Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2016) 24: 3652 – 3663
© TÜBİTAK
doi:10.3906/elk-1407-47

Wireless sensor network-based extension to KNX home automation system

Ahmet Burak GÖKBAYRAK[1], **Sermin KILIVAN**[2], **Semavi AKIN**[2], **Anıl ÇELEBİ**[3], **Oğuzhan URHAN**[1,*]

[1]Kocaeli University Laboratory of Embedded and Vision Systems (KULE), Department of Electronics and Telecommunications Engineering, Kocaeli University, Umuttepe Campus, Kocaeli, Turkey

[2]Viko by Panasonic, R&D Center, Sancaktepe, İstanbul, Turkey

[3]Department of Electronics and Telecommunications Engineering, Kocaeli University, Umuttepe Campus, Kocaeli, Turkey

Received: 07.07.2014 • **Accepted/Published Online:** 26.05.2015 • **Final Version:** 20.06.2016

Abstract: This paper presents a seamless wireless extension approach to a KNX-based home automation system. The system consists of gateway and switch units specifically designed for this purpose. The gateway acts as the coordinator of the wireless network and a bridge between wireless and KNX networks. Switch units can be operated by a power outlet or battery. With the proposed architecture, it is possible to extend functionality of the KNX to wireless nodes, which consume very low power when they are operated by battery. Experimental results show that a simple yet efficient wireless extension to the KNX system is possible by the proposed system, which also enables more than 5 years of continuous operation for battery-powered switch units.

Key words: Home automation, smart home, KNX, wireless sensor networks

1. Introduction

Technological developments make the smart home concept widespread all over the world. People nowadays would like to control basic functionalities such as lighting, heating, and cooling in their homes using touch-sensitive management devices. Wireless sensor networks (WSNs) provide an efficient infrastructure for wireless communication environments within the home. There are plenty of WSN applications that aim to achieve energy efficiency and a smart home environment at the same time [1–9].

A review of currently available options for home automation networks by taking plenty of properties such as network layer options, implementation size, market adoption, and security into consideration was presented in [1]. A power outlet module that is able to control different devices such as PIR (passive infrared sensor) detectors and lights was presented in [2]. Those modules are connected each other using the ZigBee interface and can be programmed using a base station that has Internet connectivity. A similar approach was employed in [3], where a ZigBee network was established among the devices located within the home and a Wi-Fi connection enabled remote control. Additionally, a remote control hardware for local users was also presented. It was shown in this work that the user commands in ZigBee network are executed in less than 1 s. A lighting control application using ZigBee was presented in [4]. This system employs ZigBee-enabled PIR and light sensors to adjust lighting conditions of the environment to save energy for the lighting applications. The control of the power outlet was carried out by using a ZigBee-based network approach in [5]. In this work, a central ZigBee

[*] Correspondence: urhano@kocaeli.edu.tr

controller processes commands received from an IR transmitter. Next, based on these commands, the ZigBee controller transmits control signals to ZigBee-enabled power outlet modules, which simply switch AC input to its output according to the control signals. In [6], it was shown that it can be possible to reduce expenses of consumers when a WSN-based approach is utilized for energy management. A power protection and monitoring system based on the ZigBee network was presented in [7]. The system has continuous energy monitoring and power switching capabilities. Furthermore, an additional GPRS interface allows users to control functionalities of the system. A ZigBee-based self-adjusting network architecture to alleviate problems originating from the fixed structure of existing WSNs was presented in [8]. It was shown that it can be possible to achieve up to 34% energy efficiency on sensor nodes. A lighting control system based on IEEE 802.15.4 was presented in [9], where a single battery-powered control unit consumes around 4 μ A on average in the case of extensive use. Lights are switched by a control unit according to the commands received from IEEE 802.15.4 enabled button modules.

Even though there are various efforts on the use of WSNs for home automation, there has been a standardization trend in the global home/building automation industry. The European Installation Bus Association, European Home Systems Association, and BatiBUS Club International, three of the major organizations in this area, established a partnership that is called the KNX Association in 1999 to develop a widespread standard for home automation. The standard was accepted as an international standard for home automation (ISO/IEC 14543 3) in 2006. Additionally, it has also been approved as a European (CENELEC EN50090 and CEN EN 13321-1 and 13321-2), Chinese (GB/T 20965), and US (ANSI/ASHRAE 135) standard.

KNX provides all necessary functions required for building automation. It provides an OSI-based communication environment for nodes connected to the KNX network. Its current market share in home automation systems is over 70% in Europe.

KNX allows different physical transmission mediums such as twisted pair (KNX.TP), power line (KNX.PL), radio frequency (KNX.RF), and Ethernet (KNXnet/IP), as described in [10]. KNX.TP is the most commonly used medium for KNX implementation where a serial differential connection is made to each node.

The wireless extension of KNX is possible using KNX.RF; however, it has various drawbacks such as lack of security and integrity of the messages [11]. Because of these problems, two wired KNX nodes are tunneled using an IEEE 802.15.4-based network where each KNX device has the IEEE 802.15.4 radio. In this approach, KNX packages are transmitted via IEEE 802.15.4 protocol in a wireless system. Similar security issues of KNX were investigated in [12], where 128-bit AES encryption was proposed as a solution to overcome these issues. The approach presented in [13] proposed a gateway between ZigBee and KNX networks where a direct translation approach including attribute, application, and address translation is adopted. This gateway aims to provide transparency between lower level functions of two networks, which increase the system and installation complexity. Additionally, limited battery power of wireless nodes was not taken into account in that work.

