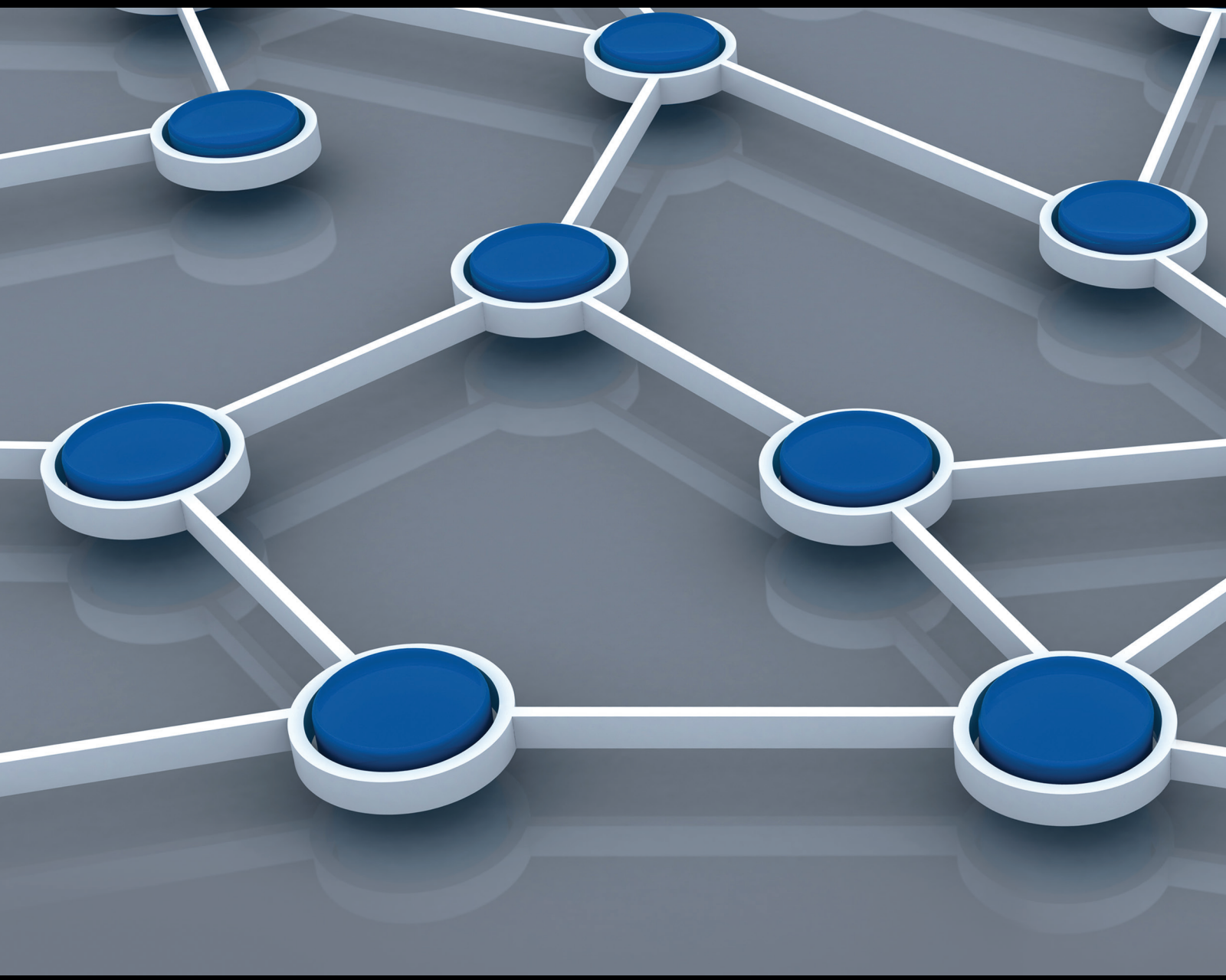
International Journal of Distributed Sensor Networks

Applications of Cognitive Radio Networks: Recent Advances and Future Directions

Guest Editors: Sung W. Kim, Miao Pan, Gyanendra Prasad Joshi, Orhan Gazi, Jianhua He, and Marceau Coupechoux



Applications of Cognitive Radio Networks: Recent Advances and Future Directions

International Journal of Distributed Sensor Networks

Applications of Cognitive Radio Networks: Recent Advances and Future Directions

Guest Editors: Sung W. Kim, Miao Pan,
Gyanendra Prasad Joshi, Orhan Gazi, Jianhua He,
and Marceau Coupechoux

Editorial Board

Contents

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2016, Article ID 4964068, 2 pages
http://dx.doi.org/10.1155/2016/4964068

Editorial

Applications of Cognitive Radio Networks: Recent Advances and Future Directions

Sung W. Kim,[1] Miao Pan,[2] Gyanendra Prasad Joshi,[1] Orhan Gazi,[3] Jianhua He,[4] and Marceau Coupechoux[5]

[1]*Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea*
[2]*Department of Computer Science, Texas Southern University, Houston, TX 77004, USA*
[3]*Department of Electric and Communication Engineering, Cankaya University, 06790 Ankara, Turkey*
[4]*Department of Electrical, Electronic and Power Engineering, Aston University, Birmingham B4 7ET, UK*
[5]*Department of Computer and Network Science, Telecom ParisTech, 75013 Paris, France*

Correspondence should be addressed to Gyanendra Prasad Joshi; joshi@ynu.ac.kr

Received 13 December 2015; Accepted 14 December 2015

Contemporary wireless networks must meet the ever increasing bandwidth requirements to assure the quality of service (QoS) to the end users. Cognitive radio (CR) technology with efficient electromagnetic spectrum management can achieve increased bandwidth beyond its traditional limits. The innovative spectrum management by CRNs allows for usage of incumbent spectrum band by unlicensed (cognitive) users possibly without interfering with the incumbent users. CR network is an intelligent and adaptive wireless communications system in which CR devices learn from its surroundings and decide the operation based on the learning. CR devices are inevitably so intelligent that they can dynamically choose carrier frequency, bandwidth, transmission rate, transmission power, and so forth.

