Home Network Security

Abhishek Anand
M.Tech Scholar in CSE
Dr.Varsha Namdeo
Associate Professor

Sarvepalli Radhakrishnan University,Bhopal
(Madhya Pradesh)India

Summary
We want to find ways to increase the security of home networks. To do this we first have to know: What needs to be protected within the home network? This question makes us think about which assets are present in a home network i.e. the elements within the home network that have a value. The idea is that if we can determine the most valuable assets within the home network, then we are able to prioritize which assets to protect first. But how can the value of an asset be determined? This is a difficult question because of the assets within home networks cannot always be expressed in a value of money. Some assets are for example personal files that may very valuable for someone but are worthless for another.

Key words:
Home Network, Home Appliance Control, Home Healthcare, Home Security

1. Introduction

With the recent rapid development of smart appliances, home networking technology becomes to attract public attention. Home network applications are categorized into data applications, AV (Audio/Video) applications, and "telemetry and control" applications [1]. Data applications have been already prevalent, which are implemented using TCP/IP and high bandwidth media (e.g., Ethernet [2] and IEEE 802.11g [3]). Besides, several protocols which work on Ethernet are proposed for AVapplications, for example, UPnP (Universal Plug and Play) [4], DLNA (Digital Living Network Alliance) [5] guidelines. Thus, AV applications are ready for widespread with these protocols.

In contrast, telemetry and control applications have a set of issues to be solved for diffuse, where primary issues are summarized as follows.

- Reduction of installation cost
- User-friendliness of setting and maintenance
- Ensured network security

It was difficult to meet these requirements by one of existing standards or a combination of them.

As a solution of low-rate wireless communication media, IEEE 802.15.4 [6] has been standardized [7]. However, 802.15.4 is mere one part of components which construct a home network, that is, an upper layer protocol (i.e. network protocol) is needed. In this paper, we propose a network protocol for home network aimed at telemetry and control applications. Evaluation system implementation and experimental results are also reported.

2. Characteristics of Home Network and Related Technologies

Generally, home network applications can be classified into three categories; data applications, AV (Audio/Video) applications, and "telemetry and control" applications. By interconnecting these application domains, wide range services are realized. However, it is difficult to employ unified protocol and media (e.g., combination of Ethernet and TCP/IP) for all applications domains, since each domain has different requirements. Therefore, each application domain would rather be constructed individually by appropriate protocol. In order to build a home network efficiently, gateways that connect different domains are indispensable.
In the following, functions of telemetry and control applications are explained, and then network architecture suitable for these functions is discussed.

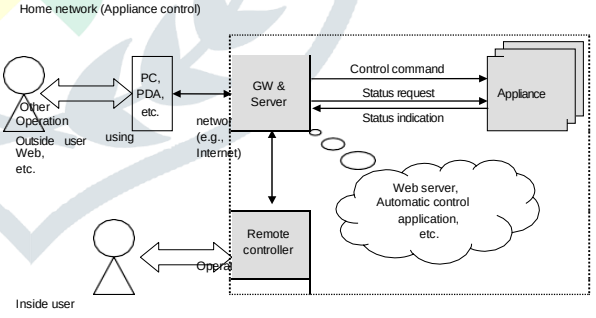


Fig. 1 Basic architecture of home network for appliance control.

First, appliance control application is explained, which controls appliances according to users' instructions and interconnects appliances. A basic structure of the network is shown in Fig. 1. Appliances and remote controllers are connected to a gateway node (GW). The number of

appliances in the network is considered to be several dozen at a maximum. The GW sends control commands to the appliances and inquires status of the appliances according to users' instructions through the remote controller or web and an automatic control application running on the GW. In this application, operations are always triggered by the commands from the GW. Appliances have only to await the command and response to it. Thus, there is no need for the controlled appliance to communicate with other appliances. The data size and frequency of communications between the GW and the appliances are several or several dozen bytes and one per several seconds at the maximum, respectively.

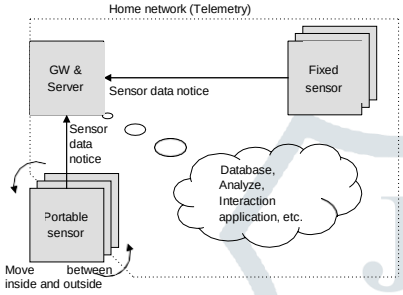


Fig. 2 Basic architecture of home network for telemetry.