In this paper, we present a seamless integration approach for KNX and IEEE 802.15.4-based WSNs for an efficient home automation system. There are several important differences of the proposed approach compared to the existing methods in the literature. The proposed approach has a simple translation scheme compared to the method in [13]. We simply utilize a look-up table (LUT) to keep track of correspondence between KNX and WSN nodes. The wireless nodes in the proposed approach do not need to be operated by battery. It is also possible to operate the wireless nodes by power lines directly and thus they have their own internal relays. These relays can also be controlled by both the node itself or wired KNX devices thanks to the proposed approach presented in this paper. We also analyzed real-life power consumption performance of the batterypowered nodes and revealed that it might be possible to achieve 5+ years of continuous operation using a single coin (CR2032)-type battery. In the proposed approach 128-bit AES encryption is adopted for data transfer between the wireless nodes and thus secure communication is achieved. Experimental results show that the proposed seamless approach allows efficient and secure integration of KNX and WSNs.

2. System overview

The system proposed in this paper includes both IEEE 802.15.4-based wireless and KNX-based wired networks that are integrated via a system control unit (SCU) as shown in Figure 1. The wireless node can be a lighting/heating sensor or actuator where these devices are considered as 'end devices' according to the WSN concept. All of the communication in the wireless network is controlled by the 'Coordinator', which also establishes the network. The IEEE 802.15.4 standard specifies a physical layer and media access control (MAC) for low bit-rate wireless communication networks. Based on these specifications, there are plenty of different protocols available, such as ZigBee, 6LoWPAN, and Wireless HART (Highway Addressable Remote Transducer).

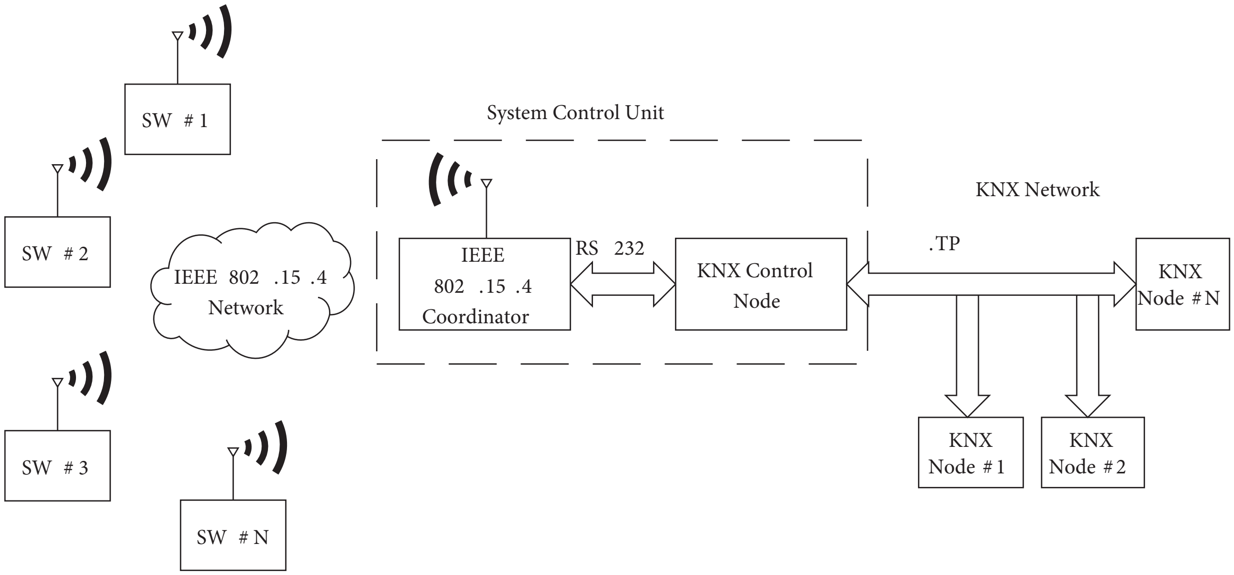

Figure 1. Overview of the proposed system.

In this work, an MCU (microcontroller unit) with wireless capability is utilized at the Coordinator and switch (SW) units. The MCU employs an IEEE 802.15.4-based royalty-free proprietary protocol from NXP called JenNet. This protocol allows tree, star, and linear network topologies and has a self-repairing function together with the support for up to 500 nodes. Additionally, JenNet enables network load balancing to avoid data congestion and it can reshape the network when it is necessary to reduce the network depth. Other important functions provided by JenNet are end-to-end message acknowledgement and efficient sleep mode support for extended battery life. Since this protocol adopts a listen-before-talk approach, it can coexist with available wireless technologies such as Bluetooth and WiFi.

In the proposed system, the SCU acts as a gateway between the JenNet and KNX networks by exchanging messages. A LUT is generated and stored in this unit to keep correspondence between KNX communication object addresses and MAC numbers of the SW nodes. This unit also has its own relays for wireless control of lighting.

It is possible to utilize two types of SW units in the proposed system. The first type of SW unit (Type-1) is directly powered by the available power lines in the walls and has its own relay units. This type of SW unit is required to control lighting modules remotely when it is possible to install a KNX control unit such as a KNX touch panel without additional KNX cabling installation into the SW units. When a button on the Type1 SW is pressed, the corresponding internal relay unit is instructed accordingly to turn on/off the lights. Additionally, this information is also transmitted to the Coordinator as an acknowledgement. It is also possible to control the relay on the Type-1 SWs using the KNX network.