There are many emerging CR networks applications based on CR technologies. This special issue is focused on presenting state-of-the-art research results on the application of CR networks. This is targeted for the innovative and productive discussion on the recent advancement in the application of CR networks and future directions.

The article "Convergence Research Directions in Cognitive Sensor Networks for Elderly Housing Design" by S. Suh et al. is about the application of CR sensor network. It defines smart home and surveys CR sensor network- (CRSN-) based systems for elderly housing. This article proposes research directions for the elderly smart home services based on CRSN. Particularly, the article is focused on adopting CRSN technologies to cope with dense sensors environment and heterogeneous network environment. It also discusses customizing sensors/networks classification correlated with the elderly types, and converging sensor network technologies with architectural technologies.

A lightweight and robust mechanism that appropriately secures the channel selection process is presented in the article "A Cognitive-Radio-Based Method for Improving Availability in Body Sensor Networks" by O. León et al. In this article, authors describe a new network paradigm known as cognitive body sensor networks (CBSNs). In the body area networks, seamless connectivity is crucial and must be guaranteed. Connectivity losses during emergency situations may prevent a patient from immediately receiving medical assistance and may end up in catastrophic results. This article discusses how to prevent CBSNs from the specific attacks by securing the sensing process. The proposed method relies on cryptographic primitives that require a minimum amount of memory and low energy consumption, thus being more suited for devices with limited resources. It offers authentication and encryption of control data shared by the sensors in the CBSN to agree on a given channel.

An energy-efficient layered video multicast (LVM) transmission over OFDM-based CR systems for "bandwidth-hungry" video services is presented in the article entitled

"Energy-Efficient Layered Video Multicast over OFDM-Based Cognitive Radio Systems" by W. Xu et al. This article proposes an energy utility- (EU-) based power allocation algorithm by jointly employing fractional programming and subgradient method. The novel performance metric EU is proposed to measure the sum of achieved quality of reconstructed video at all subscribers when unit transmit power is consumed. The objective is to maximize the system EU by jointly optimizing the intersession/interlayer subcarrier assignment and subsequent power allocation. To achieve the objective, it performs subcarrier assignment for base layer and enhancement layers using greedy algorithm and then presents an optimal power allocation algorithm to maximize the achievable EU using fractional programming.

In the article "A Cross-Layer-Based Routing Protocol for Ad Hoc Cognitive Radio Networks" by G. P. Joshi et al., the authors propose a cross-layer-based routing protocol for mobile ad hoc CR networks. The motivation for this paper is that rerouting is expensive in terms of energy, delay, and throughput. Thus, it is better to select a route in such a way that requires less channel switching. This paper examines the expectation of channel switching in the range of scenarios and proposes a novel route selection method to mitigate the frequent channel switching. Because excessive workload on a particular node causes network partitioning and induces repeated rerouting, the proposed protocol distributes the routing overheads among cognitive users in the network and prolongs the network lifetime. This protocol incorporates power awareness and spectrum information with a cross-layer approach.

The Sensor Virtualization Module (SVM) is proposed in the article "Sensor Virtualization Module: Virtualizing IoT Devices on Mobile Smartphones for Effective Sensor Data Management" by J. Ko et al. There are limited IoT resource-utilizing applications due to the traditional stovepipe software architecture, where the vendors provide supporting software on an end-to-end basis. The proposed SVM in this article provides a software abstraction for external IoT objects and allows applications to easily utilize various IoT resources through open APIs. It also presents the applications with a common virtualized environment where external IoT devices can be easily accessed from and via mobile computing platforms.

In the article "An Analytical Approach to Opportunistic Transmission under Rayleigh Fading Channels" by Y. B. Zikria et al., the authors present the effectiveness of the opportunistic transmission in terms of reliability and delay of transmission analytically. A fixed-distance-based statistical model is proposed for multihop and opportunistic transmission for CRSNs. Also, a unique generic Markov chain model is proposed to show the stability of opportunistic transmission.

Acknowledgments

This work was supported by the 2015 Yeungnam University Research Grant. Finally, we thank all the authors who submitted their work to this special issue and many experts who participated in the review process. We expect that this issue will certainly help researchers, academicians, practitioners, and industrialists to realize the recent advances and also may help them to work in the future directions.

Sung W. Kim
Miao Pan
Gyanendra Prasad Joshi
Orhan Gazi
Jianhua He
Marceau Coupechoux

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 725198, 8 pages
http://dx.doi.org/10.1155/2015/725198

Research Article

An Analytical Approach to Opportunistic Transmission under Rayleigh Fading Channels

Yousaf Bin Zikria, Sung Won Kim, Heejung Yu, and Seung Yeob Nam

Department of Information and Communication Engineering, Yeungnam University, 214-1 Dae-dong, Gyeongsan-Si, Kyongsan, Gyeongsangbuk-do 38541, Republic of Korea

Correspondence should be addressed to Sung Won Kim; swon@yu.ac.kr

Received 12 August 2015; Accepted 24 November 2015

Academic Editor: Lillykutty Jacob

In cognitive radio sensor networks, the routing methods including multiple relays have been extensively studied to achieve higher throughput and lower end-to-end delay. As one of innovative approaches, the opportunistic routing scheme was proposed. In this paper, the effectiveness of the opportunistic transmission in terms of reliability and delay of transmission is verified with an analytical way. For the analysis, we establish the probabilistic model with respect to distance and the number of relay nodes under the Rayleigh fading channels including path loss effects. Under this model, we develop a generic Markov chain model to obtain the analytical results and verify the effectiveness of the statistical analysis. The results show that an opportunistic transmission approach is better than traditional multihop transmissions in terms of successful data delivery with fewer transmissions. Consequently, it can provide an energy efficient transmission mechanism for cognitive radio sensor networks.

1. Introduction

Reliable data delivery with the fewest hops, keeping end-to-end delay and overhead minimized, is always a prime focus in cognitive radio sensor networks research that results in increased throughput. Moreover, the effectiveness of cognitive radio sensor networks is dependent on the development of the effective and energy efficient protocols. The key idea in opportunistic routing is to exploit the probability of reaching the farthest node in one transmission. If we can transmit a packet successfully, directly or with the fewest hops, even with low probability, we can drastically improve throughput and reduce end-to-end delay. The key challenge of this research is to analyze opportunistic transmission (OT) statistically and show that it is better in terms of successful transmissions and requires fewer transmissions, compared to traditional multihop transmissions, under the assumption that end-to-end distance is known.

