Journal of Biomedical Informatics 52 (2014) 406–417

Contents lists available at ScienceDirect

Journal of Biomedical Informatics

journal homepage: www.elsevier.com/locate/yjbin

All-IP wireless sensor networks for real-time patient monitoring

Xiaonan Wang *, Deguang Le, Hongbin Cheng, Conghua Xie

Computer Science Department, Changshu Institute of Technology, Jiangsu, Changshu 215500, China

ARTICLE INFO

Article history:
Received 7 September 2013
Accepted 8 August 2014
Available online 19 August 2014

Keywords:
All-IP wireless sensor network
Patient
Monitoring
Real time
Link layer

ABSTRACT

This paper proposes the all-IP WSNs (wireless sensor networks) for real-time patient monitoring. In this paper, the all-IP WSN architecture based on gateway trees is proposed and the hierarchical address structure is presented. Based on this architecture, the all-IP WSN can perform routing without route discovery. Moreover, a mobile node is always identified by a home address and it does not need to be configured with a care-of address during the mobility process, so the communication disruption caused by the address change is avoided. Through the proposed scheme, a physician can monitor the vital signs of a patient at any time and at any places, and according to the IPv6 address he can also obtain the location information of the patient in order to perform effective and timely treatment. Finally, the proposed scheme is evaluated based on the simulation, and the simulation data indicate that the proposed scheme might effectively reduce the communication delay and control cost, and lower the packet loss rate.

1. Introduction

In the next 20 years, the elderly population in the world is rapidly growing and may be reach nearly 20% of the overall population [1,2]. People as they age tend to have increasing health care needs as well as chronic conditions. Consequently, it becomes of paramount importance to deliver quality healthcare with low costs to a growing elderly population. Monitoring chromic conditions might be the most important application of WSN. The main benefit of traditional WSN applications is to achieve remote monitoring. This benefit can be used in many fields, and one typical example is human (animal) biofeedback [3,4]. With remote monitoring, the treatment of emergency conditions for patients can become easy and the people with different levels of physical disabilities can be enabled to have a more independent life. Contrary to building more hospitals, WSN technologies may provide the healthcare with a much lower cost to achieve the patient monitoring [5,6]. The application of WSNs in healthcare might offer an efficient solution for patient monitoring in an automatic way [7,8]. For example, sensors can automatically collect patients' physical data and send these collected data to a computer for analysis. Sensors can sense even small changes in vital signals that humans might overlook, and automatically and quickly notify doctors of these changes. Since these data collected from WSN can be stored in the electronic format, the electronic devices such as computers may assist a human physician to make more informed diagnoses. In this way, the diagnosis and treatment process may be semi-automated.

However, the traditional WSN is data-centric, and it is a sensor node that takes the initiative in sending data to a sink which aggregates data and then forwards the aggregated data to a computer for later analysis [9,10]. For example, when a sensor node senses changes in vital signals, such as heart rate and blood oxygen levels, it takes the initiative in sending these abnormal data to a computer in the emergency for diagnoses. During the diagnosis process, if a physician needs more real-time data for further analysis, it is impossible for a physician to take the initiative in obtaining the real-time physical parameters. Moreover, if there is an interval between the data collection and data analysis, then it is hard to achieve the real-time patient monitoring. Also, in some emergency cases, it is difficult for a physician to perform a real-time treatment because the physician cannot obtain a patient's current location information.

Therefore, it is important for a physician to take the initiative in obtaining the real-time physical parameters and location information of a patient at any time and at any places. This is a main motivation of our study, and the objective of our study is to propose a scheme where a physician can take the initiative to get any patient's physical parameters at any time and at any places to achieve the real-time monitoring. In order to achieve this objective, this paper proposes a patient monitoring scheme based on all-IP WSNs. Since the all-IP WSN can use the IPv6 protocol to achieve the end-to-end communication with the IPv6 Internet, a physician can take the initiative to get any patient's physical parameters at any time and at any places to achieve the real-time monitoring through the proposed scheme. This scheme is based on all-IP WSNs, and it has the following contributions:

* Corresponding author.

http://dx.doi.org/10.1016/j.jbi.2014.08.002
1532-0464/

(1) The all-IP WSN architecture based on gateway trees is proposed. Based on this architecture, the hierarchical IPv6 address structure for the all-IP WSN is presented in order to compress the valid length of an address and reduce the transmission cost and delay.
(2) Based on this architecture, the routing algorithm is proposed and it is performed in the link layer without route discovery, so the communication delay is shortened, the control cost is reduced and the packet loss rate is lowered.
(3) In this scheme, a mobile node is always identified by its home address and it does not need to be configured with a care-of address during the mobility process, so the communication disruption caused by the address change is avoided. As a result, the communication delay is shortened, the control cost is reduced and the packet loss rate is lowered.
(4) Through the proposed scheme, a physician can monitor the vital signs of a patient at any time and at any places. According to the IPv6 addresses of mobile nodes a patient is equipped with, a physician can obtain the location information of the patient in order to perform an effective and timely treatment.

The remainder of this paper is organized as follows. In Section 2, the related work on the patient monitoring systems based on WSNs is discussed. The architecture for the all-IP WSNs is proposed in Section 3, the mobility handover algorithm is discussed in Section 4, the patient monitoring based on all-IP WSNs is presented in Section 5, and the performance of the proposed scheme is evaluated in Section 6. We conclude the paper with a summary in Section 7.

2. Related work

The application of WSNs in healthcare offers an efficient solution for patient monitoring [7,8]. This section reviews the related work on these monitoring applications based on WSN, and it includes four parts. The first part gives an introduction to the traditional WSN, the second part discusses the benefits and key technology issues of the WSN application in the healthcare monitoring, the third part reviews the patient monitoring systems based on the traditional WSN, and the fourth part presents our solution.

2.1. Traditional WSN

A WSN is made up of a number of sensor nodes which can work cooperatively to sense and collect data from the environment and then transmit the sensed data to the user [11], and it has the following characteristics [12]:

(1) A WSN is data-centric. That means that data are transmitted based on certain attributes such as the temperature beyond a certain threshold.
(2) A WSN is application-specific. That is, the requirements of the network change with the applications. For example, in some applications sensor nodes are fixed while in the other applications, sensor nodes are mobile.
(3) In a WSN, the collected data are first aggregated and then transmitted, so it is always a sensor node that takes the initiative in sending the collected data to a sink which performs the data aggregation.
(4) A sensor node does not have a unique ID. That means that it is impossible to obtain the data collected by a specific sensor node.

Since sensor nodes are small and inexpensive, a WSN has great potential in many applications such as healthcare monitoring [13].

2.2. Benefits and key technology issues of healthcare monitoring based on traditional WSN

Alemdar and Ersoy [13] survey the recent research on future intelligent monitoring applications and discuss their benefits. The chief aim of the WSN application in the healthcare monitoring is to improve the healthcare monitoring services, especially for the elderly, children and chronically ill, and these applications achieve the following benefits:

(1) Remote monitoring

Remote monitoring can enable the people with different degrees of physical disabilities to have an independent and easy life, and make the little children be cared for in a more secure way.

(2) Identifying emergency situations

These applications make the identification of emergency conditions for patients become easy. For instance, when some emergency events, such as heart attacks, happen, they can be identified quickly so that lives can be saved.

