Scientific Research Publishing

Journal of Computer and Communications, 2020, 8, 45-70
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Modeling Secure Home Area Network Based on IoT for Resource Constraints Environment

Minsu Park[1], Mwawi Kayuni[2], Tiwonge Manda[1], Hyunsung Kim[2,3*]

[1]Department of Computer Science, Chancellor College, University of Malawi, Zomba, Malawi
[2]Mathematical Sciences Department, Chancellor College, University of Malawi, Zomba, Malawi
[2]Department of Cyber Security, Kyungil University, Kyungbuk, Korea
Email: *kim@kiu.ac.kr

How to cite this paper: Park, M., Kayuni, M., Manda, T. and Kim, H. (2020) Modeling Secure Home Area Network Based on IoT for Resource Constraints Environment. *Journal of Computer and Communications*, **8**, 45-70.
https://doi.org/10.4236/jcc.2020.81004

Received: December 11, 2019
Accepted: January 7, 2020
Published: January 10, 2020

Abstract

The Internet of things (IoT) can be used in our daily life. Home area network (HAN) is one of the applications of loT. However, deploying HAN for underdeveloped countries in Africa is not easy due to the lack of Internet connectivity and stable electricity. First of all, Internet in Africa is growing fast but the majority of countries in Africa have Internet penetration of less than 10%. Furthermore, the problem of accessing electricity varies greatly across African countries, which is still less than 30% of the average usage rate. The aim of this paper is to model a secure HAN based on IoT for resource constraints environment, which are focused on both network connectivity and energy stability. Poor connectivity, the prevalence of low-end devices and several other obstacles should be considered for the secure HAN deployment in developing and underdeveloped countries. The proposed HAN model will provide the resource constraints module composed of network connectivity function and energy stability function to support the two constraints based on the IoT basic module and the security and privacy module. The proposed HAN model could be securely applied to various countries HAN applications with poor electricity supply and network connectivity.

Keywords

Home Area Network, Security, Privacy, Internet of Things, Delegation

1. Introduction

Home automations and home area networks (HANs) have evolved into more than a connection between autonomous devices. It is evolving towards systems and processes that are becoming more intelligent and systems that are even capable of communicating with people by connecting to Internet, named as Inter-

net of things (IoT) [1] [2] [3]. According to [4], IoT will increasingly be embedded in our natural movements and interactions with our environments, both physical and social. This means we are close to having a transparent social relationship with an autonomous system, in which computers would increasingly enable the integration of simple objects, such as clothing labels, air conditioners, light switches, online classes and more, in an unobtrusive way in the user's life. The requirements for the large-scale deployment of IoT are rapidly increasing with major security concerns [5]. There are various communication standards for HAN including Bluetooth, IEEE 802.15.4 specifics the physical (PHY) and medium access control (MAC) layer standards of ZigBee and supports very low power consumption, making it a cost-effective technology [6]. The ZigBee alliance has been working on solutions for smart energy, home automation, building automation and industrial automation. There are two operation modes defined for IEEE 802.15.4 multiple-access schemes, *i.e.*, beacon enabled and non-beacon enabled modes. This paper will only focus on ZigBee as the default communication inside of the house.

The Internet in Africa is growing fast. Internet penetration levels are about 20% and rising. Mobile subscriptions are just 70% and mobile broadband access accounts for more than 90% of Internet subscriptions. At the high end of the spectrum, countries such as Morocco enjoy penetration rates above 50%, but at the other end are countries with penetration rates below 2% and the majority of countries have Internet penetration of less than 10. Considerable work is now underway to improve the conditions that currently mean users in Africa pay up to 30 or 40 times more for Internet access than their peers in developed countries [7].

Furthermore, the problem of accessing electricity varies greatly across countries. Many North African and island countries achieve high rates of access. But several countries have extended the electric grid to only a third or less of the country. Examples include Burundi (17%), Burkina Faso (25%), Sierra Leone (29%), Niger (30%), Guinea (31%), Liberia (31%) and Mali (32%). West and East African countries lag behind other regions in extending the grid. Southern Africa is a mixed picture, with many countries falling below the 36 country average (66%). These include Zimbabwe (62%), Namibia (62%), Zambia (50%), Mozambique (50%) and Malawi (42%) [8].

Especially in Malawi, low rates of Internet and mobile phone access are largely a result of high costs, which include expensive value-added taxes (VAT) of 17.5 percent on mobile phones and services and a VAT of 16.5 percent on Internet services, the costs of which are borne by consumers [9] [10]. Also, the electricity grid is concentrated in urban centers, but only 25 percent of urban households have access, compared to a mere 1 percent of rural households. Half of formal sector enterprises in Malawi rely on backup generators [11]. With our best knowledge, there is no research to solve the infrastructure constraints for IoT based HAN.

To solve the underdeveloped and developing countries' infrastructure problems, this paper proposes a new model of secure HAN based on IoT. To achieve the goal, we set our objectives as follows:

- Design a secure HAN architecture for resource constraints environment, especially focused on lack of network connectivity and energy stability.
- Design a security and privacy module for the HAN model built on delegation based security scheme.
- Implement the secure HAN model using Raspberry Pi and Arduino.

The proposed secure HAN model has three important modules, IoT basic module, resource constraints module and security and privacy module. The basic functions for HAN services are provided based on the first module in normal status. However, the proposed secure HAN model performs the resource constraints module if it copes with the harsh constraints to access network or electricity. Thereby, it provides two sub-functions named as network connectivity function and energy stability function. Security and privacy module should support the other two modules, which will be placed below from them. The proposed secure HAN model could be applied to various countries with poor electricity supply and network connectivity.

The rest of this paper is organized as follows; in Section 2, we provide preliminaries such as; basic mathematical and cryptographic concepts and related works. Section 3 proposes a new model to secure HAN based on IoT for resource constraints environment in detail. Simulation results are given in Section 4. Finally, Section 5 concludes this paper.

2. Preliminaries

This chapter summarizes some basic mathematical and cryptographic concepts, which are major tools in the security and privacy module for the proposed HAN model, and reviews related works. First of all, the definition of proxy signature and elliptic curve cryptosystem (ECC) are reviewed [12] because various delegation based authentication protocol uses ECC as their basic operation [13] [14]. Furthermore, advanced encryption standard (AES) is reviewed for confidentiality support. After that, we review related works [15]-[30]. These will guide a new HAN model setup to withdraw some required features to be achieved.

2.1. Basic Mathematical and Cryptographic Concepts

This subsection gives an overview of some mathematical preliminaries which are useful in the security and privacy module in the proposed HAN model. For more details on them, refer to [12] [14].

Designated confirmer signatures allow a signer to designate someone else to verify his (or her) signature [13]. Alice, for instance, needs to go on a business trip to someplace which does not have very good computer network access. Or maybe she is incapacitated after major surgery. She expects to receive some important e-mail, and has instructed her secretary Bob to respond accordingly.

How can Alice give Bob the power to sign messages for her, without giving him (or her) private key? Proxy signature is a solution [12]. Alice can give Bob a proxy, such that the following properties hold:

- Distinguishability: Proxy signatures are distinguishable from normal signatures by anyone.
- Unforgeability: Only the original signer and the designated proxy signer can create a valid proxy signature.
- Proxy signer's deviation: A proxy signer cannot create a valid proxy signature not detected as a proxy signature.
- Verifiability: From a proxy signature, a verifier can be convinced of the original signer's agreement on the signed message.
- Identifiability: An original signer can determine the proxy signer's identity from a proxy signature.
- Undeniability: A proxy signer cannot disavow an accepted proxy signature he created.

In some cases, a stronger form of identifiability is required that anyone can determine the proxy signer's identity from the proxy signature. Proxy signature protocols, based on different digital signature protocols, are in [12].

ECC utilizes the mathematics behind equations of elliptic curves (EC) [13]. Basic EC equation is $y^2 = x^3 + ax + b$. It has horizontal symmetry and any non-vertical line will intersect the curve in 3 places at most. A common version of ECC is ECC with Diffie Helman (ECDH). Its equation is $y^2 = x^3 + ax + b \pmod{p}$, where p is a prime number. It relies on the difficulty of EC discrete logarithm and offers similar strength with smaller keys. It is faster, but more secure. ECC uses complicated mathematics. That is its biggest weakness.