A message received from a KNX node (for example from a KNX touch control panel) is initially transmitted to the KNX Control Node using the KNX.TP interface. This node transmits the data being transmitted to KNX group addresses to KNX communication objects according to datapoint types (DPT) using a table that is automatically generated by the KNX Engineering Tool Software (ETS). This table is stored in the KNX Control Node during the installation of the system into a building. Subsequently, KNX communication object address information is sent to the Coordinator, where it is interpreted. The Coordinator checks its LUT to find the MAC address of the corresponding Type-1 SW node and then transmits an appropriate command to related node/nodes. The LUT, which includes address translation between KNX and JenNet networks, is generated during installation time by making use of a specific easy-to-use learning mode.

An internal block diagram of the outlet-powered wireless nodes is shown in Figure 2. As shown in this figure, SW units contain a wireless MCU (microcontroller unit), four switches, and two relays. S1-S2 and S3-S4 pairs are used to control (turn on/off) the R1 and R2 relays, respectively. The required supply voltage for the whole circuit is directly generated from the outlet voltage by using the internal circuitry within the SW units. The details of this mode will be given in the next section.

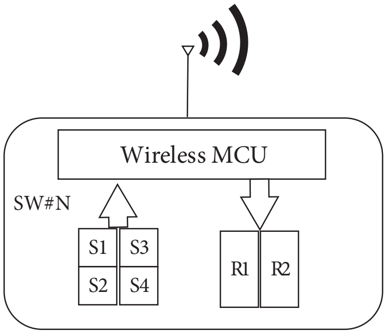

Figure 2. Internal block diagram of the outlet-powered wireless nodes.

The second type of SW (Type-2) unit is powered by batteries and does not contain internal relays. In this case, the wireless MCU in the wireless node transmits switch positions to the SCU. Then the Coordinator on the SCU arranges the relay conditions based on the data transmitted from the Type-2 SW units and finally acknowledges the KNX network. This kind of SW unit can be designed as a remote controller where it is not possible to utilize a power outlet to supply the device. Another real-life case is the restoration projects implemented in buildings where it may not be possible to install a power line into the wall where the SW will be installed.

The wireless MCU (JN5148) utilized in this system is manufactured by NXP and it is a low power SoC (System on Chip) module including a 32-bit CPU and 2.4-GHz radio. The reported current consumption data of JN5148 for receive and transmit operations are 18 mA and 15 mA, respectively, which enables coin-type battery-powered applications since that kind of batteries is only capable of providing maximum instantaneous current around 20 mA.

The JN5148 contains a hardware accelerator for secure communication between the wireless nodes, which is inevitable for home automation applications. The JenNet protocol executed on the wireless MCU enables three important security features of encryption, message integrity, and replay attack prevention. All the wireless nodes in the proposed system including the SCU and SWs employ 128-bit AES encryption for confidentiality of the messages. Since the AES is a symmetric-key algorithm, the keys in the communicating nodes must be exactly the same. Thus, a unique AES key is generated for each installation. This key is then programmed into the SCU and SWs in the field. Another important security feature provided by the JenNet is the message integrity control where intentional or accidental data modifications can be detected without using the AES key at the receiver. Replay attacks simply play back a valid and encrypted data transfer recorded previously during, for example, a SW position change. JenNet includes a frame counter into messages so that the receiver can detect how old the received message is. Thus, it becomes possible to eliminate replay attacks. These important security measures provided by the JN5148 and JenNet make the proposed WSN-based KNX extension secure. It is not clear whether this kind of security feature is utilized in the method presented in [13] or not.

When the gateway function provided in [13] is evaluated, it is concluded that the following issues may result in inefficient utilization. It was stated in [13] that each communication object in the KNX network is mapped to a ZigBee End-Point (EP). A single ZigBee node may contain more than one EP, i.e. different function. Thus, in this case, it is required to store the relation between KNX group addresses and EPs in ZigBee nodes. Since this table must be stored and utilized in ZigBee nodes, it will increase the complexity at the ZigBee nodes. Thus, this gateway is actually implemented in physically different parts, as also clearly stated in [13]. The table containing the group address and DPT relation in [13] is generated by KNX ETS. However, it is not clear how the group address/EP conversion table is generated. It is not possible to generate this table using ETS and, thus, this configuration needs to be carried out manually, which make installation of the system complex and error-prone. It might be possible to utilize a single EP for each ZigBee node to eliminate these problems. However, in this case, the number of ZigBee nodes must be increased, which is not efficient.

In the proposed approach, all the gateway operations are carried out by the SCU without the help of wireless SW nodes. We initially perform a conversion between KNX group addresses to the KNX communication object using the table automatically generated by the ETS. Next, a specific learning mode is designed to construct the relation between the KNX communication object address and MAC address of the corresponding SW nodes. As will be seen in the details given in the next section, this learning mode is quite simple and enables efficient installation of the system. Thus, in general, the proposed approach in this paper has significant advantages for the installation task in which there is no requirement of complex and error-prone operation, as in the approach presented in [13].

3. System implementation

As described in the previous sections, the proposed system consists of two main components that are the SCU and SW nodes. The SCU is implemented by two separate PCBs (printed circuit boards) where an IEEE 802.15.4 interface, relay, and power sections are combined in one board. The KNX interface is implemented on another small board. The connections between these boards are made via a flex cable. These two cards are optically isolated from each other to eliminate the possible spread of a problematic electrical signal originating from one part to another.

Pictures of the SCU developed in this work are shown in Figure 3. The board is powered by a 220-V AC power line and it generates required voltage levels for the card using an SMPS (switched-mode power supply)-based design. The board also contains four optional relay units, which can be driven from the KNX network, or Type-2 SW units. The status of these relays can be observed via four LEDs located on the cover of the box.

