrated systems. The numerous restrictions however result from the low communication range, the limited computing power, the lack of availability of the network protocol, the lack of programming security and the security failures in the areas of confidentiality, integrity and availability. A new security technique and its functionality for WSNM nodes developed. Development in the research of a secure network and suggestions for avoiding denial of service (DOS) and complexity attacks. These systems if properly implemented can provide an energy efficiency mechanism through pre-allocation and a new key from key management models with a secure routine algorithm.

Key Words : Smart Campus, Denial of Service(DOS), Internet of things(IoT), Wireless Sensors

I. Introduction

Internet of Things could be a network which implements totally inter-connection in issue to issue, human to issue, through info sensor devices and in agreement protocol. Its main options are getting all types of knowledge of the physical world through RFID and sensor devices, sending and exchange info combined with the net, communication network and alternative network, analysis and process info

*정회원, 중국 충칭대학교, 컴퓨터 과학과
**정회원, 파키스탄 농업대학교, 컴퓨터 과학과
접수일자: 2018년 11월 9일, 수정완료: 2018년 12월 1일
게재확정일자: 2018년 12월 7일

Received: 9 November, 2018 / Revised: 1 December, 2018 / Accepted: 7 December, 2018
*Corresponding Author: ahmedmateen@outlook.com
Computer Science Department, Chongqing University, China

exploitation intelligent computing technology [1].

Wireless Detective Network Monitoring (WSNM) of insecure organizations and buildings; It is flexible and difficult to replace the detector battery once it has to be drained. The answer is to use the power technology to turn energy from the environment to revive the batteries. However, due to temporary and spatial changes (for example, the release of zero energy at night in the case of star technology), the release of energy is almost timid. That is why the energy management systems are designed to ensure economical use of the energy gathered [2].

A framework is created for the dynamic energy management method within the author has planned an unintentional Dynamic Host Configuration Protocol (AH-DHCP), an Automatic Address Configuration Protocol to enable DHCP to collect completely different parameters in the mounted network, furthermore as an unconscious network [3].

The purpose of this work is to perform the detection of nodes in the non-involved network, even if the nodes change their positions in the constellation. DHCP tracks the nodes as soon as they are transferred from their position in the unintentional network. In addition, DHCP maintains the constellation using the applicable mechanism even during constant communication between different nodes. This provides DHCP to tolerate message loss and handle node quality quickly and efficiently.

The address assignment formula of an AN is intended to overcome the problem of address propagation for the new connected node to the constellation over the network [4].

Impact Security isn't a replacement idea plan. you need to correct from birth till death, affect multiple security machineries in relevance foodstuff, protection, children's, article, finance and lots of alternative a lot of aspects within which we tend to expertise fine before long. Also, if the billions of sensible device on the connected of net with the coverage of underneath the umbrella of the IoT to phenomena, it should have sturdy safeguards to the proper info to the proper things within the right/correct place at the proper/right time through the correct channel [5].

Implementation of the campus security system, here is the performance of the main subsystems of the campus security system. RFID access control system. In the campus protection system, RFID is mainly used for personnel ID cards RFID card issued to all campus teachers. You can also use a temporary card. Some of the main campus sites, such as campus doors, teaching buildings, laboratory, library, gym, RFID readers, and students need a map. Credit to access these premises. Information from the RFID card reader can record student pathways on campus. Especially when students come out of campus with RFID cards, the system sends a brief message to inform parents of the information provided by the reader so that they can be informed of their child's situation. The RFID access control system. RFID and the access control system, but also for the management of campus attendance, library teaching and laboratories, are mainly used for the identification of staff [6].

Radio frequency identification id application in military, library, airline, security, sports, library, healthcare, sports, aim figure show in 1.