(3) Low cost

The sensor devices are inexpensive for ordinary users, so the costs for pervasive healthcare systems are within the affordable range for many people.

Based on the survey of the existing healthcare monitoring applications, Alemdar and Ersoy [13] also point out that future healthcare applications still face some challenges and there are the following key technologies to be addressed:

(1) Data acquisition efficiency

The real-time acquisition of the physical data is essential. In some emergency cases, more accurate and timely data are needed for diagnosis. Therefore, it is important for a physician to obtain the real-time physical data of a patient at any time for diagnoses.

(2) Emergency data report

Healthcare monitoring applications should be able to quickly report emergency event besides periodic physiological data reporting. Under emergency conditions, emergency data should be guaranteed to be real-time.

(3) Scalability

Healthcare monitoring systems should be pervasive, so their scalability is essential. Wherever a patient is, his physiological data can be regularly reported via WSN. Similarly, wherever a physician is, he can monitor a patient's physiological data.

(4) Mobility

The chief aim of health monitoring is to provide people with high-quality healthcare services, so healthcare monitoring systems should provide mobility support. Moreover, the mobility can change a patient's position, so the acquisition of a patient's location information should be ensured because this information is essential for real-time treatment.

2.3. Patient monitoring with traditional WSN

In terms of chronology, one or two typical literatures presenting patient monitoring systems are selected each year, and they are reviewed chronologically.

Cypher et al. [14] survey previous work on wireless communications in support of healthcare networks, and they have found that the WSN application in healthcare system can provide better access and enable greater physical mobility, and in some real-time monitoring cases a continuous access to sensor nodes is important. For example, the signals from the heart are continuous, so they must be continuously sampled by sensor nodes in order to be digitized for monitoring.

Nyan et al. [15] design a healthcare monitoring system that can detect elderly people's falls. Via this system, fall-related injuries can be prevented or reduced by deploying fall impact reduction systems, such as an inflatable airbag for hip protection, before the impact. The approach is based on the characteristics of angular movements of the thigh and torso segments in falls and activities of daily living, and it is based on the assumption that thigh segments normally do not exceed a certain threshold angle to the side and forward directions in activities of daily living whereas this abnormal behavior occurs during a fall activity. This system is performed by 21 young healthy volunteers. The experimental results show that falls can be detected with an average lead-time of 700 ms before the impact occurs, and reach a sensitivity of 95.2%. This work has demonstrated that WSN can achieve the remote sensing and can be applied in the emergency conditions. However, this work is based on traditional WSN, so it is a sensor node that takes the initiative in reporting falls and a physician cannot take the initiative in detecting falls.

Dağtas et al. [16] present a secure key establishment and authentication architecture which may transmit medical data from body sensors to a hand-held device of the mobile patient. In this architecture, it is assumed the sensors might be carried on a patient's body to sense vital sign data, and a patient's hand-held device might work as a personal wireless hub. After sensors collect physical data, they may transmit these data to a handheld device which then transmits them to a local server. The local server processes and stores these data, and it also transmits the processed data to the service center for analysis and storage. This work only analyzes the architecture from the theoretical perspective, and neither specific example nor data-based findings are provided.

Huang et al. [17] present a healthcare monitoring architecture which use WSN to monitor elderly or chronic patients in their residence. A sensor node consists of various medical sensors that collect physiological data and then transmit these data via WSN to computing devices for monitoring. Three application scenarios are implemented, and they include in-home, in-hospital and nursing-home healthcare applications. These applications show that the proposed healthcare architecture promotes outpatient healthcare services with high effect and improves the nurse-monitoring process. Finally, this study also presents a monitoring application prototype for capturing sensor data from wireless sensor nodes. In this prototype application, sensor nodes collect users' physical parameters and then transmit them to electronic devices where these data are formatted in a database for long-term storage. Via reading the records in a database, one nurse or doctor is allowed to monitor several individuals at the same time. When the physical data are beyond threshold values, for example, the heart beat or body temperature goes too high or low, the nurse or doctor can be alerted.

Jara et al. [18] present a mobile protocol for hospital WSN. This proposal assumes that each node has a base network (home network) and can move into other networks, called visited networks. When a node starts moving out of a network area it detects that its link quality with the current network goes beyond a predefined threshold. The visited networks periodically send beacon messages. Thus, when this node enters a visited network it can receive the beacon messages and the needed information to communicate with the visited network.

Fotouhi et al. [19] present a reliable handoff algorithm for WSNs. This algorithm uses some parameters to determine the time for handoff, and these parameters include traffic load or energy level at access points. This scheme defines two kinds of messages: a probe request message which is sent by a node to an access point, and an acknowledgment message which is a response to a probe request and is sent by an access point to a node. In order to acknowledge the received signal strength between a node and an access point, a node periodically sends a probe request message to an access point which, in turn, returns an acknowledgment message to this node. If the node does not receive an acknowledgment message from an access point, it starts the handoff procedure immediately. This approach needs a continuous exchange of probe request/acknowledgment messages between a node and an access point to verify the link quality, and this continuous message exchange may weaken the network performance. This work only presents the handoff algorithm in the isolated WSN from the theoretical perspective, and it neither discusses the issue of WSN being connected to the Internet nor provides data-based findings. However, this work shows that WSN may support mobility and be applied in healthcare from the theoretical perspective.

González-Valenzuela et al. [20] present a patient monitoring protocol based on WSN. This protocol adopts a 2-tier network: one created by sensors used for vital signs collection, and the other by a point-to-point link established between WSN and a fixed access point. Upon experiencing poor signal reception in the latter network tier when a patient moves, the vital sign data are transmitted through sensor nodes acting as temporary relays.

Chen et al. [10] present a reliable transmission protocol based on anycast routing for wireless patient monitoring. This protocol defines three kinds of nodes: sensor nodes, router, and data receiver. Sensor nodes collect vital signs and transmit the collected data to a data receiver through the closest router. In this system, an anycast address is assigned to multiple routers scattered. If one router fails, data can be routed to a data receiver via another nearest router without communication disruption. In this way, this protocol can achieve the reliable transmission. Also, this protocol may automatically select the closest data receiver in an anycast group as a destination to reduce the transmission latency as well as the control overhead. This protocol also shortens the latency of path recovery by initiating route recovery from the intermediate routers of the original path. The performance parameters are evaluated based on simulation, and the simulation data show that anycast may reduce the communication delay and control cost. This work shows that WSN can be applied in healthcare. However, in this system, it is still a sensor node that takes the initiative in reporting data and a physician cannot take the initiative in obtaining data.

Caldeira et al. [8] first survey available healthcare solutions based on WSN, and the survey focuses on the most relevant approaches available in the literatures for hospital-WSN or medical-WSN applications. The authors point out that the major approaches are based on static nodes and it is important to achieve the ubiquitous healthcare services. With this motivation, the authors propose a healthcare solution with mobility support. This solution assumes that all nodes are registered with all the APs. Based on this assumption, a sensor node can be directly associated with an AP. If a node reaches the area all the APs cannot cover, it might be disconnected from the WSN. Moreover, this solution does not address the location-aware issue. Finally, the authors present a case study with a new ubiquitous solution for WSN in healthcare. This case study is performed by simulation using the OMNet++

tool, and simulates biofeedback monitoring in a hospital infirmary. In this scenario, it is assumed that all the nodes are identical and they are registered in all the APs that cover the monitored area. The simulation data demonstrate that the proposed solution may improve the mobility performance.