The cognitive radio sensor networks are powered by finite energy resources. Recent trends in cognitive radio sensor networks [1] and introduction of wireless multimedia sensor networks [2] highlight the importance of energy consumption. Therfore, more research is inclined to increase the cognitive radio sensor network lifetime [3]. Transmission of packets in multihop wireless networks poses a great challenge because of unreliability and inherent interference of wireless links [4]. Wireless multihop networks [5–7] encompass mobile or stationary stations interconnected via an ad hoc multihop path. Each node operates not only as a host but also as a router and forwards packets on behalf of other nodes that may not be within direct radio range of the destinations. Among recent advances, opportunistic routing has appeared as an appealing multihop routing method, which gives high throughput in dynamic wireless environments.

Opportunistic routing (OR) [8–16] takes advantage of the spatial diversity and broadcast nature of wireless networks to combat time-varying links by involving multiple neighboring nodes, also known as forwarding candidates, for each packet transmission [17]. Adopting a different philosophy in route selection, OT chooses the closest node to the destination to forward a packet out of the set of nodes that actually received previous packets. This results in high expected progress per

transmission. The flexibility of OT enables agile adaptation in fast-changing wireless environments, which are particularly suitable for serving up high-rate and delay-sensitive interactive traffic [18]. Extremely opportunistic routing (ExOR) integrates routing and medium access control (MAC) protocols. It improves throughput by selecting long-range, but lossy, links. It is designed for batch forwarding. The source node includes the list of forwarders in a packet, based on expected transmission distance from the destination. All packets are broadcast. Each packet contains a BITMAP option, which marks the successfully received packet by the receiver or higher priority nodes. However, this protocol reduces spatial reuse as it is globally synchronized, and there are duplicate transmissions as well.

Opportunistic any-path forwarding (OAPF) [19] overcomes the problem of ExOR choosing low-quality routes. It introduces an expected path-count metric. This approach recursively calculates the near optimal forwarder set at each forwarder. However, this approach incurs high computational overhead. MAC-independent opportunistic routing and encoding (MORE) [20] integrates a network coding OR to enhance ExOR. The core idea is to avoid any duplication of data. It uses the concept of innovative packets to decide whether a received packet contains new information or not. Simulation results show improvement in the total number of transmissions compared to ExOR. Opportunistic routing in dynamic ad hoc networks (OPRAH) [21] builds a threaded multipath set between source and destination. It allows intermediate nodes to have more paths back to the receiver and destination. However, duplicate packet reception is an associated drawback of this protocol.

Resilient and opportunistic mesh routing (ROMER) [22] builds the mesh route for every packet. It assumes there is an existing technique to find the minimum cost from each mesh router to the gateway. When a packet is sent from a mesh router to the gateway, the source mesh router needs to set a credit cost. The overall cost to deliver the packet is the minimum cost plus the credit cost to reach the gateway. The probability that each intermediate router can forward a packet depends on the quality of the link to the parent router. The best-link-quality intermediate node forwards the packet with a probability of 1. The other nodes send the packets with the current rate of the considered link divided by the current rate of the best link. However, the disadvantage of this protocol is that it has to rely on an existing scheme to find the minimum cost from each mesh router to the gateway. The directed transmission routing protocol (DTRP) [23] is a variant of ROMER. It adjusts the probability at a forwarder in a different way. If a node is sitting on the shortest path to the destination, it forwards each packet with a probability of 1. Otherwise, the probability is dependent on the extra distance to reach the destination. The longer the distance, the smaller the probability. Geographic random forwarding (GeRaF) [16] selects the forwarding nodes using location information. Nodes closer to the destination have a higher priority. It adopts hop-by-hop forwarder selection. The disadvantage of this protocol is the cost to acquire the location information. Coding-aware opportunistic routing (CORE) [24] is an integration of confined interflow network coding and OR. It enables a node to forward a packet to the next hop that leads to the most coding changes. This iterative forwarder-by-forwarder mechanism significantly improves coding gain with a slightly increased protocol overhead.

Cooperative opportunistic routing in mobile ad hoc networks (CORMAN) [25] is a network layer solution to opportunistic data transfer in mobile ad hoc networks. This scheme broadens the applicability of ExOR to mobile multihop wireless networks without relying on external sources. Moreover, it incurs smaller overhead than ExOR by including shorter forwarder lists in data packets. To reduce the overhead in route calculation, they developed proactive source routing [26], which introduced a large-scale live update to increase throughput and decrease delay from forwarder list adaptation. This provides robustness against link-quality variation using small-scale retransmission. Simulation results show that drastic improvement in packet delivery ratio and average delay is achieved, compared to ad hoc on-demand distance vector.

This paper contributes to a new statistical analytical model for studying traditional multihop and OT. The model shows improvement in throughput and fewer transmissions to successfully deliver packets to their destination. Although many analyses have been proposed, this work is unique because we consider cases where the distance is known. Moreover, we develop an innovative generic Markov chain model of our proposed method, which can be applied to other OT scenarios. As far as we know, this is the first method that statistically formulates and shows stability in our proposed OT. We consider all possible probabilities for successful data transmission from source to destination. Using the proposed model, we compare opportunistic transmission with conventional multihop transmission, which determines the most reliable available multihop path. Evaluation results demonstrate that the OT outperforms the best traditional multihop transmission in successful delivery, number of transmissions, transmission power, number of intermediate nodes, and delay.

The rest of the paper is structured as follows. Section 2 explains the system model. Section 3 presents our proposed analytical model, comparing opportunistic transmission with traditional multihop transmission. Section 4 demonstrates the evaluation results based on the proposed statistical analytical model. Finally, Section 5 provides the conclusion and discusses future work.