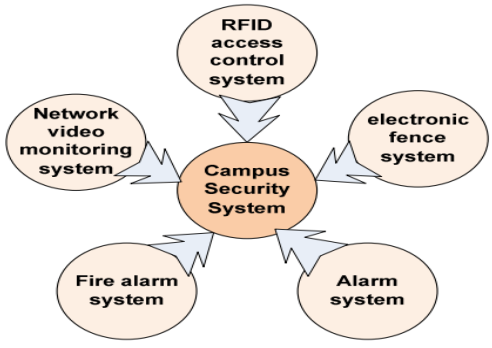

그림 1. 캠퍼스 보안 시스템 아키텍처
Fig. 1. Campus security system architecture

Frequency identification is that the wireless, contactless usage of high frequency fields of magnetism for the transmission of information for the

needs determine mechanically and track objects associated tags. While not adequate security, doubtless embarrassing info may expire tags embedded in shopper product. Even though the tag contents are secured, responses might be copied sure day, ready to violate privacy [7].

The WSNM video surveillance system (wireless sensor network monitoring). The video surveillance network includes the use of high-level networks to provide images, audio, and various methods for remote collection, export, storage, processing, broadcasting, and control. New video editing program. Major campus stations have been installed with network cameras and provide a video surveillance system on the campus network. Users can easily monitor monitoring conditions in real time and at any time. Shown in Figure .2 the CCTV network can also connect to the alarm devices. In the event of an anomaly, the system may operate with an alarm, a telephone, a mobile phone or other means that allows the user to send alarm messages and take extraordinary circumstances, but may warn the center of the alarm [8].

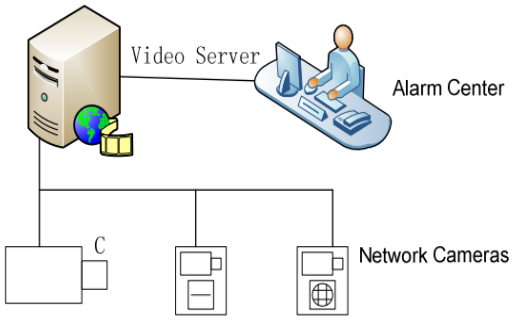

그림 2. 무선 센서 네트워크 모니터링 (WSNM)을 위한 비디오 모니터링 시스템" 와 같이 수정하기 바랍니다.
Fig. 2. Wireless sensor network Monitoring (WSNM) video monitoring system

II. Methodology

The use of the campus security system, here is the launch of the main services for the campus security system. In the campus security program, RFID is widely used for work ID cards. RFID card issued to all campus teachers. You can use a temporary-card. In few of the main campus area, such as campus museums, educational buildings, laboratory, library, gym, RFID students, and students need a map. Debt access to this site. Information from a RFID card reader can write student methods in the room. Especially when students come out of campus with RFID cards, the system sends a brief message to inform parents of the information provided by the reader so that they can be informed of their child's situation. RFID and the access control system but also for the management of campus attendance, library teaching and laboratories, are mainly used for the identification of staff [9].

Radio frequency identification id application in military, library, airline, security, sports, library, healthcare, sports, animal farms et al are below. Frequency identification is that the wireless, contactless usage of high frequency fields of magnetism for the transmission of information for the needs determine mechanically and track objects associated tags. While not adequate security, doubtless embarrassing info may expire tags embedded in shopper product. Even though the tag contents ar secured, responses might be copied sure day, ready to violate privacy [10].

Security was outlined because it somehow neutralized the ability to deal with a particular threat. A broader definition refers to many countries with threats and risks. This definition includes innate thoughts and inner aspects in a security system. Safety is an angle that depends on the perceived nature of the AN atmosphere [11].

The wireless detector network is massive and continues to expand dynamically, covering the atmosphere, the ecosystem, unstable and process monitoring, security and police management that are out of the speed of emergency response and eudemonism support. Network life can be increased by

providing security and privacy against attacks in the network layer, with nodes scattered in an impartial environment [12].