Fengou et al. [21] propose a new architecture for e-Health services. This architecture uses the WSN technology to assist the seamless integration of diverse e-Health services. Chung et al. [9] use sensor nodes to collect users' physiological signs data, and then via the sensor network these data are transferred to computers for analysis. In this system, all physiological data are stored in a database for family inquiries or accurate diagnoses by medical personnel.

Redondi et al. [22] use WSN to provide patient localization, tracking and monitoring services. In this system, a centralized implementation and a distributed solution are proposed to implement the patient localization and tracking. Strengths and weaknesses of these two solutions are discussed in terms of energy efficiency and system robustness. In the distributed solution, the burden of computation is spread across the nodes while in the centralized solution it is entirely committed to a central controller in order to save as many resources as possible on nodes. Also, in the distributed case the localization algorithm is entirely executed on resource-constrained mobile nodes, so the energy consumption is relatively large. However, the distributed solution performs all the computation needed on nodes and does not depend on any single device to execute the localization algorithm, so it is relative robust.

In Cloud Based Intelligent Health Care Service (CBIHCS) [23], sensor networks are utilized to gather specific health data which are then stored in cloud-based storage repositories for subsequent analysis and classification. One objective of CBIHCS is to correctly identify the patients as diabetic or non-diabetic, and the classification accuracy is defined as the ratio of the number of subjects correctly identified to the total number of subjects. In the experiment, the number of subjects is 27 and the number of subjects correctly identified is 25, so the classification accuracy is 92.59%.

2.4. Our solution

One main characteristic of traditional WSN is data centric [12]. Due to this characteristic, each node does not have a unique ID because routing to and from specific nodes is not required. Therefore, in the traditional WSN it is impossible to obtain the data collected by a specific sensor node.

The existing healthcare monitoring solutions show that WSN can be applied in healthcare. However, these solutions are based on traditional WSN. In these solutions, it is still a sensor node that takes the initiative in transmitting the collected data to a sink which aggregates data and then forwards the aggregated data to an electronic device for later analysis, and it is impossible for a doctor to take the initiative in obtaining the real-time physical data collected by a specific sensor node. Therefore, these solutions fail to address the key technology issues in healthcare monitoring applications [13].

This paper proposes the all-IP WSN for real-time patient monitoring. Via this scheme, wherever a physician is located, at any time he can get any patient's vital signs to achieve the real-time monitoring. This scheme adopts the following strategies to solve the key technology issues [13]:

(1) The all-IP WSN can use the IPv6 protocol to achieve the end-to-end communication with the IPv6 Internet, so it can achieve the real-time acquisition of the physiological data. Wherever a physician is located, he can obtain the real-time physiological data of a patient at any time for diagnoses.
(2) In this scheme, if the vital signs of a patient exceed a predetermined threshold, then an alarm message is promptly sent to the emergency center. In this way, emergency data can be reported in time.
(3) The all-IP WSN generally works as a stub network and is connected to the Internet via access routers. Since the Internet is deployed pervasively, the healthcare monitoring system based on all-IP WSN has strong scalability.
(4) This scheme provides a good mobility support. During the mobility process, a mobile node is always identified by its home address and can report the collected physical data at any places. The communication disruption caused by the address change is avoided. Moreover, a physician can use the IPv6 address of a mobile node's associated node to acquire the location information of a patient for real-time treatment.

3. All-IP WSN architecture

3.1. Overview

In this scheme, an all-IP WSN consists of three types of nodes: gateway nodes, fixed nodes and mobile nodes. Among them, gateway nodes and fixed nodes have routing and forwarding function, and mobile nodes have neither routing nor forwarding function. A gateway node is connected to an AR (access router) in the IPv6 network. A gateway node and multiple fixed nodes form a tree which is called the gateway tree. In a gateway tree, the root node is the gateway node, and the intermediate nodes and leaf nodes are fixed nodes. In an all-IP WSN, all gateway trees construct the routing backbone network.

A mobile node achieves the communication with the IPv6 network via the routing backbone network, and the node in a gateway tree which a mobile node directly communicates with is referred to as the associated node of the mobile node. At the same time, a mobile node has only one associated node. As illustrated in Fig. 1, the gateway trees where the gateway nodes are connected to an AR construct an all-IP subnet. The all-IP WSN architecture based on gateway trees is shown in Fig. 1.

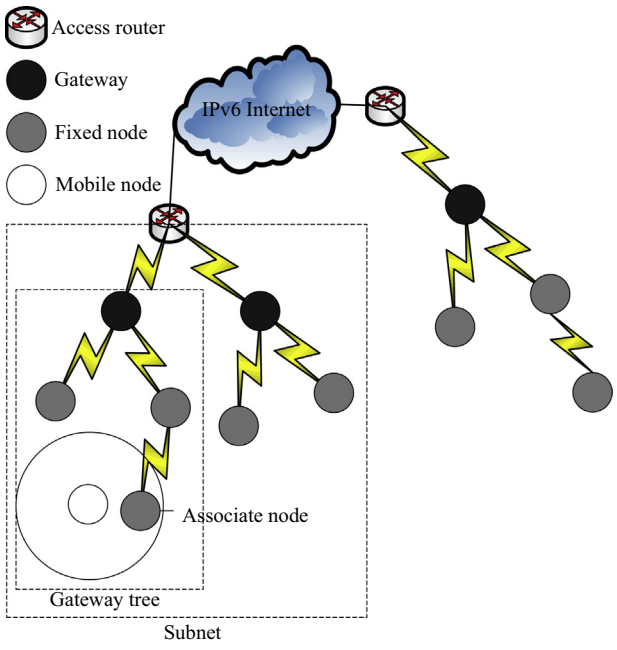


Fig. 1. Architecture based on gateway trees.

In order to achieve the real-time patient monitoring, a patient is equipped with mobile sensor nodes which are used to collect the physical data. These sensor nodes can be built into a fabric belt [17] and this belt can be placed on the body parts, such as waist or wrist. A patient should try to wear these sensor nodes in the daily living so that these nodes can collect the physical data for the real-time and continuous monitoring. The gateway nodes and fixed nodes in the all-IP routing backbone network are distributed around roads, shops, houses, etc. In these locations, a gateway should be placed in a place near an AR because it needs to be connected to an AR in the IPv6 Internet. These nodes are usually encased in a cover in order to withstand the conditions of special locations. For example, when a sensor node is encased in a SmartStud cover which is water-proof and is able to withstand 16,000 lbs, it can be protected even if it is placed on a road [24]. Take a shop for example, in each floor, a gateway node is put in an office near an AR and a few fixed nodes are evenly distributed so that they can form a gateway tree. The gateway trees in the whole shop are connected to the IPv6 Internet through an AR, and they form a subnet. When a patient equipped with mobile nodes enters a shop, it establishes an associated relationship with a node in a gateway tree, and achieves the communication with the IPv6 Internet through the associated node.

3.2. IPv6 address structure

Based on the architecture in Fig. 1, this scheme proposes the following hierarchical IPv6 address structure, as shown in Table 1.