2. System Model

The system consists of sender node S and receiver node R. The sender and receiver are at distance d from each other. In the literature, there are many geographical routing protocols in which nodes know their location. The distance can be calculated using the geometric coordinates and position of all the sensors [27]. Hence, we assume that d is known. This is a mild and reasonable assumption. We keep the distance fixed, and all the intermediate nodes are at an equal distance from each other. Every intermediate node can relay the packet to nodes within the communication range of it. Let signal a

be transmitted from given sender node S to receiver R in a Rayleigh fading channel. The probability density function of received power can be written as

$$f(a) = \frac{1}{P_r} e^{-a/P_r}, \tag{1}$$

where P_r is the average received power of the signal. Assume that the mean power level falls off according to the power of the range P_T/d^α. P_T is the product of transmitted signal power, transmitter and receiver antenna gains, and system loss. α is a path loss exponent. P_T is set to 1 for simplicity. In case of static node distribution, P_r is a constant.

For a given transmission rate R_t, provided signal-to-noise ratio, the required received power at the receiver to decode a packet successfully is given by

$$R_t = \log\left(1 + \frac{P_{rt}}{N_0}\right), \tag{2}$$

where the minimum required received power for successfully decoding a packet is given by

$$P_{rt} = N_0\left(2^{Rt} - 1\right). \tag{3}$$

Therefore, successful transmission probability is obtained as follows:

$$\begin{aligned} P_s &= \int_{P_{rt}}^{\infty} \frac{d^\alpha}{P_t} e^{-rd^\alpha/P_t} dr, \\ P_s &= \int_{P_{rt}}^{\infty} \frac{d^\alpha}{P_t} e^{-rd^\alpha/P_t} dr = \frac{d^\alpha}{P_t}\left[-\frac{P_t}{d^\alpha} e^{-rd^\alpha/P_t}\right]_{P_{rt}}^{\infty} \\ &= \left(e^{-d^\alpha P_{rt}/P_t}\right) = \frac{1}{e^{d^\alpha P_{rt}/P_t}}. \end{aligned} \tag{4}$$

3. Multihop Transmission

In the multihop scenario, the probability of success can be written as

$$P_s = P_{s_{si}} + P_{s_{ir}}. \tag{5}$$

P_s is the probability of successful transmission from source to destination. $P_{s_{si}}$ is the probability of successful transmission from sender to intermediate node, and $P_{s_{ir}}$ is the probability of successful transmission from intermediate node to receiver. The total distance is fixed, and intermediate nodes are equidistant. Therefore, the probability of success will be

$$P_s = \left(e^{-(d/2)^\alpha P_{rt}/P_t}\right)\left(e^{-(d/2)^\alpha P_{rt}/P_t}\right). \tag{6}$$

P_s for n nodes is

$$P_s = \left(e^{-n((d/(n-1))^\alpha P_{rt}/P_t)}\right). \tag{7}$$

Figure 1 describes the traditional multihop transmission, where i represents the intermediate nodes.

3.1. Opportunistic Multihop Transmission. In OT, the sender transmits the packet with a list of possible forwarders and priorities. The destination has the highest priority, a node that is nearest to the destination has the second highest priority, and so on. All the intermediate nodes can act as a relay and can forward the packet directly to the destination if it is in range; otherwise, the packet goes to the next highest priority node. All the intermediate nodes will keep a copy of overheard packets.

If the highest priority node successfully delivers packets to the destination, then the other nodes will discard the packet. Otherwise, the next highest priority node will try to deliver the packet to the destination. The cumulative success probability is the "success probability of the highest priority node and success probability of the next highest priority node, with the product of failure probability of highest priority nodes with respect to this node." In case of failure of all possible cases of the OT, the last case is a multihop, and success probability is 1. The receiver will send acknowledgement after successful delivery of the packet with a success probability of 1.

If the number of nodes is 2, then the equation remains the same as in the direct case:

$$P_s = \begin{cases} \left(e^{-d^\alpha P_{rt}/P_t}\right), & \text{if } n = 2 \\ \left(e^{-d^\alpha P_{rt}/P_t}\right) + \left(e^{-(d/2)^\alpha P_{rt}/P_t}\right)\left(e^{-(d/2)^\alpha P_{rt}/P_t}\right)\left(1 - e^{-d^\alpha P_{rt}/P_t}\right), & \text{if } n = 3 \\ \sum_{i=2}^{n-1} e^{-(((n-i)d/(n-1))^\alpha((i-1)d/(n-1))^\alpha)} \prod_{j=2}^{i}\left(i - e^{-((n-j+1)d/(n-1))^\alpha}\right) + e^{-((d/(n-1))^\alpha)^{n-1}(1-e^{-d^\alpha})} \prod_{k=0}^{n-3}\left(1 - e^{-(n-k-2)d/(n-1)}\right)^2 & \text{if } n > 3 \end{cases}. \tag{8}$$

With 3 nodes, the total number of hops is 2. The total probability of success is the sum of the probability from source S to destination R and the probability from intermediate relay node i to destination R, with the product of failure probability of direct transmission from source to destination.

If the number of nodes is more than 3, this equation shows the overall probability of success for n nodes, which is

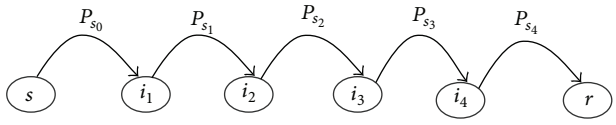


Figure 1: Traditional multihop transmission.

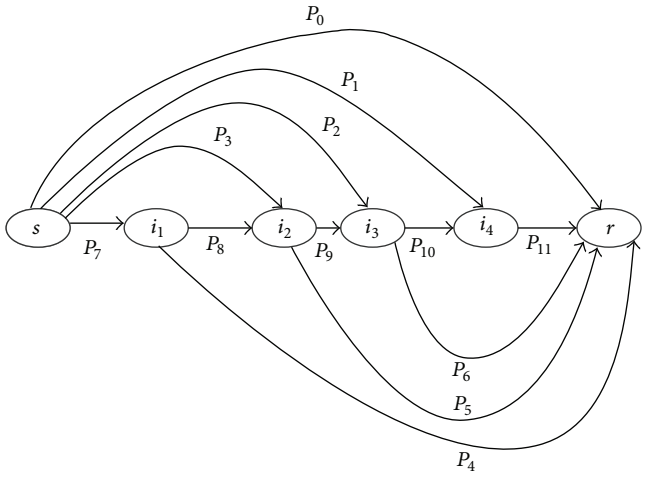


Figure 2: Opportunistic transmission.

the recursive summation of all success probabilities with failure probabilities of all the higher priority nodes with respect to that node, up to n nodes.