Wireless sensors are helpless for several varieties of attacks. Since WSNs support communication standards and information sent over a broadcast channel, it is possible to create passwords and information buzz. There have been several cryptography proposals in recent years to ensure secure communication. Cryptography-only descriptions are not enough for compromise node attacks and new behaviors in detector networks, but in future, computer security developers or programmers need to restrict 100% security mechanisms, while application writing codes [13].

The security of the Internet of Things raises the variety of open and moral issues that are currently being considered as beginners, scientific, corporative, governmental, and private. Several of these issues raised for several clear conflicts between global and national interests and the government against public interests. Wireless devices on personal or between organizations or between home network or international. The content of the various pieces of legislation must cover the right to information, provisions prohibiting or prohibiting the use of the network of facilities, and rules for such security legislation [14].

The such as Wi-Fi, Ethernet, or cellular networks. These technologies are all well established and fully functional for Internet communications and as such are Internet of Things can be deployed using any Internet capable technology, suitable to be a part of the backbone of the Internet of Things. However, the requirements of the Internet of Things the current use of PCs, laptops, smart phones and other peripherals that are connected to the Internet. Firstly, for general Internet use the increase of bandwidth has been a corner stone in development of the services associated with the web such as streaming media, cloud storage, and remote applications. For the Internet of Things however, the individual bandwidth requirement per device is low, as most devices will only collect and send sensory data, or receive actuating data [15].

IoT devices do not require a user interface as what is normally expected when working with connected devices. IoT devices are capable to function and make decisions without human intervention. Devices may collect data, the data might then be processed by some application and a suitable action could then be executed accordingly to algorithm or self-learned pattern recognition software. Wireless communication has the advantage of being easy to implement in already constructed buildings, as it requires no extra installation of wires [16].

The protocols in accordance to the general Internet Protocol layer categorization model. The IEEE 802.15.4 standard is a Physical and Data link layer correspondent for WSN, representative for Ethernet using twisted pair cable, or to that of 802.11 (Wi-Fi) for Wireless Local Area Network. The Network layer equivalent is the 6LoWPAN protocol, which is IPv6 over Low Power Wireless Area Networks, and to supply routing capabilities, the routing protocol RPL [17].

Sensor networks area unit extremely distributed networks of little, light-weight wireless sensing element nodes, deployed in massive numbers to observe the surroundings or system by the measuring of physical parameters like temperature, pressure, or ratio, sound, vibration, motion or pollutants, at totally different locations. Sink nodes act because the entry between WSNs and therefore the user [18].

A novel security technique and its practicality for WSN nodes are projected. A review of past and current analysis, the likelihood of getting a secured network and proposals meant to forestall denial of service (DOS) and quality attacks. These schemes if properly enforced will give associate energy-efficient mechanism victimization pre-allocation and a re-keying of key management models with a secured routine algorithmic program [19].

Access control campus security model working

using a card access system in campus increases security and provides a multitude of benefits for students and administrators. Access control offers stronger credential controls which can easily and quickly be issued and revoked within the campus's security system. This allows for rapid response in case of an emergency or lock down on campus, and increases feelings of safety for students. Access control model working in structure diagram show in Figure.3 Physical protection and information protection, access control (AC) is required to select access points or other sources. Accessibility control is a method or system aimed at obtaining by virtue of the right to death or understandable at the meeting. Network Access Control (NAC) is a campus protective way to try to integrate networking with maintaining network security and security. Campus security structure show in figure 3 using underground sensor all sensor connect internet thought traffic sent database server [20].

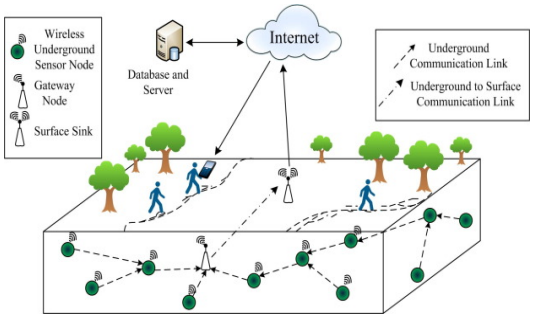

그림 3. 액세스 제어 캠퍼스 보안 모델
Fig. 3. Access control campus security model

Implementing a card system can also prove to be less costly than traditional lock and key security methods. Losing keys and replacing locks is costly and time consuming for staff members. With a card access security system, lost cards can be replaced more efficiently without compromising the safety of other students. Access Control eliminates the need for expensive hardware and, eases the role of facility mangers, and increases residence hall security.