As presented in Table 1, an IPv6 address is made up of two parts. The first part is the global routing prefix, and the global routing prefixes of all nodes in one all-IP WSN are the same. The second part is the node ID which uniquely identifies a node in one all-IP WSN, and the node ID also works as a link address. The IPv6 address of a gateway node is preset. An example of an IPv6 address is provided in Appendix A.

3.3. IPv6 address configuration

The link protocol of an all-IP WSN is IEEE 802.15.4 [25]. The command frames in our scheme are implemented through expanding the type of the IEEE802.15.4 command frame.

3.3.1. Address configuration for fixed nodes

When a fixed sensor node starts, it acquires an IPv6 address through joining a gateway tree. After a fixed node acquires an address, it begins to periodically broadcast a beacon frame. A fixed node X acquires an IPv6 address according to the following process:

(1) X broadcasts an Req_F command frame.
(2) After a neighbor gateway node/fixed node with an IPv6 address and the address space receives the Req_F frame, it returns X an Res_F command frame whose payload is the assigned node ID.
(3) X calculates the depth values of the sources nodes of all the received Res_F frames, and selects the node M with the minimum depth as its father node. Then, X returns M an Ack_F command frame whose payload is the assigned node ID, and combines the assigned node ID with its father node's global routing prefix to form its IPv6 address.

Table 1
IPv6 address structure.

$(64 + i)$ bits	$(64 - i)$ bits
Global routing prefix	Node ID

(4) After M receives the Ack_F frame, it marks the node ID assigned for X as the assigned state.
(5) X successfully joins a gateway tree and acquires an IPv6 address.

An example of a fixed node's address configuration is given in Appendix B.

3.3.2. Address configuration for mobile nodes

In this scheme, a(n) AR/gateway node/fixed node stores an associate table to record the relationship between a mobile node and its associated node. One entry in the associate table consists of two fields: the mobile node field and the associated node field. After a mobile node Y starts, it acquires its home address and associated node through the following process.

(1) Y broadcasts an Req_M command frame:
(2) After a neighbor gateway node/fixed node/mobile node with an IPv6 address and the address space receives the Req_M frame, it returns Y an Res_M frame whose payload is the assigned node ID.
(3) Y checks all the received Res_M frames, and selects the node F with the minimum length of the assigned node ID as its father node. Then, Y returns F an Ack_M command frame whose payload is the assigned node ID, and combines the assigned node ID with F's global routing prefix to form an IPv6 address. If F is a fixed node, then Y marks F as its associated node. Otherwise, Y selects the gateway node/fixed node S with the strongest signal and sends an Associate_M command frame to S.
(4) After F receives the Ack_M frame, it marks the node ID assigned for Y as the assigned state. If F is a fixed node, then it adds into the associate table an entry where the mobile node field is Y's link address and the associated node field is its link address. Otherwise, after S receives the Associate_M frame, it adds into the associate table an entry where the mobile node field is Y's link address and the associated node field is its link address, and then sends Y an Res_M command frame. After Y receives the Response_M frame, it marks S as its associated node.
(5) Y acquires an IPv6 address and its associated node and begins to periodically broadcast a beacon frame.

An example of a mobile node's address configuration is given in Appendix B.

4. Mobility handover

4.1. Next associated node

In this scheme, if the associated node of a mobile node detects that this mobile node is leaving its communication range, then it uses RSSI and AoA [26–28] to select this mobile node's next associate node. An example of selecting a mobile node's next associated node is given in Appendix C.

4.2. Intra-subnet mobility handover

If the associated node S1 of a mobile node X detects that X is about to move out of its communication range, it selects as X's next associated node the fixed node S2 which is closest to X. As illustrated in Fig. 2(a) and (b) where the node F is the nearest ancestor node of S1 and S2, when S1 and S2 belong to the same subnet, S1 does the following operations:

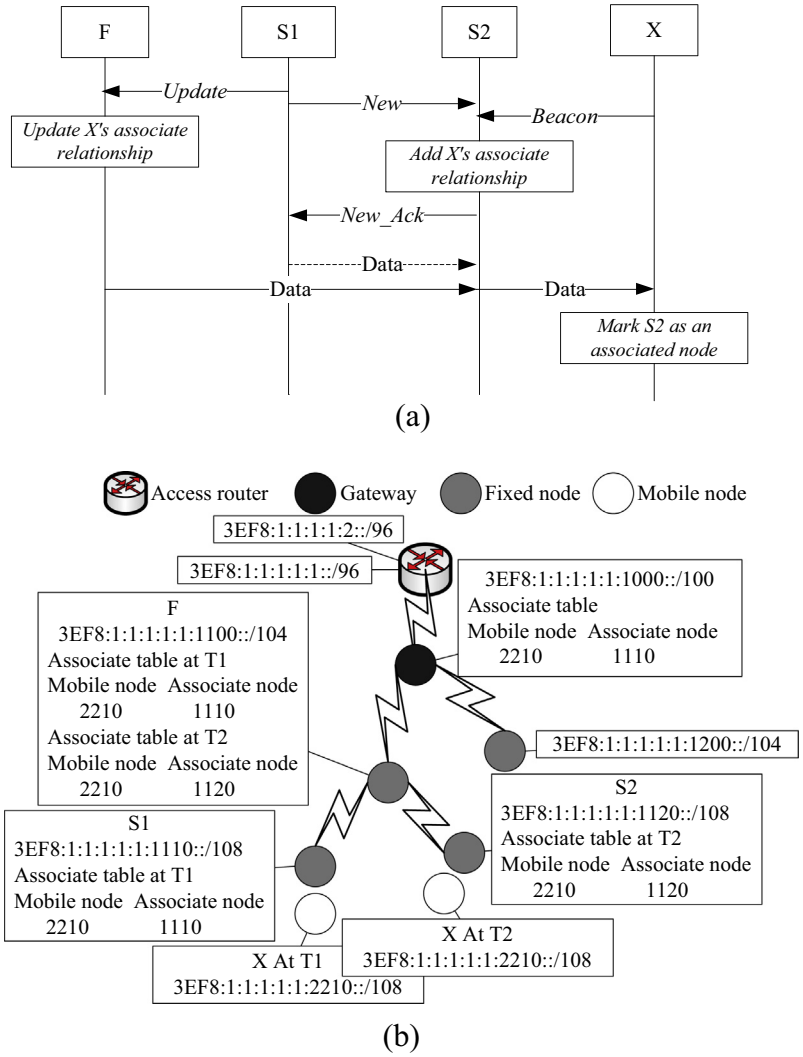


Fig. 2. Intra-subnet mobility handover.

(1) S1 sends its father node an Update command frame whose payload is X's address (If X's global routing prefix is the same as S1's one, then it is X's link address. Otherwise, it is X's IPv6 address) and S2's link address, and then S1 sends S2 a New command frame whose payload is X's address. Finally, S1 removes X's entry from the associate table.
(2) After the father node receives the Update frame, it checks whether S2 is its descendant node. If it is, the father node updates the associated node field in X's entry with S2's link address and goes to step (3). Otherwise, the father node removes X's entry from the associate table, forwards the Update frame to its father node and goes to step 2).
(3) After S2 receives the New frame from S1 and the beacon frame from X, it adds into its associate table X's entry where the associated node field is its link address, and then returns S1 an New_Ack command frame whose content is X's address.
(4) S1 receives the New_Ack frame from S2. If S1 has the data frames destined for X, then it sends the data frames to S2.
(5) After S2 receives the data frames destined for X, it forwards them to X. After X receives the data frames from S2, it marks S2 as its associated node.