Second, a telemetry application is explained. Fig. 2 shows a basic architecture of the telemetry application. The network consists of sensors and a GW. Data sensed at each sensor is aggregated into the GW, and a number of services, such as security and healthcare, are provided utilizing this data. Most of communications in the network are transmitting sensed data from sensors to the GW. Thus, there is also no need for a sensor to communicate with other sensors. Sensors are classified into two groups, fixed sensors (e.g., security sensors) and portable sensors (e.g., pedometer). Fixed sensors are always in the communication area, and data transmission to the GW is supposed to occur once in several minutes or dozens of minutes. The transmission data size at a time is usually from several bytes to several dozensbytes.

An example of portable sensors is a device worn by a user, such as a pedometer and an electrocardiogram recorder. The portable sensor stores sensed data into internal memory and sends data at once to the GW, because the sensor cannot communicate with the GW when the user is outside of communication area. Therefore, data transmission occurs at low frequency, and transmission data size is usually larger than that of fixed sensors. The transmission data size is sometimes over several dozens bytes, and it is considered that the maximum size is about several dozens kilobytes.

In summarize, a home network serving control and telemetry applications have features described below:

- The network consists of one GW and many device nodes (up to about 100). Device nodes are appliances, remote controllers, sensors, and so on.
- Basically, communications occur between the GW and one of device nodes, not between any pair of device nodes.
- Through Web UI and remote controllers, users operate appliances and get status of appliances.
- Usually, the communication data size is small (up to about 100 bytes). However, several sensors sometimes send large data (from 100 to 100,000 bytes).
- Devices can be classified into two group, fixed devices and battery-powered portable devices.

Furthermore, considering application, target users, and so on, a home network has to fulfill the following requirements.

- Low installation cost and running cost
- Easy setting and operation
- Communication data protection from interception

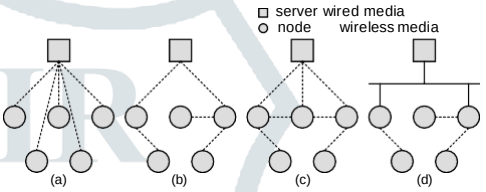


Fig. 3 Network topologies of wireless home network.

In the following, a network architecture (communication media, network topology, protocol, etc.) which meets these requirements is discussed.

A home network need not to have large bandwidth because of features described above, and thus transporting small data with low power consumption is of primary importance for home network. Wireless media is more suitable for constructing home network than wiredmedia, since the number of nodes is too many to connect nodes by wired media, and some nodes are even movable.

Star topology (Fig. 3a) with a central GW is simplest architecture. However, it is difficult for the GW to communicate directly with all device nodes, since device nodes are scattered around home and garden.

Therefore, home network architecture should be employ multi-hopping or backbone. The candidate architectures are shown in Fig. 3b, c, and d. Fig. 3b shows a tree topology with multi-hopping. Fig. 3c shows a mesh topology with multi-hopping. Fig. 3d shows an architecture which a part of network is constructed by wired media.

To implement the tree topology, a part of nodes has to support packet forwarding. The mesh topology needs a part of nodes to support mesh communication protocol. However there are no merits compared with the tree topology, since mesh routes are not required in a home network which uses only communications between the GW and one of device nodes. In Fig. 3d wired media is used as back-bone, and a part of nodes works as gateway

between wired network and wireless network. The gateway function in this architecture is basically the same as packet forwarding in Fig. 3b architecture. Comparing with Fig. 3b architecture, Fig. 3d is not suitable in terms of cost, which is caused by cable placing and more complex hardware. Thus, to implement home network supporting control and telemetry applications, wireless media and star or tree topology with a GW as root is suitable. Concrete protocol of home network is discussedbelow.

Following wireless media can be utilized for constructing home network.

- Bluetooth [8]
- Combination of IEEE 802.11 and an upper layer protocol
- Combination of IEEE 802.15.4 and an upper layer protocol

Bluetooth is a standard used for PC peripherals, headsets of cellular telephone, and so on. Bluetooth specifies from physical layer to application layer. Bluetooth network can construct a tree topology network called as scatternet. However scatternet has several limitations to cover entire home and garden. For example, a node, which works as parent node, has up to only seven children. Moreover, generally communication distance of Bluetooth node is only 10 meters.

IEEE 802.11 is widely used for PC LAN usually with TCP/IP as an upper layer protocol. Since 802.11 provides large bandwidth links, power consumption is too high for home network.

IEEE 802.15.4 is one of wireless communication standards for PAN (Personal Area Network) aiming at reduction of hardware cost and power consumption by lowering bandwidth. Since 802.15.4 provides only physical layer and MAC layer specifications, to construct a home network an upper layer protocol suitable for home network is required.

2.1. Network protocol suitable home network

There are two existing protocols, which can be considered for home network using 802.15.4; i.e. TCP/IP and ZigBee.

2.1.1. TCP/IP

IPv4 is one of the most popular network protocols that are used on the Internet and LAN. A home network with IPv4 allows seamless communication through the Internet.