The following is an example of ECDH between Alice and Bob [12].

- All parties are aware of $y^2 = x^3 + ax + b$, P, a, b, G, n and h.
- Bob picks a private key B, $1 \le B \le n - 1$ and computes $B = BG$.
- Alice picks a private key a, $1 \le a \le n - 1$ and computes $B = BG$.
- Alice picks a private key a, $1 \le a \le n - 1$ and computes $A = aG$.
- Bob sends Alice $B = (xB, yB)$. All know about A and B.
- Bob computes $SK = BaG$ and Alice computes $SK = aBG$.

AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standard and Technology (NIST) in 2001 [31]. AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. This paper will only consider 128 bits of the key size.

2.2. Related Works

In recent years, wireless sensor and actuator networks (WSNs and WANs) have gained high momentum, receiving significant attention from academia, industry and standards development organizations. One of the primary application domains of this technology is home automation networks. HANs enable monitor-

ing and control applications for home user comfort and efficient home management. The different HANs have been affected by several initiatives from the government, industry, utility companies, standard committees and technology groups [15].

This section provides related works on ZigBee based HAN [16]-[30]. Theses researches can be loosely categorized into three major classes namely: 1) security [16] [17] [18], 2) smart surveillance [19]-[24] and 3) energy management [25]-[30]. In security applications, HAN has been proposed to ensure security of a home. One of the early experimental ZigBee based home security system has been proposed in [16]. This system is capable of monitoring door and window, smoke, gas leak and water flooding in a home from a remote location. Some simple control systems have also been associated with this application. The security alarming system has been implemented by using ZigBee chip and low power consumption micro-controller. The system also supports Web interface so that a user can access the system remotely to control, search and review record. The system was configured by using an LCD panel. Another similar system has been proposed in [17]. The system has been developed for automatic door opening and closing, temperature monitoring, gas detection and light control. RFID, ZigBee and GSM have been used to implement the system. Intelligent home automation system (IHAM) has been presented to ensure security at home [18]. The system uses PIC microcontroller with ZigBee wireless communication technology, speech recognition technique and GSM network. The system has also integrated a security warning system with it so that the users can be warned about the fire hazards. This warning system has been implemented by using a smoke sensor and GSM module. The system is able to send an SMS to the user if smoke is detected.

In intelligent surveillance applications, HAN has been used to monitor the activities at home. Some of these systems also allow a user to do the same from a remote location. One such system based on ZigBee has been designed in [19]. The system transmits periodic data from a location information service to determine the current position of a user. In a similar work, digital living network alliance (DLNA) compliant digital home appliances have been addressed [20]. The authors have claimed that the ZigBee technology can be considered a suitable solution for such type of network. To interconnect DLNA compliant home appliances with a ZigBee network, a Gateway is necessary. The authors have proposed the architecture of such Gateway. They also proposed an energy efficient method for controlling the WSN. The authors have proved that the system is power efficient by measuring the power consumption in the network. Another HAN gateway based on ZigBee technology has been proposed in [21]. The system has realized the connection of low rate HAN and Internet. A user can control the home appliances through the HAN gateway. This was one of the earliest works to depict that the home appliances could be controlled from a remote location via Internet. The hardware and software used to design the home gateway and device nodes have also been presented in the same work. Another similar

wireless remote monitoring for HAN security has been proposed in [22]. In this work, a real time surveillance of the HAN security was developed based on variety of sensors, the ZigBee technology and GSM/GPRS network. The system can send abnormal images and warning messages through MMS and SMS. The system can also receive remote instruction to monitor and control the household appliances. The reliability of the system has been tested and the authors have claimed that their system can successfully guarantee HAN security for a remote user. A ZigBee WSNs of star topology has been proposed for wireless intelligent HAN in [20]. The system is suitable for a typical small HAN. The system can be remotely monitored and controlled by using GSM module. The system is composed of the following three main components: 1) home server (HS) with GSM module, 2) intelligent environment detection sensor modules, and (iii) intelligent home appliances. The concepts and the architectures of the system have been discussed in the same work. The system has been tested to ensure its remote alarming and control ability. Another HAN based on IoT and the ZigBee WSN technology has been proposed in [24]. The authors have implemented the system by using Texas Instruments MCU device. Users can access this system by using a dynamic webpage of LwIP TCP/IP protocol stack or GSM SMS. By using this system, a user can monitor and control the environmental parameters such as temperature, humidity, meter readings and light of a home.

In energy management applications, HAN has been used to save energy consumed in a home. This energy saving is achieved by controlling the electrical and electronic home appliances. One such ZigBee based power monitoring system (PMS) has been reported in [25]. In addition to ZigBee wireless communication, the PMS also utilizes digital signal processing (DSP) and Web services. The system has been constructed, tested and validated for the power management of a campus. The test results show that the functions of the PMS comply with the designed objectives. Some of the ZigBee based energy efficient system has been targeted to control the power of electric outlets for saving energy. One such work has been proposed in [26]. The system can also measure the currents drawn by electric outlets. The system has been implemented by using an embedded board and the ZigBee technology. This system has two main components namely ZigBee control module and the server module. The ZigBee control module consists of several controllable outlets, a current measurement circuit, a ZigBee transmitter, a ZigBee receiver and a micro control unit. The system can detect any overload and can send a message to the circuit breaker to safely turn off the power. In order to overcome the architectural limitations of WSN a ZigBee based intelligent self-adjusting sensor (ZiSAS) has been introduced in [27]. The ZiSAS uses a situation-based self-adjusting scheme. Hence, ZiSAS is an event driven self-adjusting sensor network implemented by using hardware and middleware. In many industrial applications, the cost of a WSN is not an important factor. It is more important to deploy the network in rapidly changing application environments and design requirements. In this regard two major issues are: 1) to rapidly construct application software for different design re-

quirements, and 2) to operate the system smoothly. One such rapidly deployable system has been reported in [28]. An automatic embedded software generation framework has been proposed in this work that can rapidly create and evolve ZigBee applications. The framework consists of several major modules namely: 1) pattern extraction, 2) code generation, and 3) architecture mapping. The authors have provided an embedded software development framework that integrates the heterogeneous readers and sensors interfaces with an optimal energy control model to enhance the quality of digital home living environments. In [29], the authors have suggested the requirements for an appropriate technology for HAN. They have claimed that selection of an appropriate technology for home and industrial automation systems should be based on low cost, easy placement and installation, easy extension, comfort benefits and mobile device connectivity. An energy aware HAN satisfying all these requirements has been proposed in [30]. The system can control load and hence can save energy. This ZigBee based system is used for remote controlling and monitoring of various home loads/appliances. The objective is efficient power utilization through real time power level indicator with the help of a PC-based GUI application.

In order to enable seamless, robust, efficient and reliable HAN communications and hence realize the high expectations for HAN communications, many research problems need to be thoroughly analyzed and solved. In the following, the authors in [2] highlighted some key research challenges. We will restrain the research issues into the following aspects.

- Design of HAN is challenging, as each node typically consists of a sensor, a radio transceiver, a microcontroller and an energy supply. In addition, the node should possess some intrinsic features, such as: low-cost, low-complexity, low-size and low-energy. Each node must have the ability to maintain long-running operation by faultlessly solving the problem of energy supply.
- Security and privacy remain a very important concern because the existing HAN applications tend to rely on legacy security schemes.

3. Modeling a Secure HAN Based on IoT

The main concern of the proposed HAN design is how to provide stability to user even in the harsh situations of network offline and blackout based on secure and privacy preserving seamless services. **Figure 1** shows the conceptual system configuration for a secure HAN model based on IoT resource constraints environment, which will be implemented on Raspberry Pi.