These devices generate an excessive amount of knowledge per second, even in petabytes per second. The preparation of the IoT raises a number of security issues, ranging from the awful nature of sensitive objects, the introduction of low-weight cryptographic algorithms, process and memory needs, and the use of normal protocols to reduce the amount of knowledge that was changed between nodes. IoT service interaction. IoT service interaction. Security and privacy attempts of the Web of Things. In terms of explicit IoT security, there are many open unit issues, such as cryptographic algorithms, authentication protocols, access management, trust or privacy, and governance frameworks. Therefore, the analysis of the key technologies should be performed together with the coding mechanism, communication security, and protective detector information and crypt logical algorithms show in figure 4. However, it is the order of the day that we want to introduce additional security mechanisms in the coming years to ensure meaningful device communication under the umbrella of the Internet of Things.

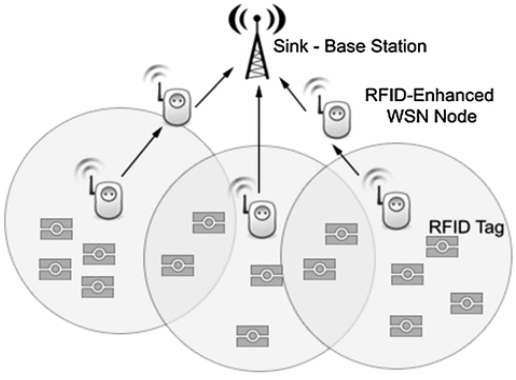

그림 4. 무선 센서 네트워크 및 RFID 작동
Fig. 4. Wireless Sensor Network and RFID Working

Ⅲ. RESULT

Performance Trends from the IEEE 802.15.4 Network Study. The aim is to provide information on the use and consumption of energy in a wireless observation system. IEEE 802.15.4 compliant effects at

two gig cycles per second, and thus the mathematical models of 802.15.4 unsupported and compatible networks. Figure 5 show experimental results. A point-to-point network, in which a node must be transferred to a destination node, presumably via a network of routers, is taken into account. As long as a router is received between availability and destination, between two-hop communication was performed; in the case of two routers, we have three jumps, and so on. The nodes add a beacon activated mode, so we tend to define = BO = zero for the case of a jump, then = zero and BO = 2 for the cases of multiple jumps. the amount of bits (the payload sealed) received the final destination due to the size of the payload. Although the bit rate of the channel is 250 kbps, the evasion performance is significantly lower than the protocol-overhead. Now we will see that the participation rate for point-to-point connections does not exceed 100 and 20 kbps. However, switching is reduced due to possible interferences between unofficial jumps.

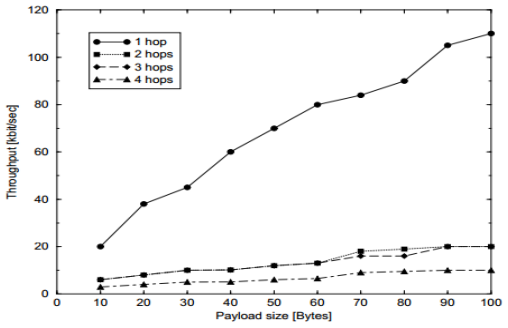

그림 5. 경우 지점 간 802.15.4 네트워크에 대한 출력 측정" 와 같이 수정하기 바랍니다.

Fig. 5. Output measure for a point-to-point 802.15.4 network when one to four routers are present.