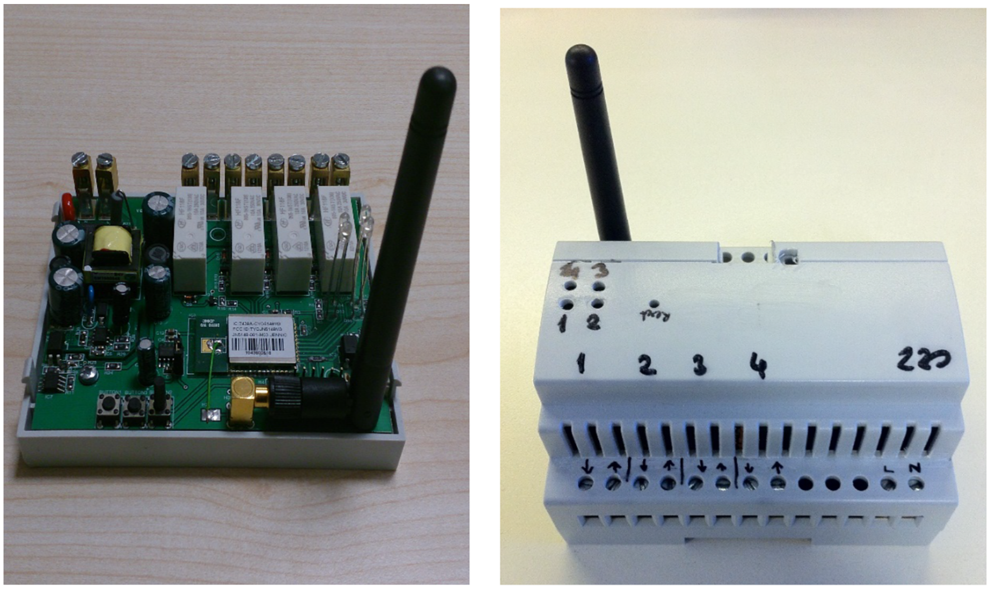

Figure 3. Pictures of IEEE 802.15.4 to KNX gateway unit.

The control of this SCU is handled by a 32-bit SoC module that has NXP's JN5148 32bit microcontroller and a 2.4-GHz ISM band radio in a single chip that enables the IEEE 802.15.4-based network environment. JN5148 has 128-kB RAM and 128-kB ROM space together with the 128-bit AES encryption accelerator. Additionally, there are plenty of onchip data and communication interfaces such as SPI, UARTs, ADC, DAC, comparators, and a temperature sensor.

It is also possible to run the ZigBee protocol on this SoC module. However, as described in the previous section, JenNet is preferred since it is a free-of-charge proprietary protocol based on IEEE 802.15.4. This protocol has a network recovery property similar to ZigBee but it has lower development complexity. Another important advantage of this proprietary protocol is that it supports up to 500 nodes within a single network, which is enough for the home automation application targeted in this paper.

Pictures of a Type-1 SW unit that includes two relays are given in Figure 4. As seen from this figure, the Type-1 SW module has a sandwich-like design with two PCBs stacked onto each other to fit into the limited available space in the case. After the assembly, the SW module is able to fit into the case designed for 2 × 2 switches. Type-2 SW units have a similar design approach where the PCB containing relays in Type1 SW units is replaced by a PCB that includes a coin-type battery as shown in Figure 5.

In the proposed design, Type-1 and Type-2 SW modules in the WSN are considered as an extension of the KNX network. Thus, a specific address from the KNX network is assigned to each SW module in the WSN. Normally, each node in the WSN has a unique MAC number, which allows other nodes to access and identify each other. The SCU developed in this work can be programmed via a serial interface to store the correspondence between KNX addresses and MAC numbers of the SW nodes into a LUT. This LUT can also be programmed during the installation using the learning mode. The LUT is established within the EEEPROM memory on the SCU.

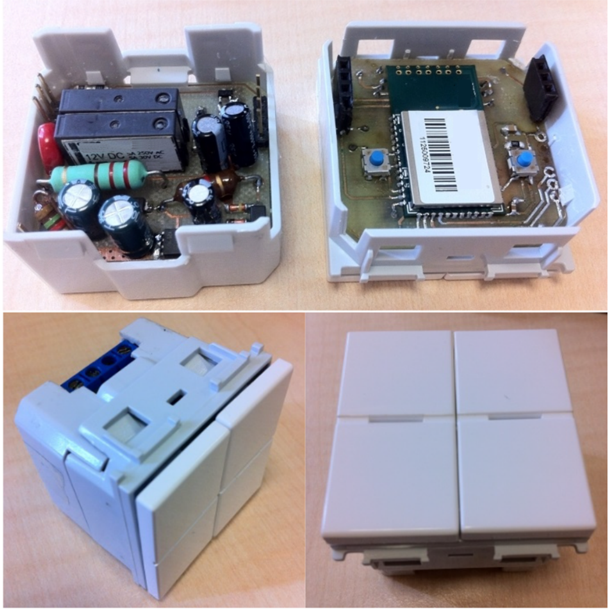

Figure 4. Pictures of Type-1 SW units.