As shown in **Figure 1**, we consider the smart home environments with multiple IoT devices and services that collect, process and exchange data with home server (HS). The environment provides users several possibilities to control and adapt the status of their home, either manually or automatically and also locally and remotely. To support the requirements, IoT devices and services exchange data with internal and external actuators. Theses interactions take place with mobile applications on user's device and also with the remote central server

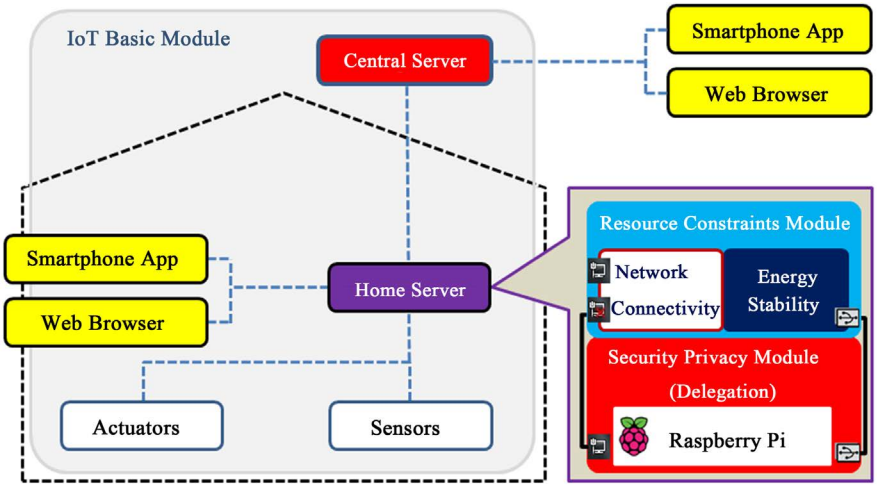

Figure 1. Conceptual Han model based on IoT for resource constraints environment.

(CS). This section proposes a secure HAN model for resource constraints environment, which is composed of IoT basic module, resource constraints module and security and privacy module with the following features.

- IoT basic module: It defines the basic functions for CS, HS and sensors/actuators during mandatory situation, which does not have any harsh situations. Each entity cooperates with each other over the security and privacy module.
- Security and privacy module: It has the very important role in the proposed HAN model because the security provision and the privacy preserving are top most important features in HAN applications. For these requirements, this module provides confidentiality, integrity, authentication and key agreement.

There are three main goals of this paper, modeling a HAN, identifying critical factors of it and assessing potential factors to it. So, it is possible to see those important goals by using Figure 1 network environment. First of all, secure HAN model will be developed, which is adaptable to resource constraints environment that could have definitions and relationships of all entities via communication line. For this, critical constraints factors on the HAN should be identified that influence implementation and operation of the HAN based on two important functions, network connectivity and energy stability. Furthermore, assessment of potential factors would be considered that may influence the use of HAN solution based on the security and privacy module.

3.1. IoT Basic Module

It has the most important role in the proposed secure HAN model, which are composed together with two different modules, resource constraints module and security and privacy module. Figure 2 presents a generic interaction model for the proposed HAN model. The HAN sensors measure applicable environmental properties such as temperature, motion and video, using periodic or aperiodic,

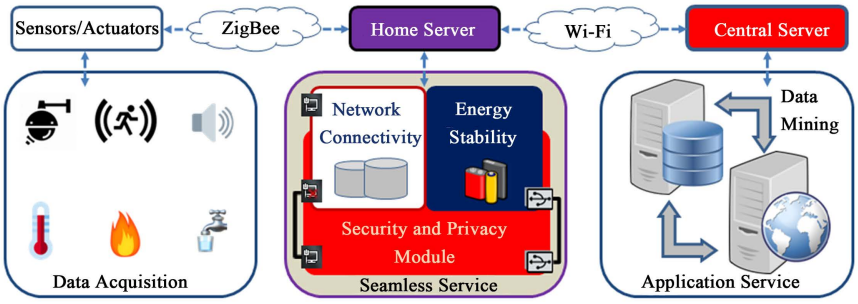

Figure 2. HAN core interaction model.

i.e. event-driven sampling sequences. The data measured by sensors are normally stored in CS after traveling through HS.

Here, HS may regularly communicate to CS or it may just keep the data in its own database depending on the network situation. Data from the sensors can then be accessed by authorized entities such as controllers, which may follow a push or a pull schedule for the data collection. CS processes the received information, correlates it with other information sources and decides upon appropriate actions to be initiated with reference to the combined events, reported and analyzed. These actions are executed with the help of actuators based on the command initiated by CS. Actuators have the capabilities to impact and change the environmental properties such as the changing the temperature or the light bulb changing the light intensity.

It is very important to use proper time schedule for data acquisition and transmission in scenarios of HAN model. Thereby, the proposed HAN model users **Figure 3** time factors as basic scheduling of each entity. There are two main time factors, ΔT_{in} and ΔT_{out}, which are used as inbound scheduling and outbound scheduling based on HAN.

Sensor/actuator is considered to be an electronic platform with some wired or wireless connectivity such as Bluetooth, ZigBee, or an analogue or digital wired connection. The common feature of it is to write the compete procedure of initializing the connected sensors and actuators, read the value, and send the values to a defined destination. The operation is to have a service such from a HS or a CS that receives requests and parse them to respond with proper content, such as the value of the sensor in every ΔT_{in}. Sensor/actuator only communicates wirelessly to HS based on ZigBee regularly. **Figure 4** shows the basic state transition diagram to show functions of sensors and actuators.

Each of sensor and actuator has a tight connection with IoT device to control and react with the cooperation to HS. Actions are executed with the help of actuators based on the commands initiated by CS or HS. Actuators have the capabilities to impact and change the environmental properties such as the changing the temperature or the light bulb changing the light intensity. It also needs a means to authenticate each device to HS and to provide security and integrity of messages. Finally, this work is targeted to be generic and application domain

Figure 3. Time factors for the proposed HAN model.

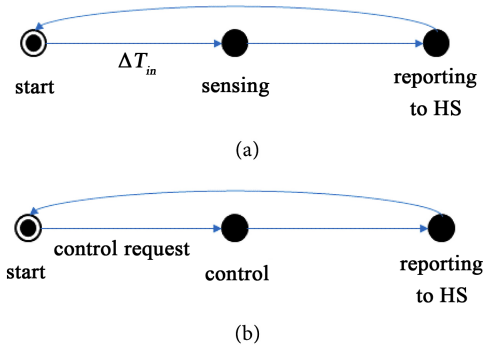

Figure 4. Basic functions on sensors and actuators. (a) Sensor data acquisition and transmission function; (b) Actuator control function.

independent. As such detailed analysis of security considerations for each application domain go beyond the main focus of this work.

HS is an electronic system, such as a Raspberry Pi or communicating not only with IoT devices, but also with Internet. The purpose of HS is twofold: it enables devices with different protocols to interact with each other, and at the same time it can process data for aggregation, analysis or security purposes and perform temporary data storage. Since HS needs to keep physical proximity with sensors/actuators, it is likely to be deployed inside a HAN. As a result, it does not necessarily offer services to Internet through inbound connections.

Here, HS may regularly communicate to CS or it may just keep the data in its own database depending on the constraints environment. Data from the sensors in every ΔT_{in} can be accessed by authorized entities such as controllers, which may follow a push or a pull schedule for the data collection. HS communicates wirelessly to sensors/actuators based on ZigBee and to the remote CS based on Wi-Fi. It serves as gateway for these devices to the external world providing access to Internet by connecting to CS or a local network. It can reside inside of any smart systems like HAN, which is accessible from its own local networks and CS via Internet. In most cases, direct communication with registered users is only possible if it is in the resource constraints mode. However, it is recommendable to access via CS to ensure privacy and security needs of the interacting system. More details on the security and privacy requirements of HS come later on after this subsection.

Figure 5 shows the basic state transition diagram to show functions of inbound and outbound of HS. Normally, the proposed HAN model could set ΔT_{in} and ΔT_{out} as the same time interval for the realtime application. However, ΔT_{out} could be set as a bit bigger than ΔT_{in} for the communication efficiency. Thereby, the basic function of HS is focused on the forwarding the data from sensor to CS.

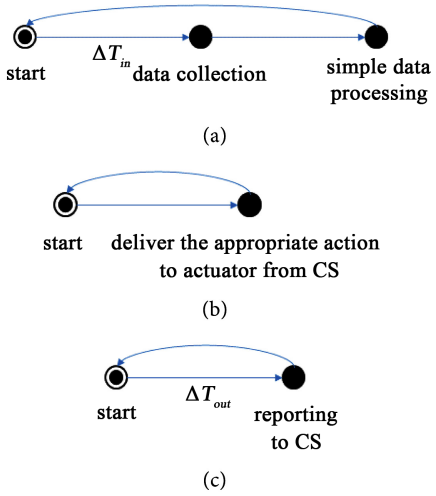

Figure 5. Basic functions of HAN. (a) Data collection function; (b) Data transfer function to CS; (c) Control request deliver function to actuator.