In Figure 6, a single recipient scenario is considered where 802.15.4 nodes transmit data to the recipient via a link (star topology) or possibly two jump (3-level tree rotated in the receiver). A network consisting of 30 nodes working in beacon mode is considered. In the figure we show the frequency as a function of the size of the packages sent by the nodes. The speed here represents the number of payloads per second received correctly by the receiver when 30 nodes attempt to access the channel and send their packages, provided that the nodes send packets of the same size.

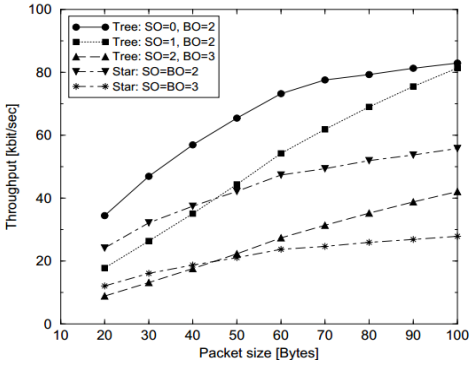

그림 6. 스타 및 트리 기반 토폴로지로 구성된 802.15.4 네트워크의 패킷 크기에 대한 Throughput" 와 같이 수정하기 바랍니다.

Fig. 6. Throughput as a function of packet size for an 802.15.4 network organized in star and tree-based topologies.

To balance equally by reducing, currents have been cut off the same BO value taken (ie super frames have the same time). As we see, small amounts of the market size look like stars, while trees are better than packets, because the nodes have the opportunity to access the channel (buttons are divided into two levels). The best condition in "condition" status as SO = 0 and BO = 2. This, in fact, is selected on the network (with 30 knots and 3-level level) better postponement of the main part of the main-catch fishing platform (where level one killer sends) and an unemployed portion (where level 1 is high).

The difference between the results is given in SO = 0 and BO = 2 because the first find is only to convert down the drops down, while the 30 nodes are finally contending with the channel. Increase the number of keys in one hand increases the fears of data transferred to each room for a while, but on the other hand, the chance to succeed, is the problem where the button has succeeded in providing the package properly believed that the network contains N 802.15.4 buttons that work

in non-bonus mode and compete to provide their packages directly to- zinc.

- System Reliability

The minimum valid data rate was 91.9% obtained in Node 10's VWC reading while the majority valid data rates of sensors in each sensor node were above 97%.

$$NR,val = \frac{Nv}{Nt} \times 100\% \quad (I)$$

Here, Nr was the quantity of packets that acquired a detector station throughout a precise amount of your time, and Sagebrush State was the quantity of valid knowledge of every detector at intervals a detector node throughout constant time. Constant sample area was used for the verification of the transmission power. *Sensor Nodes one to five failed to have EC-TE so the NR,valfor EC-TE ar N/A; detector nodes half-dozen to ten failed to have EC5-4, so the readings were N/A.4.3 In-filed Data Error Rate

During the tests, 246 pseudo PDUs were transmitted in about 45 minutes and the NR,err was 0%.

$$NR,err = \frac{Nv}{Nt} \times 100\% \quad (II)$$

Where Nt was mentioned the total number of PDUs transmitted by the pseudo-station and Ne was the number of PDUs which means field difference.

표 1. 각 센서 노드의 센서에 대한 유효한 데이터 속도
Table 1. Valid data rate for each sensor node's sensors

Node ID	NR,val (%)						
	EC5-1	EC5-2	EC5-3	EC5-4*	VWC*	EC*	Temp*
1	98.5	98.5	100	100	N/A	N/A	N/A
2	100	98.2	100	100	N/A	N/A	N/A
3	99.0	99.5	98.0	98.5	N/A	N/A	N/A
4	98.9	98.9	100	98.9	N/A	N/A	N/A
5	99.5	99	99.5	99.0	N/A	N/A	N/A
6	100	99.4	100	N/A	100	100	99.4
7	99.5	99.5	100	N/A	99.5	100	98.9
8	100	95.7	99.0	N/A	100	100	100
9	100	98.9	99.5	N/A	97.8	100	100
10	99.0	100	99	N/A	91.9	100	100
Average	99.4	98.8	99.5	99.3	91.8	100	99.7

*Sensor Nodes 1 to 5 did not have EC-TE thus the NR,valfor EC-TE are N/A; sensor nodes 6 to 10 did not have EC5-4, thus the readings were N/A.