However, according to home network characteristics, nodes except a gateway do not request seamless communications with any nodes outside home network. In addition to this, a home network using IPv4 has several problems. For example, the size of packet header is large, and IPv4 has no functions for ad hoc routing. To resolve these problems, several techniques and other protocols (e.g., DHCP [9], AODV [10], and IPSec [11]) are required. Therefore using IPv4 for a home network comes at a price. On the other hand, adoption of IPv6 with 802.15.4 for a home network and a sensor network is studied in IETF 6LoWPAN WG [12]. However the same problems as IPv4 also exist [13] and resolving them in WG may take a time.

2.1.2. ZigBee

ZigBee [14] is one of standards to implement wireless network using 802.15.4 as lower layer which is for a sensor network, a home network, building automation, and so on. For a home network, ZigBee provides HCL (Home Control Lighting) Profile. However, ZigBee suffers mainly from the following problems.

- Communications for re-connection and address resolving are caused by move of nodes since changing tree formation does not allow keeping the same address of node in the tree.
- ZigBee has no specification for secure node registration method.
- The maximum size of data which is transferred between application layers is about only 100 bytes. It is too small to transmit data stored in removable sensor node.

Therefore ZigBee also requires some extensions.

In brief, for a home network supporting appliance control and telemetry applications, wireless network using 802.15.4 which supports star or tree topology is suitable. However, a combination of 802.15.4 and conventional network protocols does not satisfy all requirements of home networks.

3. Design of Network Protocol

In accordance with above consideration, we designed a network protocol for home networks based on 802.15.4, which is outlined in Fig. 4.

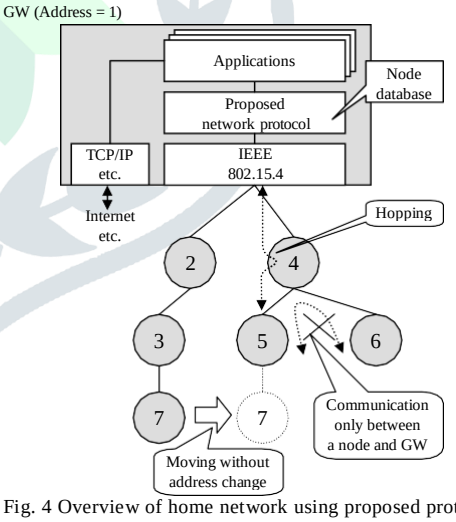


Fig. 4 Overview of home network using proposed protocol.

3.1. Header Format

As shown in Fig. 5, the frame size of a packet in IEEE 802.15.4 is small. Therefore, a compact header size of the

network layer is also desired. The header format of this protocol is shown in Fig. 6.

"Version" represents version of this protocol. "Sec" is 1 if the packet is encrypted. "Type" represents the packet type, which is set to 0 if the packet is data packet. Other 20 types of control packets are distinguished with "Type" field. "Packet ID" is used for distinguishing the packets. The other fields are explained in the following sections.

The header of a control packet does not include port number fields and fragment index, and consists of fields in only first 4 bytes of Fig. 6. The body of a control packet includes data for network controlling. As for a data packet, since most of data packets are not so large as to be needed for fragmentation, "FF" and "Fragment Index" are validated only for fragmentation data, which prevents meaningless increase of the header size for un-fragmented packets.

From the header format mentioned above, the header size of a data packet is 6 or 8 bytes. Compared with IPv4 header which is normally 20 bytes, the header size of a packet in this protocol is very small, which is achieved by specializing for home networks. Small header size can contribute to save transmission time and power consumption.

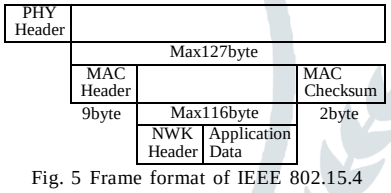
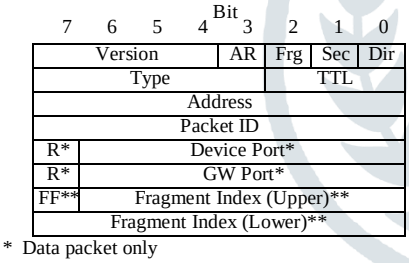


Fig. 5 Frame format of IEEE 802.15.4



* Data packet only

** Fragmented data packet only

AR : ACK Request
Frg : Fragment
Sec : Secure
Dir : Direction
TTL : Time To Live
R : Reserved
FF : Fragment Finish

Fig. 6 Header format of proposed protocol.

3.2. Topology

The proposed protocol employs tree topology as physical topology, where the root of a tree is the GW. Communications of application data occurs only between a device node and the GW, and does not occur between device nodes. Therefore, logical topology in this protocol is star topology.