CS can be any application server on Internet offering services to HS. The proposed HAN model calls such systems external from HAN as they are not in direct control of the user but are not limited to access Internet. Moreover, these systems can include some storage capabilities to fulfill the application's goal. However, even though some storage-related calls could be invoked by HS, the gateway, the external system would do some kind of processing on the data, therefore controlling data in terms of format, size, etc. CS is a term the proposed HAN model uses to refer to systems offering data storage functionality. Such systems can offer any kind of storage and querying interface. In Contrast to external systems, which manipulate input data following a specific business logic, external storage system stores and return data as provided by the user. CS processes the received information from the sensors via HS, correlates it with other information sources and decides upon appropriate actions to be initiated with reference to the combined events, reported and analyzed. **Figure 6** shows the basic state transition diagram to show functions of CS. The basic function of CS is to do data mining to provide convenient service to users after collecting sensed data from sensors. Furthermore, CS could support proper control to the proposed HAN model by controlling actuator.

Owing to the fast development of big data mining, it is feasible to utilize big data technology to extract interesting patterns or knowledge to enhance the HAN services. The transmission of large volume of data collected by sensors puts a heavy burden on sensors or HS, and as a result, data mining can be preexecuted only in CS.

3.2. Resource Constraints Module

As shown in **Figure 2**, HS does the main role for the resource constraints environment, which is based on network connectivity function and energy stability function over the security and privacy module. The information processing is

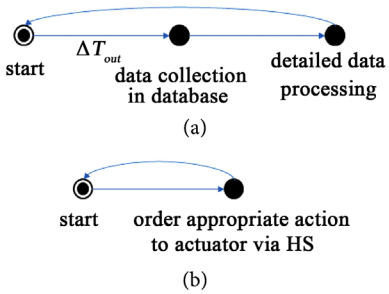

Figure 6. Basic functions of CS. (a) Data collection function; (b) Control request function to HS.

further divided into two sub-processes. When HS detects changes of the HAN parameters, it primarily deals with the information by itself. Otherwise, it initiates the connection request and transmits the received information to CS. It has the main role of HAN model between entities inside and outside of home.

This module supports Internet connectivity from HS to CS. Internet connectivity refers, which always present in IoT devices even in network offline situation and interconnected inside and outside the home. If user is in network offline, HS works as a temporal server, which collects data and provides home automation service for the whole IoT entities. However, it works as a gateway role to CS when network is online as the mandatory case. By using this module, the proposed HAN module can provide network connectivity more easily for the home appliances. This module also should be operated over on the security and privacy module.

On the other hand, HS is teamed up with another component called simple rules engine. The rules engine processes incoming sensed messages, further processing or analytic them and then controls actuators for immediate control to cope with the disastrous situation of HAN if it is in the network offline situation. This enables the possibility to build IoT applications that orchestrate, collect, process, analyze and act on data generated and published by connected devices globally without having to pay attention to the network constraints. In order to maintain usability, developers can author rules and add them to the rules engine by writing SQL-like statements. The actions list specifies a set of actions that should be performed when the SQL statement is executed.

Figure 7 shows the network connectivity state transition diagram to show functions of HS in the network constraints mode. HS keeps the sensed data and sends them to CS right after the network is reconnected. However, it needs to control HAN directly if it is emergency situation by simply check the rules engine condition with the collaboration with the actuator.

This function is designed to support power in blackout situation to HS, which is based on a rechargeable extra battery. Stability refers always powered on for IoT devices to be controlled even in blackout situation. Normally, HS should always be accessible to users and IoT entities even in blackout status due to emergency reasons to control home appliances. To support this module, the proposed HAN model uses at least a backup battery with periodic sleep mode. Figure 8

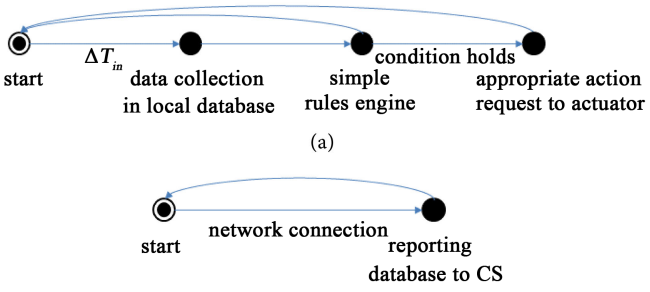

Figure 7. Network connectivity function. (a) Data acquisition and IoT control request function; (b) Data transfer function to CS.

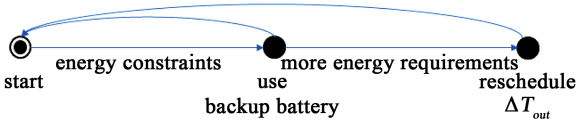

Figure 8. Energy stability function.

shows the energy stability transition diagram to show functions of HS in the energy constraints mode.

For the normal condition, HS uses landline electricity and charges the backup battery if it has low leftover battery. However, the system uses the backup battery in blackout situation for the availability. This module also should be operated over the security and privacy module.

For the normal condition, HS uses landline electricity and charges the backup battery if it has low leftover battery. However, the system uses the backup battery in blackout situation for the availability. This module also should be operated over the security and privacy module.

3.3. Security and Privacy Module

This module concerns security and privacy associated with smart environments and specifically to support confidentiality, integrity, authentication, key agreement and privacy in the presence of a multitude of constrained devices and often interactions with unknown principals. In order to allow the secure bootstrapping of IoT devices, we assume that each IoT device is able to establish a location-limited channel, by having an infrared port. Of course, if the device is to be controlled remotely it should also support other communication media. This module should cope with the threats including man-in the middle attack, injection of wrong data, unauthorized information gathering, redirection of messages, replay of messages, manipulation of messages, communication sniffing, gathering metadata and denial of service. To cope from the attacks, the proposed HAN model should provide mutual authentication, freshness, integrity, confidentiality, privacy and availability by adopting various security schemes and protocols based on the delegation based schemes. The security of IoT in general, consists to provide the following services.

- Confidentiality: It ensures that information is made unintelligible to unauthorized individual, entities and processes.
- Integrity: It ensures that data has not been modified by a third party (accidentally or intentionally).
- Authentication: It verifies that the data source is the pretended identity.
- Key agreement: It is to make two or more parties to agree on a key in such a way that both influence the outcome, which is used for the other security services.
- Privacy: It ensures that user's identities should not be identifiable nor traceable from their behaviors and their performed actions in the system.

In the context of IoT, confidentiality caters for protecting privacy of sensors/actuators, integrity looks after the data contained within the IoT devices. Any failure for the security would seriously threaten entity privacy in IoT. To provide confidentiality, the most contemporary standard symmetric key cryptosystem (CSKC) will be employed to encrypt data as a symmetric cryptosystem. Doing so, even if the exchange data is eavesdropped, the attacker will not be able to access its content. The CSKC should rely on the secrecy of the keys, which could be derived from the delegation based authentication and key agreement.

Any breach of data integrity will mean that an IoT entity cannot operate correctly but it also potentially exposes the entity to being exploited and become a compromised platform from which other attacks can be launched. The method of verifying the integrity of data is by a mathematical algorithm called a hash. IoT data requires to be protected from modification while on its journey from sensor to remote CS. While a hash technique can be used an attacker could make a change to the message and recalculate the hash. A stronger approach is by using a data integrity check with a shared private key called a keyed-hash message authentication code (HMAC). And since it needs a shared private key it must be protected just like any other cryptographic key. Configuration of data for communication and any stored device data should always be encrypted and together with the HMAC.

The authentication and key agreement of each entity in the proposed HAN model are based on the delegation based scheme. The mandatory authentication and key agreement for mobile user to access the proposed secure HAN model via the remote CS by delegating HS's right. However, the mobile user with a mobile station (MS) will directly communicate with HS when the HAN is in network connectivity module or energy connectivity module, which is in strict security and privacy constraints. This module adopts the basic notions from the schemes in [32] [33] [34] and further redesign to get an optimized one.