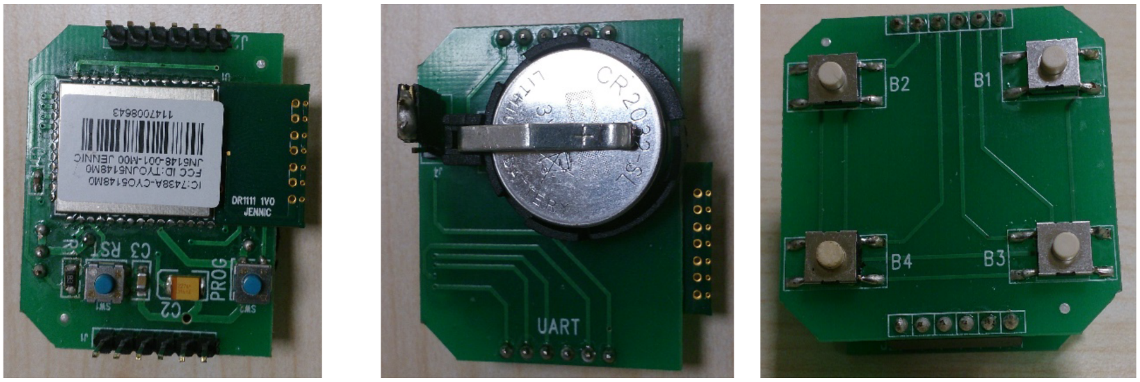

Figure 5. Pictures of Type-2 SW units.

We prefer to utilize a finite state machine (FSM) representation to illustrate the detailed operation of the modules in the proposed system. In this representation, the dashed arrow denotes the initial state of the FSM. The solid-line arrows in the FSM indicate the state transition. The event that triggers a transition is displayed above the horizontal line whereas the actions taken when the event occurs are displayed below this line. The $\wedge$ symbol is utilized below or above the horizontal line, respectively, to explicitly denote the lack of an action or event.

The detailed operation of the SCU is depicted using the FSM approach in Figure 6. As seen from this figure, before entering the initial 'Wait for packets' state, the SCU creates the network and initializes the serial port for KNX communications. Next, the device mode is set to 'operation' and a number of learned devices and the LUT generated in the previous learning stages are loaded from the nonvolatile memory. When a package from the WSN is received, required relay actions in the SCU are carried out if the SW is Type-2. Additionally, the information about this operation is transmitted to the KNX network. In the case of a Type-1 SW unit, since the relay operation is performed within the SW unit, only information about this operation is transmitted to the KNX network. When a package from the KNX network is received, the target address is investigated.

If the target is a Type-1 SW unit then the data are transmitted to corresponding node via WSN. Next, the Type-1 SW performs the relay operation. If the target is the SCU itself, then the relay positions in the SCU are adjusted. These operations carried out in the SCU are required for the gateway function of the device. Another important function of the SCU is to learn new SW units and forget these devices when required. In Figure 6, only the learning phase is shown to keep the FSM simple. However, it is important to note that the forget mode works in exactly a similar way. A specific button on the SCU needs to be pressed for 5 s to enter the learning mode. Once the SCU is in learning mode, it controls the packets coming from the SW units. If the MAC address of the transmitter is not known, a new KNX node address is assigned to this device and the LUT is updated. Additionally, the number of SW devices kept in the SCU is increased. If the MAC address of the transmitter is already recorded in the SCU, this means that this button will be used to control more than one operation lighting module. Thus, the button record is updated accordingly. There are two different ways to exit from the learning mode. The first is to wait for a time-out. The second is to reach the end of a learning cycle by learning a button for each relay in the SCU or skipping some of them. The relay change button is used to skip the learning mode for the current relay and it is possible to learn 5 buttons for a given relay.

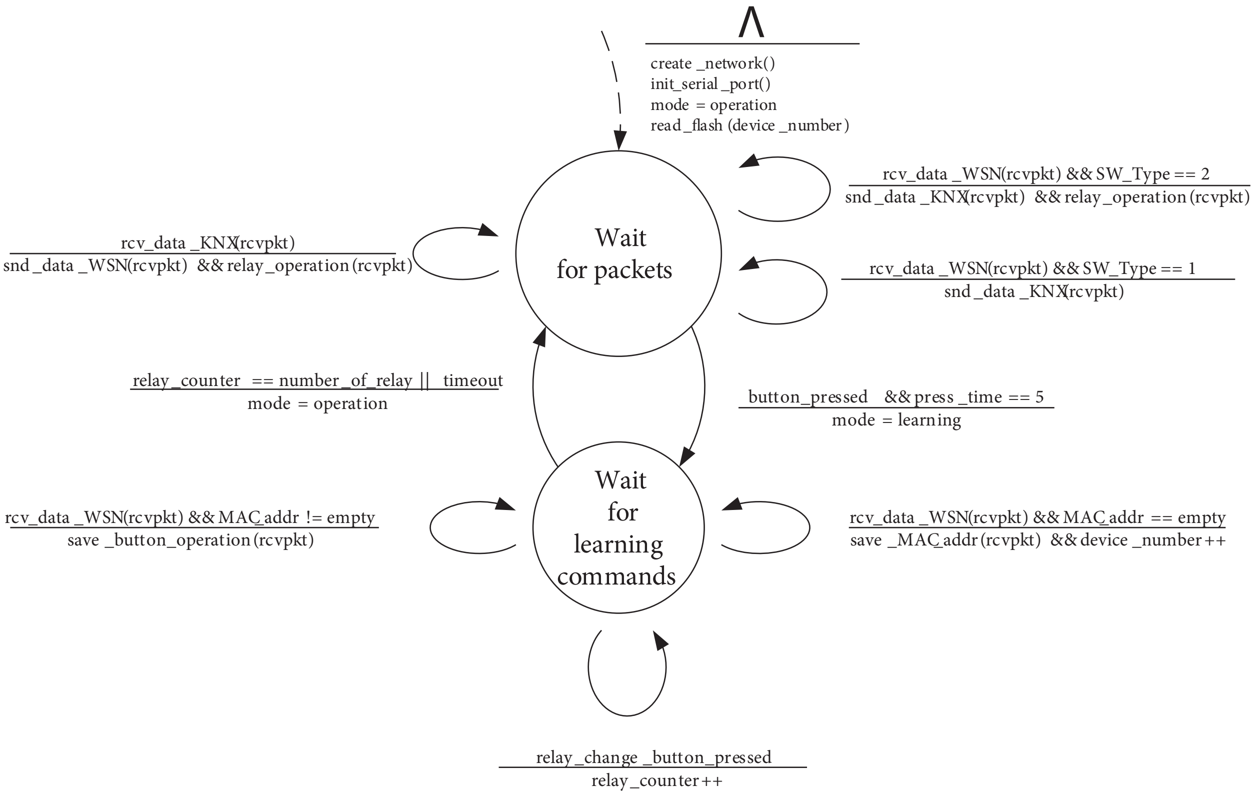
Λ
create _network()
init_serial _port()
mode = operation
read_flash (device _number)
rcv_data _WSN(rcvpkt) && SW_Type == 2
snd _data _KNX(rcvpkt) && relay_operation (rcvpkt)
rcv_data _KNX(rcvpkt)
snd _data _WSN(rcvpkt) && relay_operation (rcvpkt)
Wait for packets
rcv_data _WSN(rcvpkt) && SW_Type == 1
snd _data _KNX(rcvpkt)
relay_counter == number_of_relay || timeout
mode = operation
button_pressed && press _time == 5
mode = learning
Wait for learning commands
rcv_data _WSN(rcvpkt) && MAC_addr != empty
save _button_operation (rcvpkt)
rcv_data _WSN(rcvpkt) && MAC_addr == empty
save _MAC_addr (rcvpkt) && device _number++
relay_change _button_pressed
relay_counter++