The number of hops is controlled using "TTL" field. Since "TTL" field is 3-bit width, the maximum depth of the tree is 8, which is generally enough for covering in whole home. The number of children or descendants can be any value within the number of the network protocol address.

3.3. Services provided for application layer

In a home network, stream oriented communication is not crucial requirement. The proposed protocol only supports packet oriented communication, that is, applications communicate with each other by packets, not by stream. The packet size will be described in Section 3.9.

3.4. Management of Device Nodes

For security reason, a home network must be constructed by the devices that are registered by users, and unauthorized devices must be refused on a connection process. In the proposed protocol, the GW stores information about the registered device nodes and adds the information of a new device to the node information table on registration process. The details of device registration will be described in the next chapter.

3.5. Network Protocol Address

The proposed protocol employs 8-bit network protocol address, because the number of nodes in a home network hardly exceeds 100. The address of the GW is fixed number: 1, and the other addresses except for several peculiar addresses are assigned to device nodes by the GW on device registration. Therefore, a home network using the proposed protocol can accommodate up to about 250 device nodes.

Each device node stores assigned own address in nonvolatile memory. After registration, the address remains unchanged. Benefits of using a constant address are that the GW can easily identify a device node and need no communication for address resolution.

3.6. Routing

On transmitting or relaying packets, routing is necessary to determine the forwarding address. Since the proposed protocol employs star topology as logical topology, all packets are classified into upstream or downstream packets, and direction of each packet never change during relaying. "Dir" field in the header represents the packet direction. "Address" field indicates the address of the device node, which means the source node address in upstream and the destination node address in downstream, respectively. Upstream packets are relayed to a parent node of a relaying node and carried to the GW at the end. In contrast, downstream packets are relayed to a child node of the relaying node and it is required to determine which child

node the packet should be forwarded to. Thus, each node has a routing table. The routing table has only information of descendant nodes and is updated mainly when the node relays an upstream packet from a descendant node. Therefore, communications for management of routing table are very rarely requested.

3.7. Port Number

The GW and the devices often provide multiple application services. Therefore, the destination application on the destination node must be able to be distinguished by the source application. In home networks, the number of applications on a device node is generally less than several dozens, because of limited resources on the device nodes. Hence, this protocol employs a couple of 7-bit port numbers, "Device Port" and "GW Port", in order to identify the applications on the source node and the destination node.

3.8. Acknowledged Transmission

In wireless communications, packet losses often occur. This protocol employs ACK (Acknowledgement) packet for confirmation of packet arrival. When a data packet whose "AR" field in the header is marked is arrived, a destination node transmits an ACK packet to a source node. If the source node does not receive the ACK packet within a time-out period, the source node retransmits the data packet. The maximum number of retransmission is configurable at each node.

3.9. Packet Fragmentation

As shown in Fig. 5, the frame size of a packet in IEEE 802.15.4 is small. The maximum application data size in a packet is about 100 bytes. In transmission of small data such as sensor or device-controlling information, the frame size does not matter. However, there are applications which need large data transmission far more than 100 bytes. For example, a wearable sensor node stores sensor data when the user is outside of the network. In this case, a large amount of stored sensor data is transmitted when the node reconnect to the network.

In this protocol, a large packet, which is requested for transmission by an application, is fragmented. Fragmented packets are transmitted with IEEE 802.15.4 and reassembled by the network layer of the destination node. The transmissions are controlled using "Frg" field, "FF" field, and "Fragment Index" field. "Frg" is 1 if the packet is fragmented. "FF" indicates that the packet is last packet. "Fragment Index" indicates the packet number of fragmented packet. With this packet fragmentation, applications can transmit large packets without complicated process. The theoretical maximum packet size with this protocol is about 3 MB. The actual maximum packet size is configurable, and determined to suitthe desired function or the memory size of the destination node.

4. Security Function

Distinctive features of the proposed protocol are to support device authentication and message encryption as security function. To provide these functions, device registration is important. In device registration, the GW and the device share secret information which is known by only the GW and the device, and is used for authenticating a device and generating an encryption key.

This protocol specifies an easy-to-use device registration procedure which takes each device allocation of home networks in consideration.

4.1. Device Registration

In home networks, a device registration is needed for recognizing and managing device nodes by the GW and is also needed for sharing secret information between the GW and the device node. The restrictions of a device registration in home networks are as follows:

- User Interface (UI) of a device is usually restrictive.
- There are devices which can hardly move.

Since home appliances and sensors are restrictive on UI, it is impossible to input numbers and characters from them. Un-movable devices such as lightning equipments, which cannot communicate directly with the GW, have to process device registration with multi-hopcommunications.

Motivated by this, the proposed protocol employs a "registration proxy terminal" which is a dedicated movable node for proxy registration. Advanced remote controllers may provide a function of the registration proxy terminal.