This section provides a new development of delegation based user authentication and key agreement protocol, which keeps the merits of the original protocol and can provide user privacy. Since the focus of this paper is on authentication and key agreement of MS, which is out of the coverage of its gateway, we assume that any message between MS and its HS has to go through a CS. Also, HS of MS is assumed to have a communication link to CS that is to serve the MS. The del-

egation based user authentication and key agreement protocol have three phases: setup phase, the on-line authentication and key agreement phase and the off-line authentication and key agreement phase.

[**Setup phase**] First of all, HS chooses two private keys x and x_s, and then computes their corresponding public keys $v = x \cdot P$ and $y_s = x_s \cdot P$, respectively. Next, HS selects a random symmetric key K_{HS} with CS. After that, HS shares K_{HS}, x_s and v with CS. HS chooses a random number k as a secret key and also computes proxy key pair $K = k \cdot P$ and $\sigma = x + k \cdot H(K) \pmod q$ for each MS. Then, each MS's generated proxy key pair (σ, K) is stored in HS's database, and each MS's proxy key pair (σ, K) and public key y_s are stored in each corresponding MSs SIM card, respectively.

[**On-line authentication and key agreement phase**] The conceptual phase is shown in Figure 9 For each online authentication and key agreement session, MS precomputes $H^{(1)}(n_1)$, $H^{(2)}(n_1)$, ..., $H^{(n+1)}(n_1)$ and stores them in its SIM card,

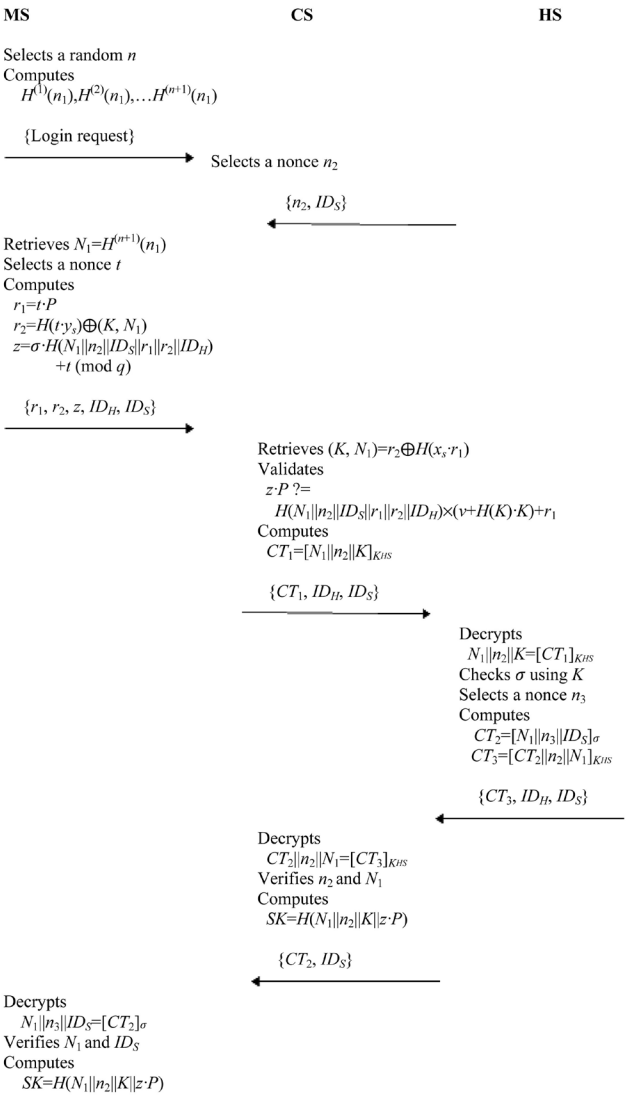

Figure 9. Privacy preserving delegation based user authentication and key agreement.

where n_1 is a random number and n is the total amount of time for offline authentication and key agreement supported by the protocol.

Step 1. MS → CS: {Login Request}

MS sends a login request to CS.

Step 2. CS → MS: $\{n_2, ID_S\}$

CS sends $\{n_2, ID_S\}$ to MS, where n_2 is randomly generated by CS.

Step 3. MS → CS: $\{r_1, r_2, z, ID_H, ID_S\}$

MS retrieves $N_1 = H(n + 1)(n_1)$ from its SIM card, and then computes $r_1 = t \cdot P$, $r_2 = H(t \cdot y_s) \oplus (K, N_1)$ and $z = \sigma \cdot H(N_1||n_2||ID_S||r_1||r_2||ID_H) + t \pmod q$, where t is a random number. Next, MS sends $\{r_1, r_2, z, ID_H, ID_S\}$ to CS.

Step 4. CS → MS: $\{CT_1, ID_H, ID_S\}$

CS first uses x_s to retrieve K and N_1 by computing $r_2 \oplus H(x_s \cdot r_1)$. Next, CS computes $z \cdot P$ and $H(N_1||n_2||ID_S||r_1||r_2||ID_H) \cdot (v + H(K) \cdot K) + r_1$, and then verifies whether the two computed values are the same. If the verification establishes, CS computes $CT_1 = [N_1||n_2||K]\ K_{HS}$ by using K_{HS} as the encryption key and then sends $\{CT_1, ID_H, ID_S\}$ to HS. Otherwise, CS denies the login request.

Step 5. HS → CS: $\{CT_3, ID_H, ID_S\}$

HS obtains $N_1||n_2||K$ by decrypting CT_1 with the secret key K_{HS}. Next, HS finds its corresponding σ from its database according to the decrypted K. HS computes $CT_2 = [N_1||n_3||ID_S]\ \sigma$ and $CT_3 = [CT_2||n_2||N_1]_{KHS}$, where n_3 is a random number and SK is the session key. Finally, HS sends $\{CT_3, ID_H, ID_S\}$ to CS.

Step 6. CS → MS: $\{CT_2, ID_S\}$

CS obtains $CT_2||n_2||N_1$ by decrypting CT_3 with the secret key K_{HS}, verifies whether n_2 and N_1 exist in the decrypted string $CT_2||n_2||N_1$ and then computes $SK = H(N_1||n_2||K||z \cdot P)$. If the verification holds, CS sends $\{CT_2, ID_S\}$ to MS. After receiving the message from CS, MS obtains $N_1||n_3||ID_S$ by decrypting CT_2 with the key σ and then checks whether N_1 and ID_S exist in the decrypted string $N_1||n_3||ID_S$. If the condition holds, MS computes the session key $SK = H(N_1||n_2||K||z \cdot P)$.

[**i-thoffline authentication and key agreement phase**] MS retrieves $H^{(n-i+1)}(n_1)$ from its database and sends $[H^{(n-i+1)}(n_1)]_{Ci}$ to CS. Upon receiving $[H^{(n-i+1)}(n_1)]_{Ci}$, CS decrypts encrypted message $[H^{(n-i+1)}(n_1)]_{Ci}$ and computes $H(H^{(n-i+1)}(n_1))$. After that, CS verifies whether the computed value $H(H^{(n-i+1)}(n_1))$ is the same as the stored value $H^{(n-i+2)}(n_1)$ in its database. If the condition holds, CS replaces $H^{(n-i+2)}(n_1)$ with $H^{(n-i+1)}(n_1)$, and computes the session key $C_{i+1} = H(H^{(n-i+1)}(n_1), C_i)$ and increases $i = i + 1$.

4. Simulation

The purpose of this section is to provide simulation results and analysis of the proposed HAN model. The model is implemented using Raspberry Pi with Arduino. Thereby we will, first of all, implement the proposed HAN model. Raspberry Pi will pose the role of HS but two Arduino devices will play home appliances in a HAN. However, a Laptop is used to from a CS with database.

In order to check the functionality of the proposed HAN model, this section

provides simulation results, which is focused on fire detection and alarm system based on IoT. A key aspect of fire protection is to identify a developing fire emergency in a timely manner, and to alert the building's occupants and fire emergency organization. Fire is crucial for the development of human society and it has become an important part of human civilization. Among different types of disasters, fire constitutes a significant threat to life and property in urban and rural area.