In this scheme, when a patient moves within one subnet, for example, from one floor to another floor in a shop, then the above mobility handover is performed to maintain the communication continuity.

4.3. Inter-subnet mobility handover

If the associated node of a mobile node X detects that X is about to move out of its communication range, it selects the fixed node S2 as X's next associated node. As illustrated in Fig. 3(a) and (b), when S1 belongs to the subnet where the AR is AR1 and S2 belongs to the subnet where the AR is AR2, S1 does the following operations:

(1) S1 sends S2 an New command frame whose payload is X's address, and then it removes X's entry from the associate table.
(2) After S2 receives the New frame from S1 and the beacon frame from X, it adds into its associate table X's entry where the associated node field is its link address, returns S1 an New_Ack command frame whose payload is X's address, and sends AR2 an Update command frame whose payload is X's address.
(3) After AR2 receives the Update frame, it adds into its associate table X's entry where the associated node field is S2's link address.
(4) S1 receives the New_Ack frame from S2. If S1 has the data frames destined for X, then it sends the data frames to S2.

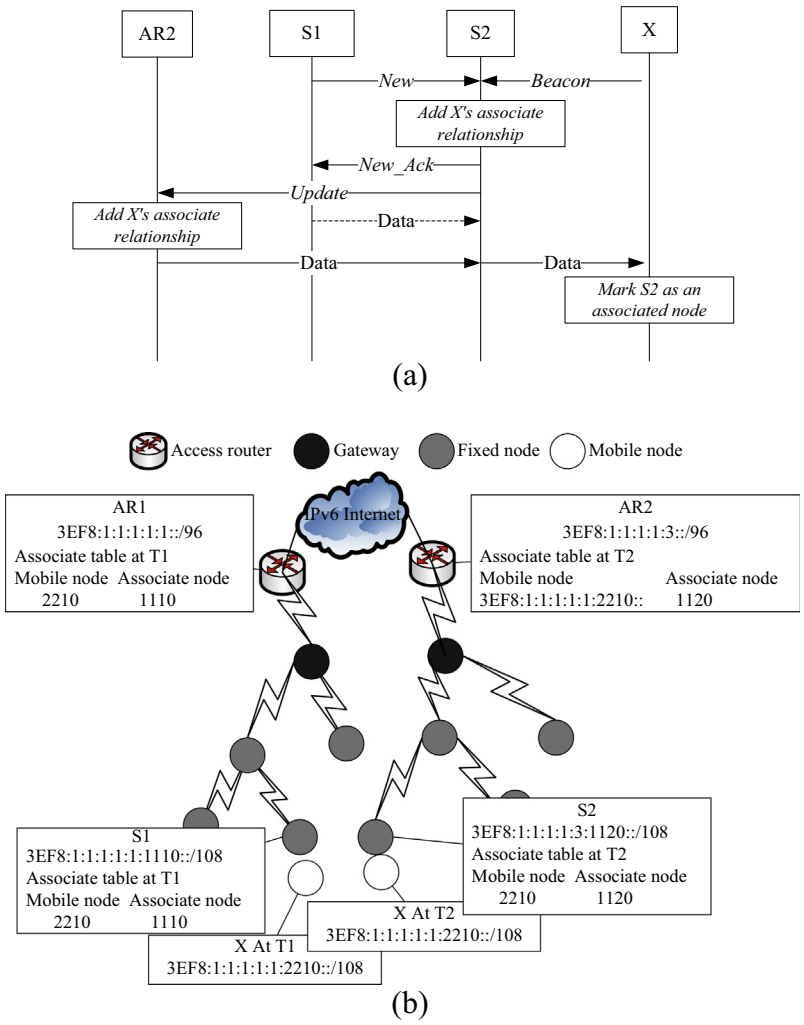


Fig. 3. Inter-subnet mobility handover.

(5) After S2 receives the data frames destined for X, it forwards them to X. After X receives the data frames from S2, it marks S2 as its associated node.

In the above process, if X's global routing prefix is different from S2's one, then AR2 still needs to notify the AR in X's home subnet of changing X's associated AR from AR1 to AR2.

In this scheme, when a patient moves between subnets, for example, from a shop to another shop, then the above mobility handover is performed to maintain the communication continuity.

5. Patient monitoring

In this scheme, the data frame format in an all-IP WSN is shown in Appendix D.

In general, vital signs are categorized into regularly collected information and emergency information [10]. The regularly collected information includes the vital signs, such as heart rate and body temperature, and it is usually transmitted in a given time period. The emergency information is generally the abnormal vital signs, such as high heart rate exceeding a predetermined threshold, and it must be transmitted immediately. For these two kinds of information, this scheme presents two types of communication modes: the regular communication and the emergent communication. In the regular communication, a physician can get a patient's vital signs at any time and at any places to achieve the real-time monitoring. In this mode, it is a physician that takes the initiative in accessing the mobile sensor nodes a patient is equipped with to get the patient's vital signs. In the emergent communication, if the vital signs of a patient exceed a predetermined threshold, then an alarm message is automatically sent to the emergency center for timely treatment. In this mode, it is a mobile sensor node a patient is equipped with that takes the initiative in sending an alarm message to the emergency center in the IPv6 Internet.

5.1. Regular communication

A physician works as an IPv6 node. An IPv6 node N takes the initiative in achieving the regular communication with a mobile node X according to the following process:

(1) N sends X a request data message to request the collected data. This message is routed in the IPv6 network, and finally reaches the access router AR1 of X's home subnet. If AR1 detects that X is located in the foreign subnet where the access router is AR2, then it forwards the message to AR2.
(2) After AR1/AR2 receives the message, it encapsulates the message with the mesh header where the final address is X's address and the destination address is the link address of X's associated node, and then sends the message to the next hop in the branch where X's associated node is located.

In the mesh header format, the final address and the destination address are two fields, as shown in Appendix D.

(3) The next hop receives the data frame. If the next hop has X's entry, then it updates the destination address in the mesh header with the associated node field in X's entry. If the next hop is X's associated node, then it goes to step (4). Otherwise, the next hop forwards the frame to the next hop in the branch where X's associated node is located and goes to step (3).
(4) X's associated node receives the data frame. If the associated node has not X's entry, then it indicates that X moves out of its communication range, and X's associated node sends the data frame to X's current associated node. Otherwise, X's associated node forwards the data frame to X and goes to step (6).
(5) After X's associated node receives the data frame, it directly forwards the data frame to X.
(6) After X receives the data frame, it encapsulates the collected information into a response data frame without the mesh header, and then sends the frame to its associated node.
(7) After the associated node receives the data frame, it routes the frame to AR1/AR2 through the gateway tree. Then, AR1/AR2 encapsulates the collected information into a response data message and sends the message to the IPv6 network where the data message ultimately reaches N.

Through the above process, a physician can acquire a patient's vital signs at any time and at any places. If a physician detects that the physical data of a patient are abnormal, he sends an alarm message to the corresponding sensor node in order to attract the patient's attention. In addition, a physician can determine the patient's location information based on the IPv6 address of the mobile node's associated node in order to perform the timely and effective treatment. An example of the regular communication is shown in Appendix E.