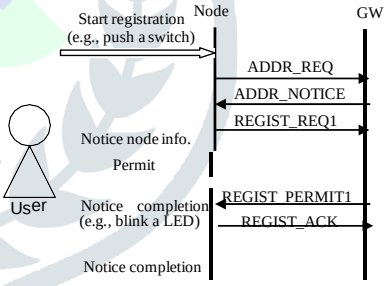


Fig. 7 Message sequence chart for direct registration.

This protocol provides two kinds of device registration processes: "direct registration" and "proxy registration."

In direct registration, a joiner device is brought near to the GW and communicates directly with GW during the registration. Fig. 7 shows a message sequence chart for direct registration, omitting processes about IEEE 802.15.4 such as a scan and an association. The sequence is started by a user's instruction. In an address request (ADDR_REQ) and an address notice (ADDR_NOTICE), the joiner device receives a temporary address from the GW. Then, the joiner device transmits the registration

request (REGIST_REQ1) that includes its information such as device type and model number. In reception of this request, GW displays this information through its UI and asks the user whether to permit the device registration. If permitted, the secret information is transmitted to the joiner device (REGIST_PERMIT1). The registration is completed by the reception of the registration ACK at the GW (REGIST_ACK).

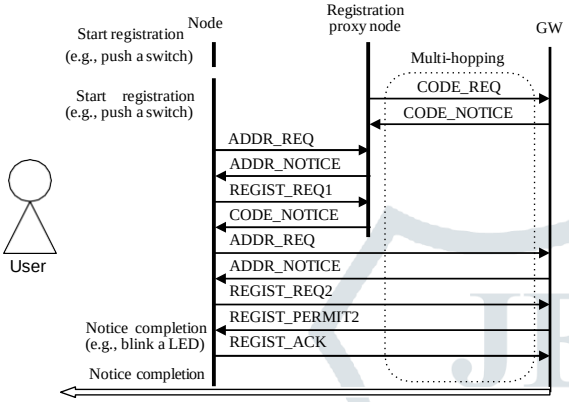


Fig. 8 Message sequence chart for proxy registration.

If it is impossible to bring the joiner device near to the GW, "proxy registration" can be executed. In this sequence, the joiner device is brought near to a "registration proxy terminal." Fig. 8 shows message sequence of this process. First, through the initial code request (CODE_REQ) and the initial code notice (CODE_NOTICE), the registration proxy terminal gets a random number called "initial code" from the GW. Since the registration proxy terminal, which is one of registered nodes, is already connected to the network and communications with the GW are encrypted, the initial code can be received securely in a multi-hop environment. Next, the registration proxy terminal starts the registration sequence against the joiner device. Until the registration request (REGIST_REQ1), the message sequence is the same as the sequence of "direct registration," except that the destination node is the registration proxy terminal instead of the GW. Then, the registration proxy terminal notifies the initial code to the joiner device. After getting the initial code, the joiner device creates a temporary connection with the GW via other device nodes. At this time, the joiner device is notified of a random number. Then, the joiner node send back hash sum calculated from the random number and the initial code in the registration request to the GW (REGIST_REQ2). If the hash sum is verified by the GW, the GW transmits the registration permit notice (REGIST_PERMIT2) which includes the secret information. The secret information is encrypted with the initial code as the encryption key so the secretinformation not to leak to forwarding nodes and unauthorized nodes. In addition, the initial code is checked for time-out. If the GW cannot receive the registration request in time-out period, the initial code become invalid and the registration process ends in failure.

Required user's operations to a joiner device during a registration are instructing to start the registration and confirming the completion of the registration. Thus, UIs on the joiner node can be implemented with very simple interfaces such as a push button and an LED. Therefore, the registration function can be implemented at low cost and be utilized without complicated operation.

The security strength of the authentication and the data encryption is determined by the probability of leaking the secret information. In both of the above two registration sequences, the secret information is notified to the registration node via radio waves. Since a joiner device can be near to the GW or a registration proxy terminal during registration, transmission power can be lowered in transmitting secret information. Low power transmission enables nodes closely located to the GW or the registration proxy terminal, i.e. usually only the joiner node, to receive the packet, and prevents distant nodes from intercepting messages. In a home network, there are many device nodes which can hardly move (e.g. lightning equipments and refrigerators). This protocol introduces the registration terminal so that the GW notifies the secret information even to the fixed devices, whilst it also achieves the same security strength and usability as the direct registration. However, if absolute security is need, secret information needs to be transmitted via dedicated wired or storage media.

4.2. Authentication and Encryption

When device nodes join to a network, the GW authenticates the node. After authentication, communications are protected by message encryption. In this protocol, the authentication and the encryption are processed based on the secret information that is informed from the GW to the node in the registration process.