Upon fire occurrence, sensors will operate. The actuator will react to extinguish the fire from SS's request or CS'S request depending on the network situation, which the HAN model recognizes as an emergency condition. The HAN model will then activate one or more signaling circuits to sound building alarms and summon emergency help. It may also send the signal to another alarm system so that it can be monitored from a remote point.

Figure 10 shows the HAN model simulation environment focused on the fire detection and alarm system based on Arduino, Raspberry Pi and Laptop. To further explain this, assume that a building's fire alarm system has 2 circuits, which has a smoke detector and a fire distinguisher, which is specified shown in Table 1. A fire ignition in the room causes a smoke detector to go into alarm. This will be reported by HS or CS as a fire in circuit. Each of HS and CS requires some forms of operational test to verify it is in working condition. The proposed HAN model has been validated by means of a wide functional evaluation. The main goal this simulation is to show the functionality impact of the proposed HAN model and its sustainability on different environment with constraints. In order to test constrained sustainability of the proposed HAN model, we performed two main experiments focused on the energy and the network.

Table 1. Specification of the simulation envornment.

Entity	Device	Specification
Sensors/Actuators	Actuator-Arduino R3 Sensor-DHT11, MQ-9	• Microcontroller: ATmega328 • Flash memory: 32 KB of which 0.5 KB • Used by bootloader • SRAM: 2 KB • EEPROM: 1 KB
Home Server	Raspberry Pi 3	• SoC: BCM2837 • CPU: Quad Cortex A53 @ 1.2 GHz • RAM: 1GB SDRAM • Storage: micro-SD • Ethernet: 10/100 • Wireless: 802.11n/Bluetooth4.0
Portable Battery	PLM06ZM	• Battery type: Lithium polymer • Charge time: 10 hours • Battery capacity: 20,000 mAh
Central Server	Laptop-LGU56	• Intel(R) Core (TM) i3-3217U CPU • Window 10 pro • 4 GB RAM • 64 bits

The aims of the experimental sessions are planned to answer the following questions.

- Could the proposed HAN model provide stable HAN services even if the target HAN environment is in the constrained situation?
- What is the maximum period does the proposed HAN model provide services even if the target HAN environment is kept in the constrained situation?
- Does the proposed HAN model work on a real Zomba environment scenario with the constrained situation?

Figure 11 shows the energy consumption simulation results depending on the variation of ΔT_{in} and ΔT_{out} within 1 hour. We assumed that there are communications between HS and CS only after the communication between HS and IoT device. For the clarity, Figure 11 shows the variations on energy consumption rate depending on ΔT_{in} of 2, 4, 6, 8 and 10, which has effects to ΔT_{out}.

The proposed HAN model could support service for 46 hours and 23 minutes even if it has a severe energy constraint. It should use much bigger capacities' battery if the system requires more energy constraints support. We've been simulated the system functionality for a month from August 1 to August 31 and found out the blackout pattern of 5 hours at most. It is recommendable to use a battery with 5000 Amh in that constraints.

Furthermore, for the network constraints simulation, we also used the proposed HAN model and found out that it provides good functionalities even if it is in the network constraints situation.

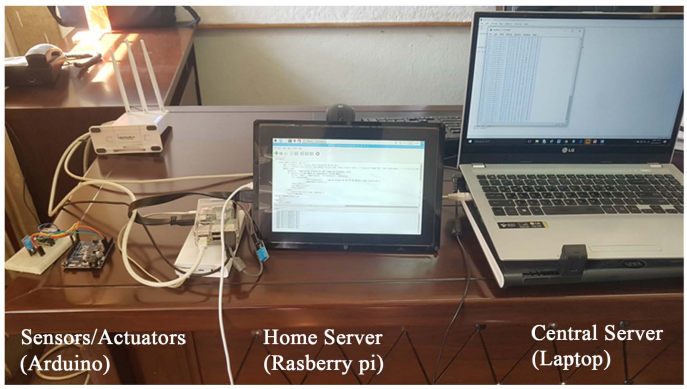

Figure 10. HAN model simulation environment for fire detection and alarm system.

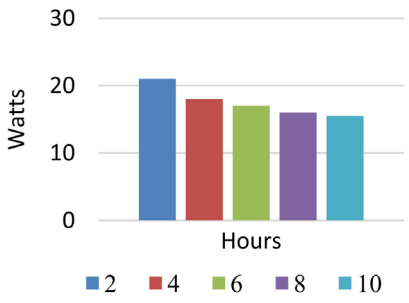

Figure 11. HAN model energy consumption simulation results.

5. Conclusions

This paper has been proposed a secure HAN model based on IoT for resource constraints environment, which is focused on network connectivity and energy restrictions. Poor connectivity, the prevalence of low-end devices and several other obstacles should be considered for the secure HAN deployment in developing and underdeveloped countries. The proposed HAN mode provides network connectivity module and energy connectivity module to support the two constraints based on the basic module for security and privacy. Both of two modules distinguish the constraints situations and disconnect the connection with two modules distinguish the constraints situations and disconnect the connection with the remote server but work in standalone mode. Security and privacy module adopt the delegation based security to provide confidentiality, integrity, authentication and key agreement of HAN that CS delegates security service of HS. The proposed design could be securely applied to various countries with poor electricity supply and network connectivity.

Further research should be performed focused on the real environmental field tests and revision. There should be a need to revisit the current HAN model and the extent to which applicant-led rezoning could help achieve the balance between certainty and flexibility. During this research, we have realized that adopting the proposed HAN model is critical to the optimal service and re-source management in heterogeneous IoT networks and their applications.

Acknowledgements

The results in this paper are the parts of Mr. Minsu Park's Master degree Thesis. Hyunsung Kim is the corresponding author. This work was supported by Basic Science Research program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Li, M., Gu, W., Chen, W., He, Y., Wu, Y. and Zhang, Y. (2018) Smart Home: Architecture, Technologies and Systems. *Procedia Computer Science*, **131**, 393-400. https://doi.org/10.1016/j.procs.2018.04.219

[2] Marikyan, B., Papagiannidis, S. and Alamanos, E. (2019) A Systematic Review of the Smart Home Literature: A User Perspective. *Technological Forecasting and Social Change*, **138**, 139-154. https://doi.org/10.1016/j.techfore.2018.08.015

[3] Filho, G.P.R., Villas, L.A., Goncalves, V.P., Pessin, G., Loureiro, A.A.F. and Ueyama, J. (2019) Energy-Efficient Smart Home Systems: Infrastructure and Decision-Making Process. *Internet of Things*, **5**, 153-167. https://doi.org/10.1016/j.iot.2018.12.004

[4] Mohankumar, P., Ajayan, J., Yasodharan, R., Devendran, P. and Sambasivam, R.

(2019) A Review of Micromachined Sensors for Automotive Applications. *Measurement*, **140**, 305-322. https://doi.org/10.1016/j.measurement.2019.03.064

[5] Hou, J., Qu, L. and Shi, W. (2019) A Survey on Internet of Things Security from Data Perspectives. *Computer Networks*, **418**, 295-306. https://doi.org/10.1016/j.comnet.2018.11.026

[6] Cheng, J. and Kunz, T. (2009) A Survey on Smart Home Networking. Technical Report SCE-09-10, Carleton University, Ottawa.

[7] Nyirenda-Jere, T. and Biru, T. (2015) Internet Development and Internet Governance in Africa. Internet Society, Reston, 1-44.

[8] Penar, P. (2016) What Lies behind Africa's Lack of Access and Unreliable Power Supplies. The Conversation. https://theconversation.com/what-lies-behind-africas-lack-of-access-and-unreliable-power-supplies-56521

[9] Frontier Economics (2008) Taxation and the Growth of Mobile Services in Sub-Saharan Arica. GSMA. http://bit.ly/1Pk9rVc

[10] Gondwe, G. (2013) Internet VAT Bites Consumers. Biztech Africa. http://bit.ly/1Zim7Ai

[11] Freedom House (2015) Malawi Freedom on the Net. http://freedomhouse.org/report/freedom-net/2015/malawi

[12] Mambo, M., Usuda, K. and Okamoto, E. (1995) Proxy Signatures. *Proceedings of the* 1995 *Symposium on Cryptography and Information Security*, Inuyama, 24-27 January 1995, B1.11.1-17.