5.2. Emergent communication

If a mobile sensor node Y detects that the collected information exceeds a threshold, it sends an alarm message to the specified IPv6 node N (a physician or emergency center). The emergent communication process between Y and N is described as follows:

(1) Y sends N an alarm data frame whose payload is the collected information, and the destination address in the MAC header of the frame is the link address of Y's associated node S1. In the MAC header, the destination address is one field, as shown in Appendix D.
(2) After S1 receives the alarm data frame, it routes the frame to the access router AR1 in the subnet through the gateway tree.
(3) Then, AR1 encapsulates the alarm data into an alarm data message, and sends the message to the IPv6 network where the alarm data message ultimately reaches N.
(4) After N receives the alarm message, based on the IPv6 address of S1 it can determine the location information of the patient in order to perform the timely and effective treatment.

An example of the emergent communication is shown in Appendix E.

6. Simulation

NS-2 is used to simulate this scheme, and in Appendix F the simulation parameters are described. The proposed scheme is compared with the typical protocol AODV [29], and in Appendix F AODV is described. Also, in Appendix F the communication delay, the control cost and the packet loss rate are defined. As shown in Figs. 4–6, the performance parameters, including the communication delay, the control cost and the packet loss rate, are evaluated in the regular communication mode and emergent communication mode.

With the increase in speed, the link stability weakens and the packet loss rate grows. As illustrated in Fig. 4, in the proposed scheme and AODV, due to the extra delay caused by the retransmission of the lost packets, the communication delay increases with speed. AODV has longer communication delay than the proposed scheme due to the reestablishment of the disrupted routing. In the proposed scheme, in the regular communication mode, a node needs to query the associate table to update the mesh header, so the regular communication delay is longer than the emergent communication delay. In the regular communication mode, the

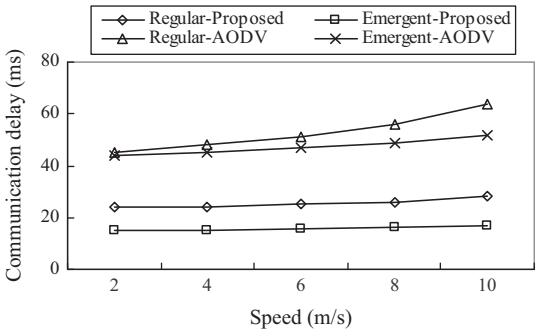


Fig. 4. Communication delay.

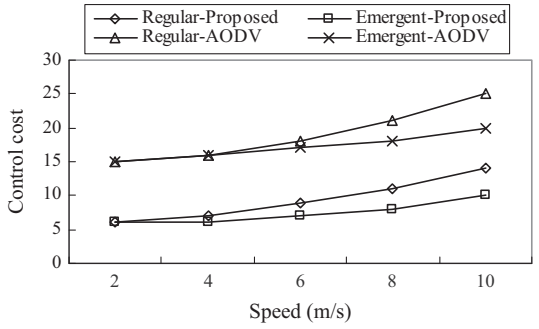


Fig. 5. Control cost.

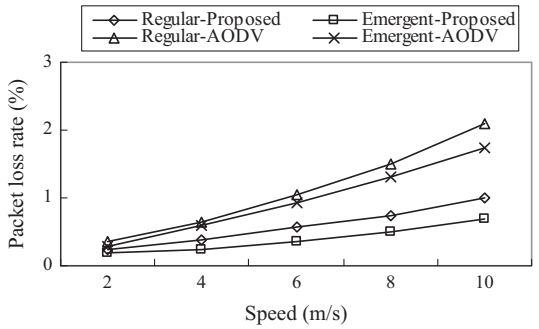


Fig. 6. Packet loss rate.

destination node is a mobile node. In AODV, if a mobile node moves out of the upstream node, then the routing reestablishment has to be performed. As a result, the regular communication delay is longer than the emergent communication delay.

With the increase in speed, the packet loss rate grows. From Fig. 5, it can be seen that the control cost in AODV is more than the one in the proposed scheme. In AODV, due to the extra cost caused by the retransmission of the lost packets and the reestablishment of the disrupted routing, the control cost increases with speed. In the proposed scheme, with the increase in speed, the probability of performing the inter-subnet mobility handover grows, so the control cost grows. In the proposed scheme, in the regular communication mode a mobile node is the destination node while in the emergent communication mode a mobile node is the source node. Therefore, during the regular communication process, the probability of performing the mobility handover to maintain the communication continuity is greater, so the control cost is more than the one in the emergent communication mode. In AODV, in the regular communication mode, the destination node is a mobile node. During the communication process, if a mobile node moves out of the communication range of the upstream node, then the routing reestablishment has to be performed. As a result, the control cost in the regular communication mode is more than the one in the emergent communication mode.

With the increase in speed, the link stability weakens. From Figs. 4 and 5, it can be seen that with the increase in speed both the communication delay and the control cost grow. Therefore, as shown in Fig. 6, the packet loss rate also increases with speed,

From Figs. 4–6, it can be seen that the proposed scheme has better performance, and the reasons are analyzed as follows:

(1) The hierarchical IPv6 address structure reduces the valid length of an address, so the transmission cost and delay are reduced.
(2) The routing based on gateway trees can be automatically performed in the link layer without route discovery, so the communication delay is shortened, the control cost is reduced and the packet loss rate is lowered.
(3) A mobile node does not need a care-of address during the mobility process, so the communication disruption caused by the address change is avoided. As a result, the communication delay is shortened, the control cost is reduced and the packet loss rate is lowered.

7. Conclusion

Compared with the traditional WSN which is data-centric, the all-IP WSN is address-centric and can use the IPv6 protocol to achieve the end-to-end communication with the IPv6 Internet. Therefore, this paper proposes the all-IP WSN for real-time patient monitoring so that a physician can get any patient's physical parameters at any time and at any places.

In order to reduce the communication delay, the all-IP WSN architecture based on gateway trees is proposed and it has the following characteristics:

(1) A mobile node achieves the communication with the IPv6 network via the routing backbone network where the routing is performed in the link layer without route discovery.
(2) A mobile node is always identified by its home address and it does not need to be configured with a care-of address during the mobility process, so the communication disruption caused by the address change is avoided.

In this architecture, a patient is equipped with mobile nodes, and the all-IP routing backbone network is distributed around roads, shops, houses, etc. When a patient is located in one of these places, the mobile nodes can always use its home address to perform the communication with the internet via the all-IP routing backbone. In this way, the real-time patient monitoring is achieved.

Based on this architecture, for the regularly collected information and emergency information, two types of communication modes are presented: the regular communication and the emergent communication. In the regular communication, a physician can get a patient's vital signs at any time and at any places to achieve the real-time monitoring. In the emergent communication, if the vital signs of a patient exceed a predetermined threshold, then an alarm message is automatically sent to the emergency center for the timely treatment. In these two modes, a physician can use the IPv6 address of a mobile node's associated node to determine the location information of a patient in order to perform the timely and effective treatment.

The performance parameters of the proposed scheme are simulated, and the simulation data indicate that the proposed scheme might effectively shorten the communication delay, reduce the control cost and lower the packet loss rate.