First, we discuss the scope of the encryption. The effect and the computational cost depend on the layer to be encrypted. There are two ways of message encryption:

- Encrypting the application data and the header information of the network layer.
- Encrypting only the application data.

In the first case, the header information including device address can be also protected. However, in relaying packets, the forwarder nodes must decrypt and encrypt the header information in order to decide the route and to update TTL. As a result, the computational cost and delay at the forwarder nodes increase. Furthermore, in this method, the forwarder nodes must know the encryption key used by the source node, which causes an overhead in notification and management of the encryption key. Therefore, if the encryption of the header information is employed, it is impractical that each node uses a unique

encryption key. Thus, the same key should be used in the network.

In the latter case, since the header information is not encrypted, a forwarder node recognizes the destination node without decryption. Therefore, a forwarder node does not have to manage keys of descendants, which allows a device node to have an unique key.

To compare both methods, the first one requires high computational cost in relaying packets. In addition, sharing a key in a whole network has weakness against attacks from internal nodes. As for attacks from external nodes, it also decreases security strength due to protection depending on only one key. In contrast, the latter method does not causes additional computational cost in relaying packets including encrypted message and allows each node to use a unique key, whereas the header information is not protected.

Taking the above comparison into consideration, only the application data is encrypted in the proposed protocol. The encryption scheme is counter (CTR) mode [15] of 128-bit AES [16]. The encryption key is secret information which is generated in the device registration. The initial vectors (IV) are generated every connection, and are different between upstream anddownstream.

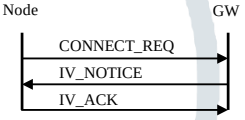


Fig. 9 Message sequence chart for authentication.

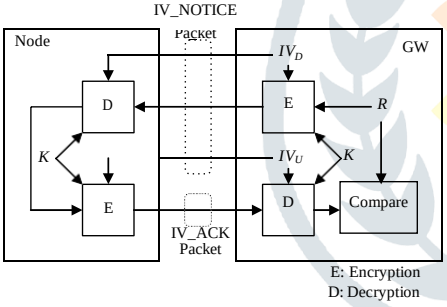


Fig. 10 Block diagram of authentication.

Next, we consider the authentication. A device node is authenticated when the node connects to a network, whilst initialization for message encryption is performed at the same time. The message sequence chart for the authentication and the block diagram of the authentication are shown in Fig. 9 and Fig. 10, respectively. An authentication starts by a connection request from a device node (CONNECT_REQ). On receipt of it, the GW generates IV_U (IV for upstream packets), IV_D (IV for downstream packets), and R (random number). Then, the GW encrypts R with K (encryption key) and IV_D and transmits the encrypted R, IV_D and IV_U to the device node (IV_NOTICE). The device node initializes her encryption module with K, IV_D and IV_U and decrypts R. After that, R is encrypted with K and IV_U and sent back to the GW (IV_ACK). Although both IV_NOTICE and IV_ACK include encrypted R, cipher texts of these messages differ since IVs used for upstream and downstream are different.

5. Implementation of Evaluation System

To evaluate the proposed protocol, we fabricated prototype communication adapters and implemented our protocol.

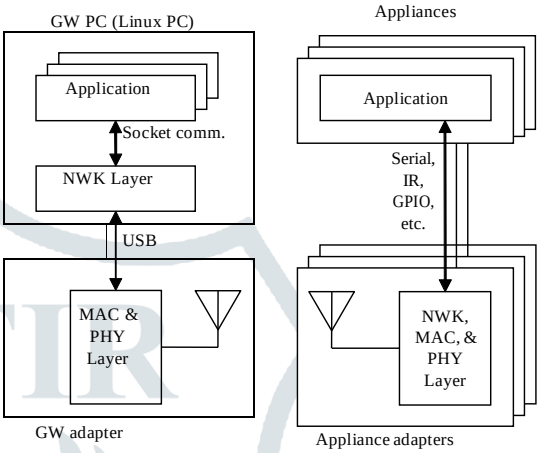


Fig. 11 Structure of evaluation system.

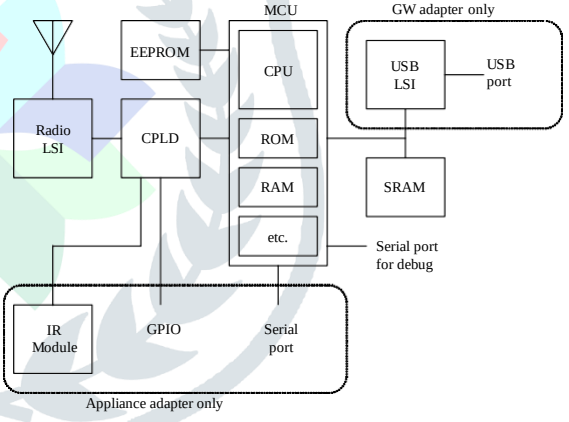


Fig. 12 Organization of communication adapter.