Ⅳ. CONCLUSION

The Internet of Things as a platform on the Smart Campus has become increasingly popular. It requires an infrastructure consisting of communication networks, sensor nodes and gateways connect to the Internet. Each sensor node is responsible for gathering data from the environment. For the design of a WSN, in fact, define that which will be used in the most appropriate technology and implements the communication protocols are (topology, signal processing, strategies, etc.). If all things are connected to the web and prepared to be accessed by smartphones and alternative PDAs from anyplace for any services, the safety problems shouldn't be resolved. The safety of sensible devices, primarily within the calculation of the threat of threats, that results in an exact loss valuable of devices, is sensitive to device vulnerabilities. IoT and via wireless detector network security, varied factors can rely on the necessities of field security. Security on wireless sensors has attracted attention over the past few years. The use of power and the need for wireless sensors makes the computer level of this process even more challenging than normal networks. Non-secure components can be a point of attack. So it is important to integrate security into any part of declining safety and privacy in all design features. While each security solution can be part of the successful WSN saving method. This document writes an online wireless network for controlling the Smart Campus control.

Reference

[1] Bellis, D. and L. Lapadula. 2013. Secure Computer Systems: Decision-Making Information Sensing Devices. *International Journal of Computer Applications*.**6**(9): 7-10.

[2] Popovic, Z. and K. Hocenski. 2014. Network Security Monitoring for Orginaztion. 33rd MIPRO

International Convention. **8**(6): 344-349.

[3] Adarbah, S. 2015. Energy-Efficient Route Discovery for Noisy Mobile Hoc Ad-Hoc Networks.*IEEE Transactions on Dependable and Secure Computing.***7**(2): 321-331.

[4] Khatri, M., F. Kolhe, T. Dynamic and Z. Alothmani. 2013. Dynamic Address Allocation Algorithm for Mobile Ad hocNetworks. *Convergence of Information and Communication Technology.*30-39.

[5] Maiwald, E. 2012.Fundamentals of Network Security Multiple Security Machineries *IEEE McGraw Hill Technology Education Common Surv Tutorials*, New York. **4**(1): 2-23.

[6] Agrawal, S. 2011. Internet of Things: Future Internet Applications, Engineering (NUiCONE). IEEE Nirma University International Conference, India.1 - 7.
DOI:https/doi.org/10.1109/NUiConE.2011.6153246.

[7] Weis, S.A. 2013. Security and Privacy in Radio-Frequency Identification Devices.*Doctoral dissertation, Massachusetts Institute of Technology,* USA. **7**(1): 678 - 92.

[8] Perrig, A., K. Szewczyk and D. Culler. 2014. Security was Define as the Ability to Deals with a Specific Threat. *ACM Annual International Conference on Mobile Computing and Networking*, Italy. 108-118.

[9] Libelium, Y., D. Huang and S. Wang. 2012. Towards Temporal Access Control in Computing. *31st IEEE International Conference on Computer Communication,* China.**6**(2): 2576-2580.
DOI:https/doi.org/10.1109/INFCOM.2012.6195656

[10] Sami, A.W. and A. Swailem. 2015. A Path Redundancy Based Security Algorithm for Wireless Sensor Networks. *IEEE Wireless Communication and Networking Conference X Kowloon*, China. **6**(3):175 - 182.

[11] Weber, R.H. 2010. New Security and Privacy Challenges.*Compute Law Secure RevFUJITSU Sci. Technology,* England. **2**(1):210 - 233.