[13] Schneier, B. (1996) Applied Cryptography. John Wiley & Sons, Hoboken.

[14] Wikipedia. Elliptic-Curve Diffie-Hellman. http://en.wikipedia.org/wiki/Elliptic_curve_Diffie-Hellman

[15] Gomez, C. and Paradells, J. (2010) Wireless Home Automation Networks: A Survey of Architectures and Technologies. *IEEE Communications Magazine*, **48**, 92-101. https://doi.org/10.1109/MCOM.2010.5473869

[16] Chen, D. and Wabg, M. (2006) A Home Security ZigBee Network for Remote Monitoring Application. *Proceedings of IET International Conference on Wireless, Mobile, and Multimedia Networks*, Hangzhou, 6-9 November 2006, 1-4. https://doi.org/10.1049/cp:20061246

[17] Patil, M. and Reddy, S.R.N. (2013) Design and Implementation of Home/Office Automation System Based on Wireless Technologies. *International Journal of Computer Application*, **69**, 19-22. https://doi.org/10.5120/13745-1504

[18] Narayanan, V.S. and Gayathri, S. (2013) Design of Wireless Home Automation and Security System Using Pic Microcontroller. *International Journal of Computer Applications in Engineering Sciences*, **3**, 135-140.

[19] Park, W.C. and Yoon, M.H. (2006) The Implementation of indoor Location System to Control ZigBee Home Network. *Proceedings of International Joint Conference SICR-ICASE*, Busan, 18-21 October 2006, 2158-2161. https://doi.org/10.1109/SICE.2006.315641

[20] Kawamoto, R., Emon, T., Sakata, S. and Youasa, K. (2007) Energy Efficient Sensor Control Scheme for Home Networks Based on DLNA-ZigBee Gateway Architecture. *Proceedings of the First International Global Information Infrastructure Symposium*, Marrakech, 2-6 July 2007, 73-79. https://doi.org/10.1109/GIIS.2007.4404170

[21] Zhang, S., Xu, D., Jiang, Y. and Wang, R. (2007) Realization of Home Remote Con-

trol Networks Based on ZigBee. *Proceedings of the* 8*th International Conference on Electronic Measurements and Instrumentations*, Xi'an, 16-18 August 2007, 4-344-4-348. https://doi.org/10.1109/ICEMI.2007.4351154

[22] Hou, J., Dong, W.C., Yuan, Z. and Tan, J. (2008) Research of Intelligent Home Security Surveillance System Based on ZigBee. *Proceedings of the Initial Symposium on Intelligent Information Technology Application Workshop*, Shanghai, 21-22 December 2008, 554-557. https://doi.org/10.1109/IITA.Workshops.2008.223

[23] Wu, J. and Qin, H. (2008) The Design of Wireless Intelligent Home System Based on ZigBee. In: *Proceedings of the* 11*th IEEE International Conference on Communication Technology*, IEEE, Piscataway, 73-76. https://doi.org/10.1109/ICRIS.2016.35

[24] Zhang, C., Zhang, M., Su, Y.S. and Wang, W. (2012) Smart Home Design Based on ZigBee Wireless Sensor Network. *Proceedings of the* 7*th International ICST Conference on Communications and Networking*, Kunming, 8-10 August 2012, 463-466. https://doi.org/10.1109/ChinaCom.2012.6417527

[25] Chang, J.Y., Yuan, T., Hung, M.H. and Chang, Y.W. (2007) A ZigBee Based Power Monitoring System with Direct Load Control Capabilities. In: *Proceedings of IEEE International Conference on Networking, Sensing, and Control*, IEEE, Piscataway, 895-900. https://doi.org/10.1109/ICNSC.2007.372900

[26] Bai, Y.W. and Hang, C.H. (2007) Remote Power ON/OFF Control and Current Measurement for Home Electric Outlets Based on a Low-Power Embedded Board and ZigBee Communication. In: *Proceedings of IEEE International Symposium on Consumer Electronics*, IEEE, Piscataway, 1-4. https://doi.org/10.1109/ISCE.2008.4559539

[27] Byun, J.S., Jeon, B., Noh, J. and Kim, Y. (2012) An Intelligent Self-Adjusting Sensor for Smart Home Services Based on ZigBee Communication. *IEEE Transaction on Consumer Electronics*, **58**, 799-802. https://doi.org/10.1109/TCE.2012.6311320

[28] Shih, C. and Liang, B.C. (2012) A Model Driven Software Framework for ZigBee Based Energy Saving Systems. *Proceedings of the* 3rd *International Conference on Intelligent Systems, modeling and Simulation*, Kota Kinabalu, 8-10 February 2012, 487-492. https://doi.org/10.1109/ISMS.2012.62

[29] Deepak, K., Bavisker, J., Makwana, R. and Niraj, P. (2013) An Intelligent Self-Adjusting Sensor for Smart Home Services Based on ZigBee Communication. *Proceedings of the International Conference on Advances in Computing, Communications, and Informatics*, Mysore, 22-25 August 2013, 1779-1784.

[30] Zhu, J., Gao, X., Yang, Y., Li, H., Ai, Z. and Cui, X. (2010) Developing a Voice Control System for ZigBee Based Home Automation. In: *Proceedings of IEEE International Conference on Network Infrastructure and Digital Content*, IEEE, Piscataway, 7737-7741. https://doi.org/10.1109/ICNIDC.2010.5657880

[31] AES Encryption. https://aesencryption.net

[32] Tasi, J.L., Lo, N.W. and Wu, T.C. (2012) Secure Delegation-Based Authentication Protocol for Wireless Roaming Service. *IEEE Communications Letters*, **16**, 1100-1102. https://doi.org/10.1109/LCOMM.2012.052112.120525

[33] Hummen, R., Shafagh, H., Raza, S., Voig, T. and Wehrle, K. (2014) Delegation-Based Authentication and Authorization for the IP-Based Internet of Things. *Proceedings of Eleventh Annual IEEE International Conference*, Singapore, 30 June-3 July 2014. https://doi.org/10.1109/SAHCN.2014.6990364

[34] Lee, C.C., Chang, R.X., Chen, T.Y. and Chen, L.A. (2012) An Improved Delega-

tion-Based Authentication Protocol for PCSs. *Information Technology and Control*, **41**, 258-267. https://doi.org/10.5755/j01.itc.41.3.857

[35] Burrow, M., Abadi, M. and Needham, R. (1990) A Logic of Authentication. *ACM Transactions on Computer Systems*, **8**, 18-36. https://doi.org/10.1145/77648.77649

Appendix: Security Analysis

Especially, the security and privacy module will be evaluated by a formal well known security and privacy verification logic using Burrows, Abadi and Needham (BAN) logic [35]. Formal security analysis of the proposed delegation based user authentication and key agreement is verified with the help of BAN logic [35]. The formal analysis of a network security protocol using BAN logic involves following steps.

- Converting original protocol statements to their idealized form.
- Determining the assumptions about the initial state of the system.
- Representation of the state of the system after executing each statement as logical assertions by attaching logical formulas to each statement.
- Application of logical postulates to assumptions and assertions.

The following notations are used in formal security analysis using the BAN logic:

- $Q \mid\equiv X$: Principal Q believes the statement X.
- #(X): Formula X is fresh.
- $Q \mid\Rightarrow X$: Principal Q has jurisdiction over the statement X.
- $\mid \overset{K}{\rightarrow} Q$: Principal Q has a public key K.
- $Q \lhd X$: Principal Q sees the statement X.
- $Q \mid\sim X$: Principal Q once said the statement X.
- (X, Y): Formula X or Y is one part of the formula (X, Y).
- $\langle P \rangle_Q$: Formula P combined with the formula Q.
- $Q \overset{SK}{\leftrightarrow} R$: Principal Q and R may use the shared session key, SK to communicate among each other. The session key SK is good, in that it will never be discovered by any principal except Q and R.

In addition, the following four BAN logic rules are used to prove that the proposed delegation based user authentication and key agreement provides a secure mutual authentication among MS, CS and HS.

Rule 1. **Message-meaning rule:** $\dfrac{R \mid\equiv R \overset{Y}{\leftrightarrow} S, R \lhd \langle X \rangle_Y}{R \mid\equiv S \mid\sim X}$.