Fig. 11 shows structure of evaluation system, which comprises a GW set (a GW adapter and a GW PC) and multiple appliance sets (pairs of appliance adapters and appliances). The GW PC executes multiple application software and network layer software which handles packets according to the proposed protocol. The network layer software is connected to the GW adapter by a USB (Universal Serial Bus) and communicates with device nodes in a network via the GW adapter. 802.15.4 MAC and PHY are processed on MCU (Micro Control Unit) and RF LSI on the GW adapter. In contrast, an appliance adapter also processes the proposed protocol in addition to

802.15.4 MAC and PHY. Fig. 12 and Fig. 13 show the organization of the communication adapter and the photograph of the adapters, respectively. The GW adapter and the appliance adapter employ almost the same structure for simplicity and efficiency of designing, debugging, and experimenting. Thus, there is a room for downsizing, reducing the component cost, and improving power consumption. Main components of the adapters are summarized in Table 1.

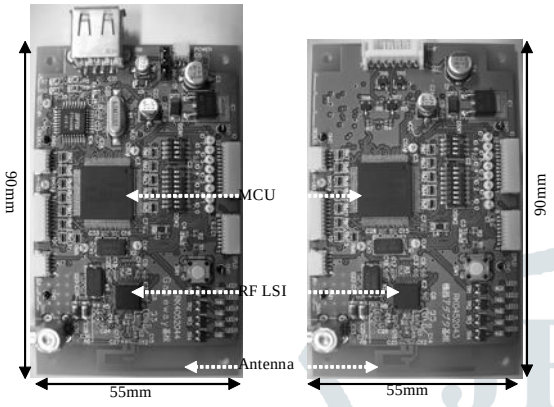


Fig. 13 GW adapter (a) and appliance adapter (b).

Table 1: Main components of communication adapter.

RF LSI	2.4 GHz IEEE 802.15.4 compliant[1]
MCU	general-purpose, 16-bit, 3.3 V, RAM 32 KB, ROM 384KB[2]
External SRAM	256 Kwords x 16 bits
External EEPROM	2 Kbits (connected by I2C)

The RF LSI performs PHY layer of 802.15.4. MCU's operate at the frequency of 25 MHz (GW adapters) or 22 MHz (appliance adapters), for which firmware is installed in built-in ROM. Data encryption is processed on the RF LSI, which reduces the load of MCU. Our prototype adapters have 512 KB external RAM, whilst required memory size depends on the application. Our protocol processing software uses 128 KB of SRAM. EEPROM (Electrically Erasable Programmable Read Only Memory) is used for a storage of permanent information (network protocol address, secret information, etc.). CPLD (Complex Programmable Logic Device) is used for implementation of combinational circuit which intermediates signal transmissions between the RF LSI and the MCU. In addition, the GW adapter has an USB port which is connected to the GW PC and is used for electric supply and communication with the software on the GW PC. Instead of the USB port, the appliance adapter has an I/O circuit which handles serial communication or infrared communication. In particular, communicating via infrared communication enables some kind of legacy devices which are controlled by IR remote controller to join a home network.

[1] Texas Instruments CC2420 [17]
[2] Renesas H8S/2329 [18]

6. Evaluation

In order to evaluate the proposed protocol, this section shows comparison between the proposed protocol and ZigBee and results of experiments using a prototype system.

6.1. Comparison with ZigBee

As described in Chapter 2, ZigBee is one of conventional protocols for home network using IEEE 802.15.4. Comparison between the proposed protocol and ZigBee is summarized in Table 2. The comparison is based on the assumption that ZigBee network uses tree topology, since HCL profile of ZigBee uses tree topology, while ZigBee supports several network topologies. Functionality of port number and arrival acknowledgement using ACK packet are also provided in ZigBee. Our proposed protocol has an advantage when large data is transmitted, since ZigBee does not provide packet fragmentation. A greatdifference is on network protocol address. In ZigBee network, addresses are 16bits number and depend on the node locations in tree. Since forwarding address is decided with the destination address and the address of the relaying node, packet routing on each node requires no routing table. Meanwhile applications have to resolve the address of the target node before transmission. Moreover, when a node disconnects with its parent node, not only the node but also all children nodes have to execute reconnect process. In proposed protocol, network protocol address does not change, which children nodes need no reconnection process.

Table 2 Comparison proposed protocol with ZigBee.