Figure 6. FSM of the system control unit (SCU).

The detailed operation mode of SW units is shown in Figure 7. As seen from Figure 7a, Type-1 SW units are initially connected to the WSN. If a button in this SW unit type is pressed, internal relays are instructed to turn on/off the corresponding lights. Then the information about this operation is sent to the SCU for propagation of this operation to the KNX network. When a KNX network node such as a touch panel requires to control the relays in the Type1 SW units, this information is initially sent by the SCU to the corresponding Type1 SW unit via JenNet protocol. After the relays are switched to the requested position, an acknowledgement about this operation is sent to the KNX network via the WSN. Thus, other KNX nodes such as KNX control panels will be aware of the current situation of the lighting modules.

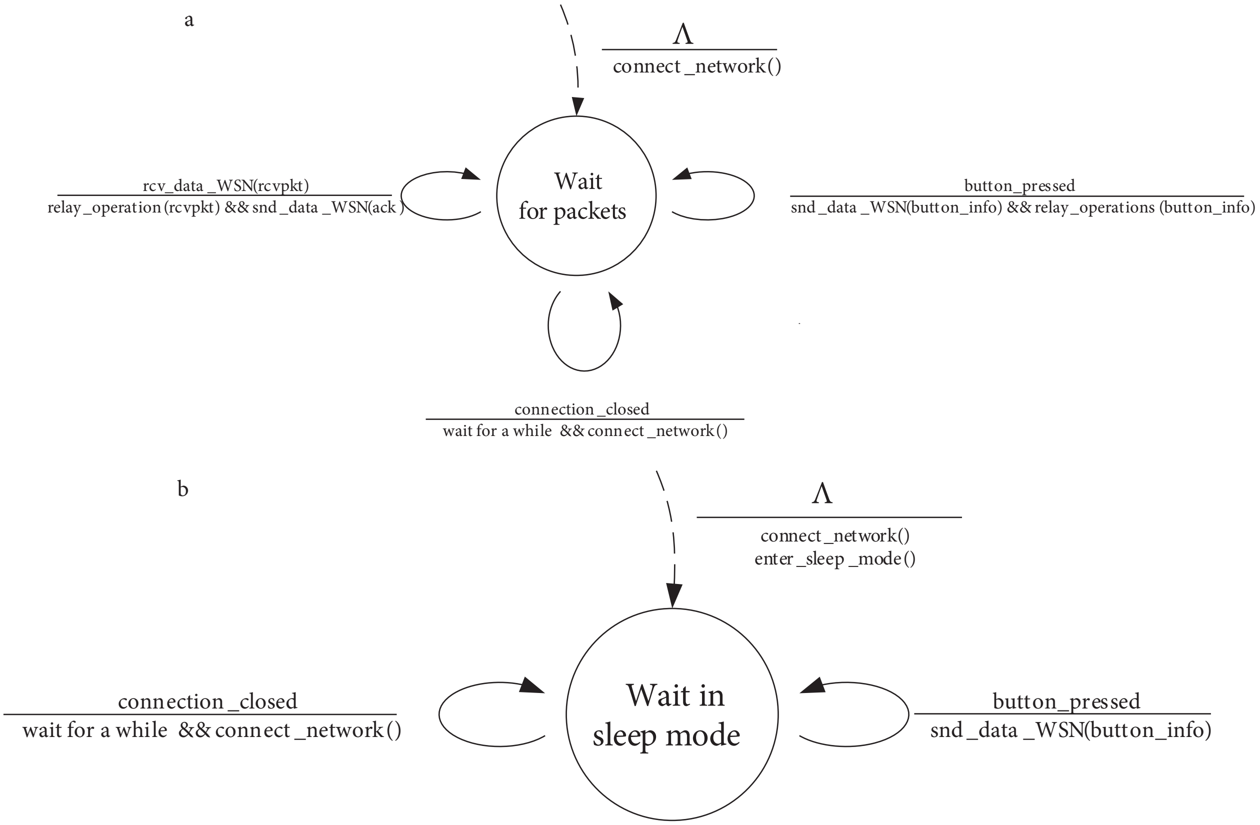
a
Λ
connect_network()
rcv_data_WSN(rcvpkt)
relay_operation (rcvpkt) && snd_data_WSN(ack)
Wait for packets
button_pressed
snd_data_WSN(button_info) && relay_operations (button_info)
connection_closed
wait for a while && connect_network()
b
Λ
connect_network()
enter_sleep_mode()
connection_closed
wait for a while && connect_network()
Wait in sleep mode
button_pressed
snd_data_WSN(button_info)