Rule 2. **Nonce-verification rule:** $\dfrac{R \mid\equiv \#(X), R \mid\equiv S \mid\sim X}{R \mid\equiv S \mid\equiv X}$.

Rule 3. **Jurisdiction rule:** $\dfrac{R \mid\equiv S \mid\Rightarrow X, R \mid\equiv S \mid\equiv X}{R \mid\equiv X}$.

Rule 4. **Freshness-concatenation rule:** $\dfrac{R \mid\equiv \#(X)}{R \mid\equiv \#(X,Y)}$.

In order to show that the proposed delegation based user authentication and key agreement provides secure mutual authentication between among *MS*, *CS* and *HS*, we need to achieve the following goals.

Goal 1: $MS \mid\equiv \left(MS \overset{SK}{\leftrightarrow} CS \right)$.

Goal 2: $CS \mid\equiv \left(CS \overset{SK}{\leftrightarrow} MS \right)$.

Goal 3: $MS \mid\equiv CS \mid\equiv \left(CS \overset{SK}{\leftrightarrow} MS \right)$.

Goal 4: $CS \mid\equiv MS \mid\equiv \left(MS \overset{SK}{\leftrightarrow} CS \right)$.

Idealized from: The arrangement of the transmitted messages among *MS*, *CS* and *HS* in the proposed delegation based user authentication and key agreement to the idealized forms is as follows:

Message 1. $MS \to CS$: Login Request.

Message 2. $CS \to MS : n_2, ID_S$.

Message 3. $MS \to CS : \langle r_1 \rangle_t, \langle r_2 \rangle_{Ys}, \langle z \rangle_{Ys}, ID_H, ID_S$.

Message 4. $CS \to HS : \langle CT_1 \rangle K_{HS}, ID_H, ID_S$.

Message 5. $HS \to CS : \langle CT_3 \rangle K_{HS}, ID_H, ID_S$.

Message 6. $CS \to MS : \langle CT_2 \rangle_\sigma, ID_S$.

Assumptions: The following are the initial assumptions of the proposed delegation based user authentication and key agreement:

A1: $MS \mid\equiv \#(t, n_2)$.

A2: $CS \mid\equiv \#(n_1)$.

A3: $HS \mid\equiv \#(n_3)$.

A4: $MS \mid\equiv \left(MS \overset{(K,\sigma)}{\leftrightarrow} HS \right)$.

A5: $HS \mid\equiv \left(HS \overset{(K,\sigma)}{\leftrightarrow} MS \right)$.

A6: $MS \mid\equiv \overset{Y_s}{\to} CS$.

A7: $CS \mid\equiv \left(CS \overset{K_{HS}}{\leftrightarrow} HS \right)$.

A8: $HS \mid\equiv \left(HS \overset{K_{HS}}{\leftrightarrow} CS \right)$.

A9: $MS \mid\equiv CS \mid\Rightarrow MS \overset{SK}{\leftrightarrow} CS$.

A10: $CS \mid\equiv MS \mid\Rightarrow CS \overset{SK}{\leftrightarrow} MS$.

Proof:

In the following, we prove the test goals in order to show the secure authentication and key agreement using the BAN logic rules and the assumptions.

Based on Message 2, we could derive:

Step 1. $MS \lhd n_2, ID_S$

According to assumption A2 and the message meaning rule, we could get:

Step 2. $MS \mid\equiv CS \mid\sim (n_2, ID_S)$

According to assumption A1 and the freshness concatenation rule, we could get:

Step 3. $MS \mid\equiv \#(n_2, ID_S)$

According to Step 2, Step 3 and the nonce verification rule, we could get:

Step 4. $MS \mid\equiv CS \mid\equiv (n_2, ID_S)$

Based on message 3, we could derive:

Step 5. $CS \lhd \langle r_1 \rangle_t, \langle r_2 \rangle_{Ys}, \langle z \rangle_{Ys}, ID_H, ID_S$

According to the message meaning rule, we could get:

Step 6. $CS \mid\equiv MS \mid\sim \left(\langle r_1 \rangle t, \langle r_2 \rangle_{Ys}, \langle z \rangle_{Ys}, ID_H, ID_S \right)$

According to assumption A1 and the freshness concatenation rule, we could get:

Step 7. $CS \mid\equiv \#\left(\langle r_1 \rangle_t, \langle r_2 \rangle_{Ys}, \langle z \rangle_{Ys}, ID_H, ID_S \right)$

According to Step 6, Step 7 and the nonce verification rule, we could get:

Step 8. $CS \mid\equiv MS \mid\equiv \left(\langle r_1 \rangle_t, \langle r_2 \rangle_{Ys}, \langle z \rangle_{Ys}, ID_H, ID_S \right)$

According to Step 8, assumption A6 and the believe rule, we could get:

Step 9. $CS \mid\equiv MS \equiv\mid\!\xrightarrow{Y_s} CS$

Based on Message 4, we could derive:

Step 10. $HS \lhd \langle CT_1 \rangle K_{HS}, ID_H, ID_S$

According to assumptions A5 and A8 and the message meaning rule, we could get:

Step 11. $HS \mid\equiv CS \mid\sim \left(\langle CT_1 \rangle K_{HS}, ID_H, ID_S \right)$

According to assumption A1 and the freshness concatenation rule, we could get:

Step 12. $CS \mid\equiv \#\left(\langle CT_1 \rangle K_{HS}, ID_H, ID_S \right)$

According to step 11, Step 12 and the nonce verification rule, we could get:

Step 13. $CS \mid\equiv HS \mid\equiv \left(\langle CT_1 \rangle KH_S, ID_H, ID_S \right)$

According to Step 13, assumption A7 and the believe rule, we could get:

Based on Message 5, we could derive:

Step 14. $CS \lhd \langle CT_3 \rangle K_{HS}, ID_H, ID_S$

According to assumptions A7 and the message meaning rule, we could get:

Step 15. $HS \mid\equiv CS \mid\sim \left(\langle CT_3 \rangle K_{HS}, ID_H, ID_S \right)$

According to assumption A3 and the freshness concatenation rule, we could get:

Step 16. $HS \mid\equiv \#\left(\langle CT_3 \rangle K_{HS}, ID_H, ID_S \right)$

According to Step 15, Step 16 and the nonce verification rule, we could get:

Step 17. $CS \mid\equiv HS \mid\equiv \left(\langle CT_3 \rangle K_{HS}, ID_H, ID_S \right)$

According to Step 17, assumption A8 and the believe rule, we could get:

Step 18. $CS \mid\equiv HS \mid\equiv \left(HS \overset{K_{HS}}{\leftrightarrow} CS \right)$

According to Step 17, assumption A8 and the believe rule, we could get:

Step 19. $CS \mid\equiv \left(CS \overset{SK}{\leftrightarrow} MS \right)$ **(Goal 2)**

Based on Message 6, we could derive:

Step 20. $MS \lhd \langle CT_2 \rangle_\sigma, ID_S$

According to assumption A4 and the message meaning rule, we could get:

Step 21. $MS \mid\equiv CS \mid\sim \left(\langle CT_2 \rangle_\sigma, ID_S \right)$

According to assumption A1 and the freshness concatenation rule, we could get:

Step 22. $MS \mid\equiv \#\left(\langle CT_2 \rangle_\sigma, ID_S \right)$

According to Step 21, Step 22 and the nonce verification rule, we could get:

Step 23. $MS \mid\equiv CS \mid\equiv \left(\left\langle CT_2 \right\rangle_{\sigma}, ID_S\right)$

According to Step 23, assumption A4 and the believe rule, we could get:

Step 24. $MS \mid\equiv CS \mid\equiv \left(CS \overset{SK}{\leftrightarrow} MS\right)$ **(Goal 3)**

According to assumption A9 and the jurisdiction rule, we could get:

Step 25. $MS \mid\equiv \left(MS \overset{SK}{\leftrightarrow} CS\right)$ **(Goal 1)**

According to Step 24, assumption A10 and the jurisdiction rule, we could get:

Step 26. $CS \mid\equiv MS \mid\equiv \left(MS \overset{SK}{\leftrightarrow} CS\right)$.