[12] Alfred, R. 2014. Security Engineering: A Functional for Internet Communications with Wireless Network Internet of Things with Cellular Networks. *Journal of Security Engineering.* **2**(1): 640-645.

[13] Lampson, B.W. 2012. Wireless Sensor Networks Symposium on Information Sciences and Systems.*International Conference on Computational Science and Its Applications.*18-24.

[14] Kaefer, G., and R.Roman, 2013. WPAN protocol Architecture Corporate Research and Technologies, Munich, Germany, Siemens AG. *IEEE International Workshop on the Web of Things.***14**(4): 1-7.

[15] Alvaro, J. and B. Barros. 2013. A Review Destination Nodes are Distinguishing Devices with Powerful Computation. *Journal of Computer and Applications.***2**(2): 40-45.

[16] Doerr, R. and M.A. Neufeld. 2012. Comparative Analysis of Access Control Systems on Wireless Network Controlling System. *In International Symposium on New Frontiers in Dynamic Spectrum Access Networks*. IEEE.142-146.

[17] Brucker, A., L. Bru, P. Kearney and B. Wolff. 2013. An Approach to Modular and Transmission Security Models of Real World Health care Applications. IEEE 16th ACM Symposium on Access Control Model and Technologies. 2(2): 133-142. ISBN 978-1-4503-1950-8

[18] Adarbah, S. 2015. Energy-Efficient Route Discovery for Noisy Mobile Ad-Hoc Networks.IEEE Transactions on Dependable and Secure Computing.7(2): 321-331.

[19] Choudhury, A.J., P. Kumar, P. Sain, H. Lim and J. Lee. 2015. Strong User Authentication Framework Security. IEEE Asia Pacific Services Computing Conference.110-115.

[20] Chen, D. and H. Zhao. 2012. Data Security and Privacy Protection in Wireless Network Sensor Computing.Computer Science and Electronic Engineering.1(5): 647-651.
DOI: https/doi.org/10.1109/ICCSEE.2012.193

저자 소개

Ahamed Mateen(정회원)

- 2000년 8 월 : 펀 자브 대학교에서 과학 학사
- 2003년 5 월 : 라호르 대학교 MCS
- 2007년 4 월 : 농업 대학 파이살 라 바드 (Faisalabad) 대학 철학 석사
- 2004년 4 월 ~ 현재 : 농업 대학 파이살라 바드, 컴퓨터 공학 강사
- 2017년 ~ 현재. 중국 충칭 대학교 P.hD.Scholar 컴퓨터 과학과 Computer Science Department, Chongqing University China, 400044.
- 그의 관심 분야는 무선, 기계 학습, 네트워크, 실시간 시스템, 분산 컴퓨팅입니다. 농업 모델링 및 시뮬레이션
- Wireless Machine Learning ,Networks, Real Time Systems, Distributed Computing, Agriculture Modeling and Simulation.

Qingsheng Zhu(정회원)

- Qingsheng Zhu (M'11)는 B.S., M.S. 및 Ph.D.를 받았다. 1983 년, 1986 년, 그리고 1990 년에 충칭 대학교에서 컴퓨터 과학 학위를 취득했습니다. 그는 현재 충칭 대학교 (Chongqing University) 컴퓨터 과학 대학의 교수이자 소프트웨어 이론 및 기술의 충칭 키 연구소 (Chongqing Key Laboratory) 소장입니다. 주요 연구 분야는 전자 상거래, 데이터 마이닝 및 서비스 지향 컴퓨팅

Salman Afsar(정회원)

- Dr. Salman Afsar has completed his Ph.D. Computer Science from Tajik National State University. Currently he is serving as Lecturer Computer Science Department UAF, Pakistan. His area of Interest is Network Management and Security.

Muhammad Usman(정회원)

- Mr. Muhammad Usman is currently pursuing his M.Phil. Computer Science from UAF, Pakistan. His area of interest is Sensor Network.