Figure 7. FSM of the SW units.

As seen from the FSM in Figure 7b, the Type-2 SW units enter into sleep mode once they are connected to the WSN to reduce the power consumption. Note that these nodes cannot receive data from the SCU since it is not required for the targeted application. The device will wake up when a button is pressed and the button code will be transmitted to the SCU via the WSN. Then the device will enter into sleep mode again until the next button is pressed. Thus, the device will be in sleep mode for most of the time of operation. When the button information is received by the SCU, the corresponding relays that are learned in the learning mode will be set accordingly.

4. Experimental results

The proposed system is tested by plugging the developed SCU and Type-1 and Type-2 SW units into a KNX.TP network. Several different types of commands (such as on/off) from a KNX node to the KNX.TP network are broadcasted. Our observations reveal that the proposed Type-1 and Type-2 modules are able to carry out the required functions correctly. The KNX network is observed by a KNX line data logger connected to a PC in order to analyze acknowledgments received from the SCU. Contents of these packages are also confirmed in long-term runs.

We measured the received signal strength indicator (RSSI) at the receiver side to analyze signal quality with respect to the distance. Figure 8 shows the RSSI versus distance plot obtained from our implementation.

The transmitted power is set to 0 dBm in this experiment, which is also the usual case in our system. As expected, the RSSI value continuously decreases as the distance between transmitter and receiver increases.

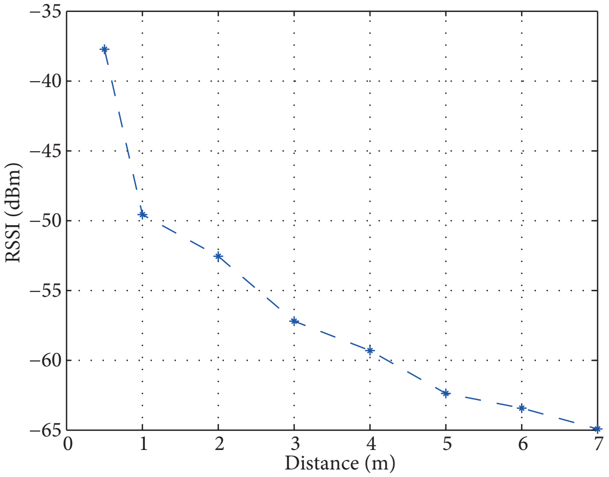

Figure 8. RSSI versus distance.

Additionally, we have investigated packet loss rate (PLR) with respect to the distance between the receiver and transmitter. Normally the wireless data transfer rate in our lighting application will be as low as several hundred packages in 1 h. Thus, we do not perform any additional throughput analysis. However, we set our system to transmit data at around 20 kbps data rate to observe packet losses in the case of continuous transmission. The Table shows the obtained PLR at different distances in our implementation for 100,000 packages at each distance. The experiment is conducted in an indoor environment so that there are reflections because of walls and furniture. As seen from this table, the PLR is quite low when the distance between the transmitter and receiver is less than 1 m. However, the PLR increases inevitably as the distance increases. These results are consistent with the RSSI values where PLR is increasing as the RSSI decreases, as expected.

Table. PLR versus distance.

Distance (m)	0.5	1	2	3	4	5	6	7
PLR (%)	2.0×10^{-5}	1.0×10^{-4}	2.3×10^{-4}	2.8×10^{-4}	6.1×10^{-4}	8.3×10^{-4}	8.5×10^{-4}	1.1×10^{-3}

Power consumption analysis for Type-2 SW units are also carried out in our work. As is widely known, the sleep mode in MCUs enable significantly lower power consumption. The deep sleep mode provided by JN5148 enables an even lower power consumption that is less than 1 μ A. However, since the WSN connection is closed in this mode it takes around 5 s to reconnect the WSN at the wake-up. Since this delay is not acceptable for home automation applications, we prefer to utilize the RAM retention sleep mode, which requires around 3.45 μ A current consumption. Type-2 SW units are mostly in this sleep mode in their typical operation. When a button is pressed the total active time of a Type2 SW unit is less than 30 ms. If an intensive usage such as 10 times per hour is considered, approximately 7 s of active time in a day is obtained. Thus, the overall current consumption is dominated by the sleep mode consumption.

A serial 7.5Ω resistor is connected between the battery and JN5148 to sense the current for power monitoring. Figure 9 shows the voltage observed on this resistor when the device is transmitting information via the IEEE 802.15.4 network and is in sleep mode. Average current consumption according to our measurement is 17 mA and 3.5 μ A for transmission and sleep modes, respectively. These measurements are consistent with the data provided by the wireless SoC manufacturer. The data transmission duration of SW units is less than 30 ms, which is small enough to enable real-time operation. These tests show that the Type2 (battery-powered) SW nodes consume less than 4.75 μ A on average for 10 times per hour usage, which enables 5+ years of battery life when a 250-mAh battery is utilized.