Acknowledgments

This work is supported by Jiangsu Nature Science Foundation (BK20141230) and National Natural Science Foundation of China (61202440).

Appendix A

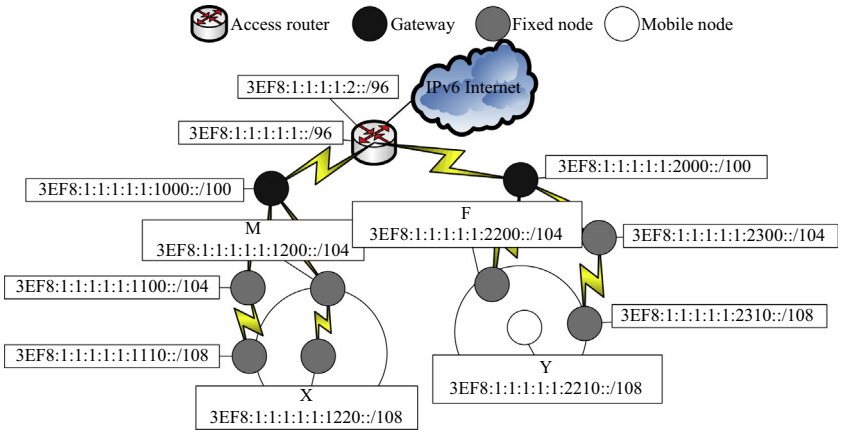
The purpose of this appendix is to show an example of an IPv6 address. In Table 1, the valid length l ($l \leqslant (64 - i)$) of a fixed node's node ID is proportional to the depth d of the fixed node in the corresponding gateway tree, as shown in formula (1) where λ is the proportional coefficient. It is assumed that a gateway node's depth is 1.

$$l = \lambda \times d \tag{1}$$

In Table 1 and formula (1), i and λ are determined by the network size and the node density in the practical applications. Taking the generality into account, this scheme sets i to 32 and λ to 4. In this way, a subnet can contain up to 15 (except 0) gateway trees, the depth of a tree can reach up to 8, and a node in a tree can have up to 15 child nodes (except 0). For example, if the IPv6 address of a gateway node is 3EF8:1:1:1:1:1:1000::/100, then the addresses of its child nodes are 3EF8:1:1:1:1:1:1X00::/104 where X ranges from 1 to F.

Appendix B

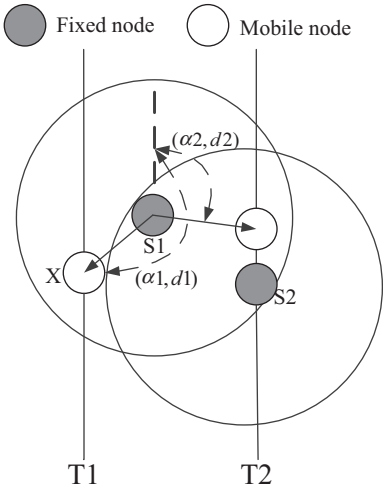
The purpose of this appendix is to show an example of a node's address configuration. In the following figure, a fixed node X acquires an IPv6 address 3EF8:1:1:1:1:1:1220::/108 from the neighbor node M, and then it marks M as its father node to join a gateway tree. It can be seen that this address configuration algorithm can reduce the valid length of a fixed node's IPv6 address in order to reduce the transmission delay. In the following figure, a mobile node Y obtains an IPv6 address 3EF8:1:1:1:1:1:2210::/108 from a fixed node F. Since F is a fixed node, Y marks F as its associated node. It can be seen that this address configuration algorithm can reduce the valid length of a mobile node's IPv6 address in order to reduce the transmission delay.



Appendix C

The purpose of this appendix is to show an example of selecting a mobile node's next associated node. In this scheme, a fixed node can calculate the distance to one neighbor fixed node by measuring the signal strength of a beacon frame from the neighbor node, and can also obtain the angle between itself and one neighbor fixed node by measuring a beacon frame from the neighbor node with AoA [26–28]. In this way, a fixed node can store the relative positions of its neighbor fixed nodes. In the same way, the associated node of a mobile node can determine whether the mobile node is leaving its communication area by measuring the signal strength of a beacon frame from the mobile node, and can acquire the relative position of the mobile node by measuring a beacon frame from the mobile node with AoA. If the associated node of a mobile node detects that this mobile node is leaving its communication range, then it selects as this mobile node's next associate node the neighbor fixed node which is closest to this mobile node.

In the following figure, the relative positions between a mobile node X and its associated node S1 at the time T1 and T2 are $(\alpha 1, d1)$ and $(\alpha 2, d2)$ respectively. At the time T2, S1 detects that X is leaving its communication area, so it selects as X's next associated node the neighbor fixed node S2 which is closest to X.



Appendix D

The purpose of this appendix is to show the data frame format and the mesh header format, as shown in the following tables. The definitions in the remaining fields are the same as the ones in RFC 4944 [30].

Data frame format

MAC header	Mesh header	Fragment type	Fragment header	Payload	
Mesh header					
2 bits	2 bits	4 bits	1 byte	(1–4) bytes	(1–16) bytes
10	O	F	Hop limit	Destination address	Final address

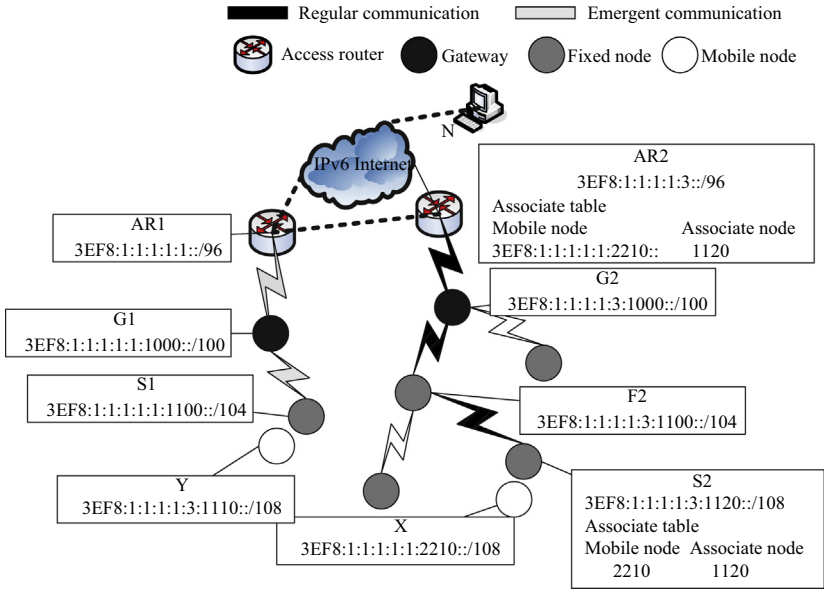
In the data frame format, the MAC header includes the source link address field whose value is the link address of the node forwarding this data frame, and the destination link address field whose value is the link address of the next hop. In the mesh header, O and F indicate the length of the destination address and the length of the final address respectively. For example, 0 indicates that the address length is 1 byte, and 1 means that the address length is 2 bytes, and so on. The value of the hop limit is the maximum depth of a gateway tree and decreases by 1 with one hop. In this scheme, the routing is performed in the link layer, so only the first fragment includes the IPv6 header.