Figure 2 depicts the probability of success of all possible routes to the receiver.

3.2. Expected Number of Transmissions. The expected number of transmissions (ETX) [28] can be calculated as

$$\text{ETX} = \frac{1}{P_s}. \tag{9}$$

ETX is inversely proportional to the probability of success P_s.

3.3. Markov Chain Model for Opportunistic Transmission. X_n is the state of a given packet at time n. In the considered problem, state means the node where the current packet is located. The state transition diagram is shown in Figure 3. The transition a_{ij} from current state i to next state j is

$$a_{ij} = P_r\left(X_{n+1} = j \mid X_n = i\right). \tag{10}$$

If $m_{j,j}$ is the expected number of transitions until the Markov chain, starting in state j, returns to that state, then

$$\pi_j = \frac{1}{m_{j,j}}. \tag{11}$$

We are interested in $m_{j,j}$. To calculate $m_{1,1}$ transitions from state 1 till we return to state 1, we have

$$\begin{aligned} m_{1,1} &= m_{1,N} + 1, \\ m_{1,N} &= m_{1,1} - 1. \end{aligned} \tag{12}$$

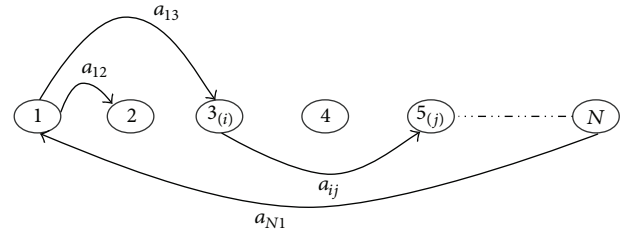


Figure 3: State diagram for opportunistic transmission.

The generic state transition matrix is

$$p = \begin{bmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1N} \\ 0 & 0 & a_{23} & \cdots & a_{2N} \\ \vdots & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & a_{(n-1)N} \\ a_{N1} & & & & 0 \end{bmatrix}, \tag{13}$$

$$\pi = \left(\pi_1 \pi_2 \pi_3 \cdots \pi_N\right).$$

The positive recurrent aperiodic states are called ergodic. For an irreducible ergodic Markov chain, $\lim_{n\to\infty} P_{i,j}^n$ exists and is independent of i. Furthermore, let

$$\begin{aligned} &\pi = \pi P \text{ or } \pi_j = \sum_i \pi_i P_{ij} \text{ or } \pi_j = \sum_i \pi_i a_{ij}, \\ &\pi_1 = a_{N1}\pi_N = \pi_N, \\ &\pi_j = \sum_i \pi_i a_{ij} = \sum_{1\le i<j} \pi_i a_{ij}, \\ &\pi_2 = \pi_1 a_{12}, \\ &\pi_3 = \pi_1 a_{13} + \pi_2 a_{23}, \\ &\pi_3 = \pi_1 a_{13} + \pi_1 a_{12} a_{23}, \\ &\pi_3 = \pi_1 \left(a_{13} + a_{12} a_{23}\right), \\ &\pi_4 = \pi_1 a_{14} + \pi_2 a_{24} + \pi_3 a_{34}, \\ &\pi_4 = \pi_1 a_{14} + \pi_1 a_{12} a_{24} + \pi_1 \left(a_{13} + a_{12} a_{23}\right) a_{34}, \\ &\pi_4 = \pi_1 \left\{a_{14} + a_{12} a_{24} + a_{13} a_{34} + a_{12} a_{23} a_{34}\right\}. \end{aligned} \tag{14}$$

From the above calculations, we can make a generic equation for $j \ge 3$ as follows:

$$\pi_j = \pi_1 \left[a_{1j} + \sum_{k=2}^{j-1} \prod_{1<b_1<\cdots<b_{k-1}<j} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{(k-1)j}} \right]. \tag{15}$$

Now, we will show that the above relation is valid using induction:

(i) $j = 3$

$$\pi_3 = \pi_1 \left[a_{13} + \sum_{k=2}^{2} \prod_{1<b_1<3} a_{1b_1} a_{b_{13}} \right], \tag{16}$$

$$\pi_3 = \pi_1 \left(a_{13} + a_{12} a_{23} \right). \tag{17}$$

(ii) We assumed that (16) is valid for $j \le n$. Therefore, let us prove this relation is valid:

$$\pi_{n+1} = \sum_{i=1}^{n} \pi_i a_{i(n+1)}, \tag{18}$$

$$\pi_{n+1} = \pi_1 a_{1n+1} + \pi_2 a_{2n+1} + \sum_{i=3}^{n} \pi_i a_{i(n+1)}, \tag{19}$$

$$\pi_{n+1} = \pi_1 a_{1n+1} + \pi_1 a_{2n+1} + \sum_{i=3}^{n} \pi_1 a_{i(n+1)} \cdot \left[a_{1i} + \sum_{k=2}^{i-1} \prod_{1<b_1<\cdots<b_{k-1}<i} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{k-1i}} \right], \tag{20}$$

$$\pi_{n+1} = \pi_1 a_{1n+1} + \pi_1 \sum_{i=2}^{n} a_{1i} a_{i(n+1)} + \sum_{i=3}^{n} \pi_1 a_{i(n+1)} \cdot \sum_{k=2}^{i-1} \prod_{1<b_1<\cdots<b_{k-1}<i} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{k-1i}}. \tag{21}$$

We simplify the last part of (21):

$$= \pi_1 \sum_{i=3}^{n} \sum_{k=2}^{i-1} \prod_{1<b_1<\cdots<b_{k-1}<i} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{k-1i}} a_{i(n+1)}$$

$$= \pi_1 \sum_{k=2}^{n-1} \prod_{1<b_1<\cdots<b_k<n+1} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{kn+1}}, \tag{22}$$

$$\pi_{n+1} = \pi_1 a_{1n+1} + \pi_1 \sum_{i=2}^{n} a_{1i} a_{i(n+1)} + \pi_1 \sum_{k=2}^{n-1} \prod_{1<b_1<\cdots<b_k<n+1} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{kn+1}}.$$