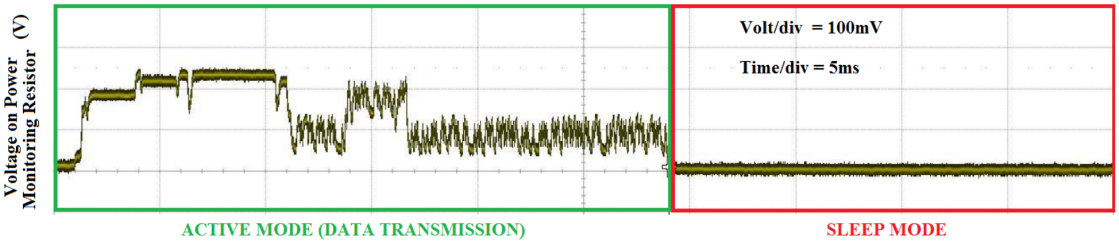

Figure 9. Power consumption measurements for active and sleep mode.

Since there is not any information about power consumption for wireless nodes in [13], it is not possible to directly compare it against our implementation. However, in [14], a detailed power consumption analysis of Bluetooth Low Energy (BLE), ZigBee, and ANT protocols for data transmission at 120-s intervals was carried out. The devices are put into sleep mode for the remaining time. Thus, it is quite similar to our experimental scenario. It was reported in [14] that the wireless nodes using BLE, ZigBee, and ANT requires 10.1 μ A, 15.7 μ A, and 28.2 μ A, respectively. When the same scenario is executed in our JenNet-based implementation, our wireless nodes consume around 8 μ A on average, which is significantly lower than the ZigBee that is the adopted approach in the gateway design presented in [13]. Note that this improvement is mainly achieved by the use of JenNet and JN5148.

5. Conclusions

In this paper, an efficient and seamless integration of KNX.TP and IEEE 802.15.4-based wireless networks is presented. Additionally, IEEE 802.15.4 enabled switch nodes are designed to show the effectiveness of the proposed gateway. The experiments carried out show that it is possible to control wireless SW units over the KNX network by making use of the designed gateway. It is also possible to inform the KNX network about button presses in a SW unit.

Acknowledgments

This work was supported by the Turkish Ministry of Science, Industry and Technology under Grant No. 1480.STZ.2012-2. The authors thank Y Öztürk and B Baykal for their technician level contributions in some PCB/code implementations and power measurements. The authors would also like to thank the anonymous reviewers and the editor for their valuable and insightful comments, which have improved the manuscript substantially.

References

[1] Gomez C, Paradells J. Wireless home automation networks: a survey of architectures and Technologies. IEEE Commun Mag 2010; 48: 92-101.

[2] Song G, Ding F, Zhang W, Song A. A wireless power outlet system for smart homes. IEEE T Consum Electr 2008; 54: 1688-1691.

[3] Gill K, Yang SH, Yao F, Lu X. A ZigBee-based home automation system. IEEE T Consum Electr 2009; 55: 422-430.

[4] Han DM, Lim JH. Smart home energy management system using IEEE 802.15.4 and ZigBee. IEEE T Consum Electr 2010; 56: 1403-1410.

[5] Han J, Choi CS, Lee I. More efficient home energy management system based on ZigBee communication and infrared remote controls. IEEE T Consum Electr 2011; 57: 85-89.

[6] Kantarci ME, Mouftah HT. Wireless sensor networks for cost-efficient residential energy management in the smart grid. IEEE T Smart Grid 2011; 2: 314-325.

[7] Huang LC, Chang HC, Chen CC, Kuo CC. A ZigBee-based monitoring and protection system for building electrical safety. Energy Buildings 2011; 43: 1418-1426.

[8] Byun J, Jeon B, Noh J, Kim Y, Park S. An intelligent self-adjusting sensor for smart home services based on ZigBee communications. IEEE T Consum Electr 2012; 58: 794-802.

[9] Baykal B, Hacihamzaoglu AT, Kilivan S, Urhan O, Erturk S. A low-power lighting control system using wireless sensor network approach. In: IEEE International Symposium on Consumer Electronics; 3–6 June 2013; Hsinchu, Taiwan. pp. 41-42.

[10] Merz H, Hnasemann T, Huber C. Building Automation: Communication Systems with EIB/KNX, LON, and BACnet. 1st ed. Berlin, Germany: Springer-Verlag Press, 2009.

[11] Reinisch C, Granzer W, Neugschwandtner G, Praus F, Kastner W. Wireless communication in KNX/EIB. In: KNX Scientific Conference; 9–10 November 2006; Vienna, Austria. pp. 1-15.

[12] Cavalieri S, Cutuli G. Implementing encryption and authentication in KNX using Diffie-Hellman and AES algorithms. In: IEEE International Conference on Industrial Electronics; 3–5 November 2009; Porto, Portugal. pp. 2459-2464.

[13] Lee WS, Hong SH. Implementation of a KNX-ZigBee gateway for home automation. In: IEEE International Symposium on Consumer Electronics; 25–28 May 2009; Kyoto, Japan. pp. 545-549.

[14] Dementyev A, Hodges S, Taylor S, Smith J. Power consumption analysis of Bluetooth low energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario. In: IEEE International Wireless Symposium; 14–18 April 2013; Beijing, Chania. pp. 1-4.