Appendix E

The purpose of this appendix is to show the communication process. The regular communication process is shown in the following figure where an IPv6 node N sends a request data message to a mobile node X to request the collected data. This message first reaches the access router AR1 of X's home subnet. Since AR1 detects that X is located in the foreign subnet where the access router is AR2, it forwards the message to AR2. According to the associate table, AR2 can learn that X's associate node is the fixed node S2, so it forwards this message to the next hop G2 in the branch where S2 is located. Based on S2's address, G2 forwards this message to the next hop F2 which forwards this message to S2. Finally, S2 directly forwards this message to X. X encapsulates the collected information into a response data message and sends this message to S2. After S2 receives this message, it sends this message to F2. In this way, based on the gateway tree, this message finally reaches AR2 which then sends this message to the IPv6 network where this message ultimately reaches N.

The emergent communication process is also shown in the following figure where a mobile sensor node Y detects that the

collected information exceeds a threshold. Therefore, Y sends an alarm message to the specified IPv6 node N. This message first reaches Y's associated node S1 which then forwards this message to S1's father node G1. Finally, via the gateway tree this message reaches the access router AR1 which then sends this message to the IPv6 network where this alarm message ultimately reaches N.



Appendix F

The purpose of this appendix is to show the simulation parameters, as shown in the following table.

Simulation parameters Parameter description	Parameter value
Simulation area	100×200 m^2
Number of subnets	2
Number of fixed nodes	50
Number of mobile nodes	200
Mobility model	Random walk mobility model
Maximum speed	10m/s
Mobile angle	$[0, 2\pi]$
Communication range of a node	30 m
MAC protocol	IEEE 802.15.4
Simulation time	200 s

The terms in the simulation are described as follows:

AODV: the Ad hoc On-Demand Distance Vector protocol is intended for use by mobile nodes in a network, and it can determine unicast routes to destinations within the network.

Communication delay: it is the delay taken by routing a frame from a mobile node to an access router.

Control cost: it is the total number of command frames used for routing and mobility handover during one communication process.

Packet loss rate: it is a ratio of the number of packets failing to reach their destination to the total number of packets transmitted.

References

[1] Kinsella K, He W. An aging world: 2008. International Population Reports, US Census Bureau, Washington, DC, Tech. Rep. P95/09-01; 2009.
[2] Kinsella K, Phillips DR. Global aging: the challenge of success. Popul Bull 2005;60.
[3] Fowler K. Sensor survey: Part 1 the current state of sensors and sensor networks. IEEE Instrum Meas Mag 2009;12(1):39–44.
[4] Fowler K. Sensor survey: Part 2 sensors and sensor networks in five years. IEEE Instrum Meas Mag 2009;12(2):40–4.
[5] Kulkarni P, Öztürk Y. Requirements and design spaces of mobile medical care. Mobile Comput Commun Rev 2007;11(3):12–30.
[6] Varshney U. Pervasive healthcare and wireless health monitoring. Mobile Netw Appl (MONET) 2007;12(2–3):113–27.
[7] Pavel M, Jimison HB, Wactlar HD, Hayes TL, Barkis W, Skapik J, et al. The role of technology and engineering models in transforming healthcare. IEEE Rev Biomed Eng 2013;6:156–77.
[8] Caldeira JMLP, Rodrigues JJPC, Lorenz P. Toward ubiquitous mobility solutions for body sensor networks on healthcare. IEEE Commun Mag 2012;50(5):108–15.
[9] Chung YF, Liu CH. Design of a wireless sensor network platform for telehomecare. Sensors 2013;13(12):17156–75.
[10] Chen SK, Kao T, Chan CT, et al. A reliable transmission protocol for ZigBee-based wireless patient monitoring. Inform Technol Biomed IEEE Trans 2012;16(1):6–16.
[11] Yick J, Mukherjee B, Ghosal D. Wireless sensor network survey. Comput Netw 2008;52(12):2292–330.
[12] Manjeshwar A, Agrawal DP. TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: Parallel and Distributed processing symposium, international. IEEE Computer Society, vol. 3; 2001. p. 30189a–30189a.
[13] Alemdar H, Ersoy C. Wireless sensor networks for healthcare: a survey. Comput Netw 2010;54(15):2688–710.
[14] Cypher D, Chevrollier N, Montavont N, et al. Prevailing over wires in healthcare environments: benefits and challenges. Commun Mag IEEE 2006;44(4):56–63.
[15] Nyan MN, Tay FEH, Murugasu E. A wearable system for pre-impact fall detection. J Biomech 2008;41(16):3475–81.
[16] Dağtas S, Pekhteryev G, Sahinoğlu Z, et al. Real-time and secure wireless health monitoring. Int J Telemed Appl 2008:1–10. Article ID 135808.
[17] Huang YM, Hsieh MY, Chao HC, et al. Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. Selected Areas Commun IEEE J 2009;27(4):400–11.
[18] Jara AJ, Zamora MA, Skarmeta AFG. Hwsn6: hospital wireless sensor networks based on 6lowpan technology: mobility and fault tolerance management. Computational science and engineering, 2009. CSE'09. International Conference on IEEE, vol. 2; 2009. p. 879–84.
[19] Fotouhi H, Alves M, Koubaa A. On a reliable handoff procedure for supporting mobility in wireless sensor networks. In: 9th Int'l. Wksp. Real-Time Networks (RTN 2010) in conjunction with the 22nd Euromicro Int'l. Conf. Real-Time Systems (ECRTS 2010), Brussels, Belgium; July 6–9 2010.

[20] González-Valenzuela S, Chen M, Leung VCM. Mobility support for health monitoring at home using wearable sensors. Inform Technol Biomed IEEE Trans 2011;15(4):539–49.
[21] Fengou M, Mantas G, Lymberopoulos D, et al. A new framework architecture for next generation e-health services. Biomed Health Inform IEEE J 2013;17(1):9–18.
[22] Redondi A, Chirico M, Borsani L, et al. An integrated system based on wireless sensor networks for patient monitoring, localization and tracking. Ad Hoc Netw 2013;11(1):39–53.
[23] Kaur PD, Chana I. Cloud based intelligent system for delivering health care as a service. Comput Methods Programs Biomed 2014;113(1):346–59.
[24] Coleri S, Cheung SY, Varaiya P. Sensor networks for monitoring traffic. Allerton conference on communication, control and computing; 2004. p. 32–40.
[25] IEEE Computer Society. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). IEEE Standard 802.15.4. August; 2007.
[26] Wang X, Zhong S, Zhou R. A mobility support scheme for 6LoWPAN. Comput Commun 2012;35(3):392–404.
[27] Patwari N, Ash JN, Kyperountas S, et al. Locating the nodes: cooperative localization in wireless sensor networks. Signal Process Mag IEEE 2005;22(4):54–69.
[28] Zhang L, Cheng Q, Wang Y, et al. A novel distributed sensor positioning system using the dual of target tracking. Comput IEEE Trans 2008;57(2):246–60.
[29] Perkins CE, Royer EM, Das SR. Ad hoc on-demand distance vector (AODV) Routing. IETF RFC 3561; July 2003.
[30] Montenegro G, Kushalnagar N, Hui J. Transmission of IPv6 Packets over IEEE802.15.4 Networks. IETF RFC 4944; September 2007.