Let $k + 1 = k'$. Consider

$$\pi_{n+1} = \pi_1 a_{1n+1} + \pi_1 \sum_{i=2}^{n} a_{1i} a_{i(n+1)} + \pi_1 \sum_{k'=3}^{n} \prod_{1<b_1<\cdots<b_{k'-1}<n+1} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{(k'-1)(n+1)}}, \tag{23}$$

$$\pi_{n+1} = \pi_1 \left\{ a_{1n+1} + \pi_1 \sum_{k'=2}^{n} \prod_{1<b_1<\cdots<b_{k'-1}<n+1} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{(k'-1)(n+1)}} \right\}.$$

Since $\sum_i \pi_i = 1$, we have

$$\sum_{i=1}^{N} \pi_i = \pi_1 + \pi_1 a_{12} + \sum_{i=3}^{N} \pi_1 \left\{ a_{1i} + \sum_{k=2}^{i-1} \prod_{1<b_1<\cdots<b_{k-1}<i} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{k-1i}} \right\},$$

$$\frac{1}{\pi_1} = 1 + a_{12} + \sum_{i=3}^{N} \left\{ a_{1i} + \sum_{k=2}^{i-1} \prod_{1<b_1<\cdots<b_{k-1}<i} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{k-1i}} \right\}, \tag{24}$$

$$m_{1,N} = m_{1,1} - 1,$$

$$m_{1,N} = \frac{1}{\pi_1} - 1,$$

$$m_{1,N} = a_{12} + \sum_{i=3}^{N} \left\{ a_{1i} + \sum_{k=2}^{i-1} \prod_{1<b_1<\cdots<b_{k-1}<i} a_{1b_1} a_{b_1 b_2} \cdots a_{b_{k-1i}} \right\}.$$

Figure 4 describes the overall opportunistic transmission flow strategy. When the sender transmits the data to the receiver, the algorithm assigns the priorities according to the node's distance from the receiver. The highest priority node is always the receiver, and the next highest priority is allocated to the node that is nearest to the receiver, and so on. If the highest priority node fails to receive the data or to transmit the data to the receiver, then the next highest priority node will try to transmit the data to the receiver. According to this flow chart, we have developed our probabilities, considering the success and failure probabilities of all possible paths to the destination. The final outcome of the equations is shown in (8) described in the previous section.

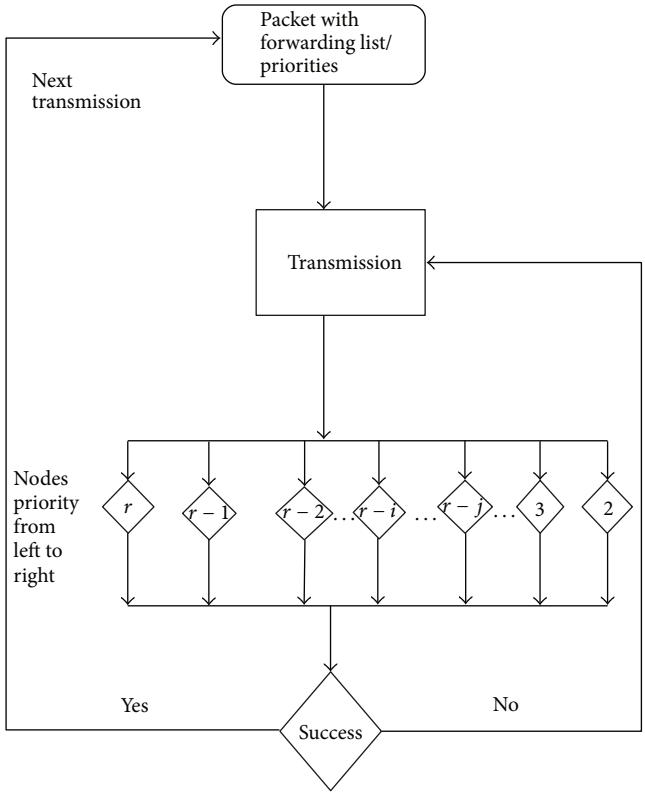


Figure 4: System flow chart.

Table 1: Nodes versus distance for multihop transmission.

Nodes	Distance/success probability				
	40	80	120	160	200
3	0.993696	0.964859	0.906123	0.816797	0.702214
5	0.997767	0.987432	0.965747	0.930953	0.882508
8	0.999035	0.994552	0.985058	0.969567	0.947442
11	0.999435	0.996805	0.991222	0.982063	0.968875
15	0.999659	0.99807	0.994691	0.989133	0.981093

4. Results and Discussion

We set the following parameters for our simulation for this scenario. P_T is set to 1, α is 2.5, and we increase the number of relay nodes between source and receiver to see the impact on the probability of success.

The impact of distance on the probability of success for multihop is depicted in Table 1. It can be seen that the probability of success decreases with increasing distance for different numbers of nodes. When the distance between sender and receiver exceeds a certain threshold, it decreases the probability of success. Moreover, the signal amplitude is decreased with increasing propagation distance. In case of failure of transmission of multihop transmission, transmission needs to follow the same path again until the data is successfully transmitted.

Table 2 shows the impact of distance on the probability of success for OT. It is clearly seen that the probability of success is reduced as the distance increases. If we compare the values with multihop transmission, the probability of success for OT is higher than multihop in all cases. The probability of success decreases with increasing distance, but the impact is very low for OT. The main reason is that if one of the possible paths to the destination fails, there are other paths that can lead to successful delivery of the data. The number of paths to the destination increases with an upsurge in the number of nodes in a network, which increases the probability of success.

Table 2: Nodes versus distance for opportunistic transmission.

Nodes	Distance				
	40	80	120	160	200
3	1	0.999969	0.999409	0.99556	0.98055
5	1	0.999626	0.996542	0.99590	0.98199
8	1	0.9999	0.998949	0.99611	0.98362
11	1	1	0.999522	0.99683	0.98521
15	1	1	0.999777	0.998402	0.99174

Table 3: ETX for multihop transmission.