	Proposed protocol	ZigBee
Max. # of nodes	253	About 65,000
Network protocol address	Constant	Changing
Communication between two device nodes	Not supported	Supported
Port number	Supported	Supported
Max. size of packet	About 3Mbytes	About 100bytes
Secure node registration method	Provided	Not provided

6.2. Experiment using prototype adapter

We constructed a home network using prototype adapter, and functions of the proposed protocol were confirmed. The evaluation network consists of from one to four appliance nodes, which is a combination of a prototype adapter and a PC instead of home appliances. Functions listed below are confirmed.

- Node registration (direct registration andregistration using registration proxy terminal)
- Connection and disconnection of nodes
- Multi-hop transmission
- Arrival acknowledgement and re-transmission
- Large data transmission using packet fragmentation
- Encryption of transmission data and updating encryption key

In addition to these confirmations, an experiment is carried out in order to verify safety of node registration method. The experiment environment is shown in Fig. 14. An appliance node (node A) is placed at 50cm from registration proxy terminal (node B), and another node (node C) is placed.

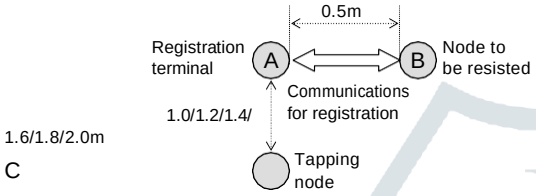


Fig. 14 Environment of experiment.

In the environment role of node C is tapping node. If node C can receive packets which are transmitted in registration process between node A and node B, node C can get secret information for node As a result, node C becomes to be able to decryption data transmitted from/to node A. The node for registration sent 200 packets at each transmission power, and we measured the number of received packet without error at node C. The measurements are made with A-C distance of 1.0, 1.2, 1.4, 1.6, 1.8, and 2.0 meters. Experimental results are shown in Table 3.

The results shows when transmission power is lower than -25dBm, a node located more than 1.5m from node A can not receive any packets from node A. Attackers are a few meters away from the user to tap without user's noticing. Probability of tapping registration process with very low transmission power is near zero. Therefore registration process in the proposed protocol is enough safety against tapping.

Table 3 Percentage of successful receive on tapping node.

Tx. Power (dBm)	Distance between nodes (m)					
	1.0	1.2	1.4	1.6	1.8	2.0
-7	100	100	100	100	100	100
-10	100	100	100	100	100	100
-15	100	100	100	100	100	100
-25	100	100	100	0	0	0

6.3. Field Test

Dozens of the prototype adapters are used in the field test of Home Healthcare Project, which is promoted by NEDO (New Energy and Industrial Technology Development Organization) [19] with support of Japanese Government. In this field test, a number of healthcare devices are integrated in a home network via our adapters. Effectiveness of the home network for healthcare application was evaluated. Through this test it is confirmed that the proposed protocol implemented on the prototype adapters effectively works in practice.

7. Conclusion

In this paper, a network protocol for home networks using IEEE 802.15.4 is proposed, which is designed in consideration of features and requirements of home networks for control and telemetry applications. The protocol makes processes on device nodes simple, and includes a new node registration method, "proxy registration". To evaluate and verify the protocol, an evaluation system including prototype adapter is constructed. The system shows that the functions included in the protocol works correctly, and experimental results show that the node registration method is enough safety.

References

[1] S. Teger, and D. J. Waks, "End-User Perspectives on Home Networking," IEEE Communication Magazine, vol. 40, no. 4 pp. 114–119, Apr. 2002.
[2] IEEE, IEEE Std. 802.3-2005, Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, Dec. 2005.
[3] IEEE, IEEE Std 802.11g-2003, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, June 2018.
[4] UPnP Forum, UPnP Device Architecture 1.0, Dec. 2012.
[5] DLNA, http://www.dlna.org.
[6] IEEE, IEEE Std. 802.15.4, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), October 2017.
[7] E. Callaway, P. Gorday, L. Hester, J. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks," IEEE Communications Magazine, vol.40, Issue 8, pp.70–77, Aug. 2002.
[8] J.C. Haartsen, "The Bluetooth Radio System," IEEE Personal Communications, vol.7, Issue 1, pp.28–36, Feb. 2000.
[9] R. Droms, "Dynamic Host Configuration Protocol (DHCP)," IETF Request for Comments (RFC) 2131, Mar. 2001.
[10] C.E. Perkins, E.M. Belding-Royer, and I. Chakers, "Ad Hoc On Demand Distance Vector (AODV) Routing," IETF Internet draft, Oct. 2010.
[11] R. Thayer,N. Doraswamy, and R. Glenn, "IP Security Document Roadmap," IETF Request for Comments (RFC) 2411, Nov. 2018.
[12] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF Internet draft, Jan. 2017.