Nodes	Distance/ETX				
	40	80	120	160	200
3	1.006344	1.036421	1.103603	1.224295	1.424067
5	1.002238	1.012728	1.035468	1.074168	1.133134
8	1.000966	1.005478	1.015169	1.031388	1.055473
11	1.000566	1.003205	1.008856	1.018265	1.032125
15	1.000342	1.001933	1.005337	1.010987	1.019271

Table 4: ETX for opportunistic transmission.

Nodes	Distance/ETX				
	40	80	120	160	200
3	1	1.000031	1.000591	1.019459	1.019831
5	1.00001	1.000374	1.00347	1.018008	1.016969
8	1.000003	1.0001	1.001052	1.006382	1.015093
11	1.000001	1.000043	1.000479	1.003180	1.013006
15	1	1.000019	1.000223	1.001601	1.008325

The impact of distance on the expected number of transmissions for multihop is shown in Table 3. It can be seen that ETX increases in proportion to increasing distance.

The expected number of transmissions for opportunistic transmission is presented in Table 4. It is clearly seen that the impact of distance results in more transmissions. In comparison with multihop transmission, OT requires fewer transmissions to successfully deliver the data.

Figure 5 shows the outcome of increasing transmission power on the probability of success. The probability of success rises with increased power for multihop and opportunistic transmission. Opportunistic transmission outperforms multihop transmission.

It is clearly seen from Figure 6 that the number of transmissions decreases as we increase transmission power. OT performs better than traditional multihop transmission. The outcome shows that OT is more efficient approach to deliver

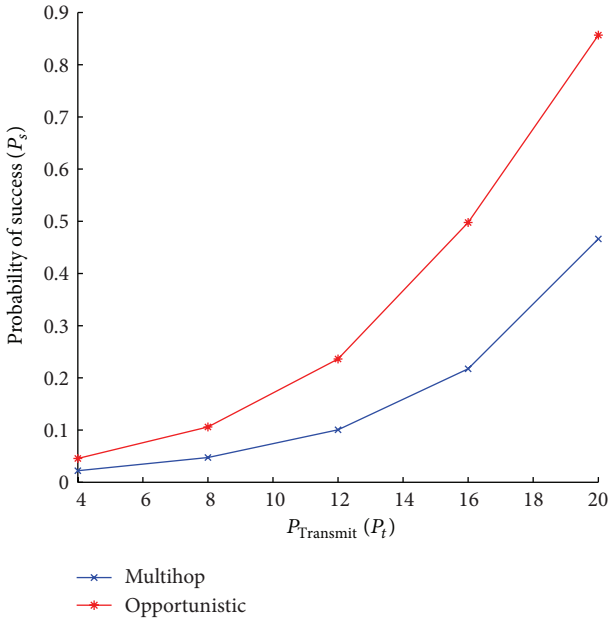


Figure 5: Effect of transmission power on P_s.

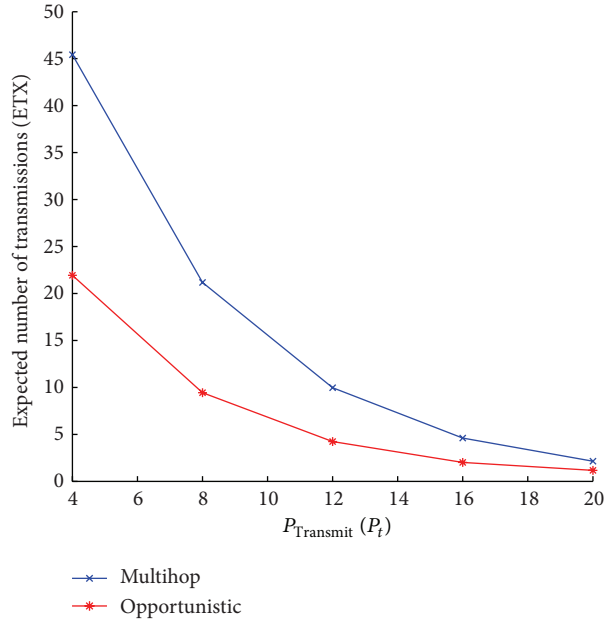


Figure 6: Effect of transmission power on ETX.

the data to the destination in fewer transmissions. Further, it reduces the energy consumption due to the less packet losses and retransmissions. Therefore, OT reduces the energy consumption and keeps the most important resource of sensors for a long period of time for communications. Consequently, maximizing the lifetime of the resource constrained cognitive radio sensor networks. Hence, the overall performance of the cognitive radio sensor networks is enhanced.

5. Conclusion

Two types of transmission have been studied in this paper, multihop and opportunistic. More specifically, a fixed-distance-based statistical model is proposed for multihop and OT for cognitive radio sensor networks. Additionally, the unique generic Markov chain model is proposed to show the stability of OT. OT shows improvement in reliably delivering the packet in fewer transmissions in contrast to multihop transmission. Hence, OT successfully delivers the data in an energy efficient way, increases the sensor's lifetime, and improves overall system performance. It opens a new direction for multihop cognitive radio sensor networking-related research.

We will extend this statistical analysis for random-distance intermediate node scenarios. We will also work on a cross-layer protocol design by incorporating these statistical analyses.

Conflict of Interests

The authors declare no conflict of interests.

Acknowledgment

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2015R1D1A1A01058751).

References

[1] O. B. Akan, O. B. Karli, and O. Ergul, "Cognitive radio sensor networks," *IEEE Network*, vol. 23, no. 4, pp. 34–40, 2009.

[2] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer Networks*, vol. 51, no. 4, pp. 921–960, 2007.

[3] S. Salim and S. Moh, "A robust and energy-efficient transport protocol for cognitive radio sensor networks," *Sensors*, vol. 14, no. 10, pp. 19533–19550, 2014.

[4] R. Rajmohan, "Topology control and routing in ad hoc networks: a survey," *ACM SIGACT News*, vol. 33, no. 2, pp. 60–73, 2002.

[5] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, no. 4, pp. 445–487, 2005.

[6] S. Lee, S. Banerjee, and B. Bhattacharjee, "The case for a multihop wireless local area network," in *Proceedings of the IEEE International Conference on Computer Communications*, pp. 894–905, Hong Kong, March 2004.

[7] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, "Link-level measurements from an 802.11b mesh network," in *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '04)*, pp. 121–132, ACM, Portland, Ore, USA, August-September 2004.

[8] S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 1, pp. 69–74, 2004.

[9] S. Biswas and R. Morris, "ExOR: opportunistic multi-hop routing for wireless networks," in *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '05)*, pp. 133–144, ACM, Philadelphia, Pa, USA, August 2005.

[10] J. Ai, A. A. Abouzeid, and Z. Ye, "Cross-layer optimal policies for spatial diversity relaying in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, pp. 2930–2939, 2008.

[11] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, 2006.

[12] H. Füßler, J. Widmer, M. Käsemann, M. Mauve, and H. Hartenstein, "Contention-Based forwarding for mobile ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 4, pp. 351–369, 2003.

[13] P. Larsson, "Selection diversity forwarding in a multihop packet radio network with fading channel and capture," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 47–54, 2001.

[14] R. C. Shah, A. Bonivento, D. Petrović, E. Lin, J. Van Greunen, and J. Rabaey, "Joint optimization of a protocol stack for sensor networks," in *Proceedings of the IEEE Military Communications Conference (MILCOM '04)*, vol. 1, pp. 480–486, IEEE, Monterey, Calif, USA, November 2004.

[15] B. Zhao and M. C. Valenti, "Practical relay networks: a generalization of hybrid-ARQ," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 1, pp. 7–18, 2005.

[16] M. Zorzi and R. R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: energy and latency performance," *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 349–365, 2003.

[17] K. Zeng, W. Lou, and M. Li, *Multihop Wireless Networks: Opportunistic Routing*, Wiley, 2011.

[18] M.-H. Lu, P. Steenkiste, and T. Chen, "Video transmission over wireless multihop networks using opportunistic routing," in *Proceedings of the Packet Video Workshop*, pp. 52–61, IEEE, Lausanne, Switzerland, November 2007.

[19] Z. Zhong, J. Wang, S. Nelakuditi, and G. Lu, "On selection of candidates for opportunistic anypath forwarding," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 10, no. 4, pp. 1–2, 2006.

[20] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '07)*, pp. 169–180, ACM, Kyoto, Japan, August 2007.

[21] C. Westphal, "Opportunistic routing in dynamic ad hoc networks: the OPRAH protocol," in *Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS '06)*, pp. 570–573, Vancouver, Canada, October 2006.

[22] Y. Yuan, H. Yang, S. H. Wong, S. Lu, and W. Arbaugh, "ROMER: resilient opportunistic mesh routing for wireless mesh networks," in *Proceedings of the 1st IEEE Workshop on Wireless Mesh Networks (WiMesh '05)*, Santa Clara, Calif, USA, September 2005.

[23] M. S. Nassr, J. Jun, S. J. Eidenbenz, A. A. Hansson, and A. M. Mielke, "Scalable and reliable sensor network routing: performance study from field deployment," in *Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM '07)*, pp. 670–678, Anchorage, Alaska, USA, May 2007.

[24] Y. Yan, B. Zhang, J. Zheng, and J. Ma, "CORE: a coding-aware opportunistic routing mechanism for wireless mesh networks," *IEEE Wireless Communications*, vol. 17, no. 3, pp. 96–103, 2010.

[25] Z. Wang, Y. Chen, and C. Li, "CORMAN: a novel cooperative opportunistic routing scheme in mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 289–296, 2012.

[26] Z. Wang, Y. Chen, and C. Li, "PSR: a lightweight proactive source routing protocol for mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 859–868, 2014.

[27] G. Guido, A. Vitale, V. Astarita, F. Saccomanno, V. P. Giofré, and V. Gallelli, "Estimation of safety performance measures from smartphone sensors," *Procedia—Social and Behavioral Sciences*, vol. 54, pp. 1095–1103, 2012.

[28] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th annual international conference on Mobile computing and networking (MobiCom '03)*, pp. 134–146, San Diego, Calif, USA, September 2003.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 272869, 13 pages
http://dx.doi.org/10.1155/2015/272869

Research Article

A Cognitive-Radio-Based Method for Improving Availability in Body Sensor Networks

Olga León,[1] Juan Hernández-Serrano,[1] Carles Garrigues,[2] and Helena Rifà-Pous[2]

[1] *Telematics Department, Technical University of Catalonia, 08034 Barcelona, Spain*
[2] *IT, Multimedia and Telecommunications Department, Open University of Catalonia, 08018 Barcelona, Spain*

Correspondence should be addressed to Olga León; olga@entel.upc.edu

Received 11 July 2015; Accepted 20 September 2015

Academic Editor: Gyanendra P. Joshi

One of the main threats to body sensor networks (BSNs) is Denial of Service attacks that disrupt communications used to transmit patients' health data. The application of cognitive radio (CR) technology into BSNs can mitigate such a threat and improve network availability, by allowing network nodes to cooperatively agree on a new radio channel whenever the quality of the channel being in use decreases. However, the cooperative spectrum sensing mechanisms used by CRs should also be protected to prevent an attacker from predicting the new channel of operation. In this work, we present a lightweight and robust mechanism that appropriately secures the channel selection process while minimizing resources consumption, thus being suited for resource constrained devices such as body sensor nodes. The proposed method has been analyzed in terms of energy consumption and transmission overhead and it has been shown that it outperforms existing cryptographic approaches.

1. Introduction

Sensor and wireless communication technologies are rapidly evolving and spreading to many fields, such as medical services. Body sensor networks (BSNs) [1, 2] are becoming more popular and powerful every day and ongoing efforts, such as the IEEE 802.15.6 standard optimized for low-power BSN devices [3], clearly reflect the increasing importance and potential of these types of networks.

A typical BSN is composed of a number of sensors that are placed at various locations on the body or in body, also known as implantable medical devices (IMDs). As depicted in Figure 1, these sensors forward sensed data to a more computationally powerful device or gateway (e.g., a smartphone) that, in its turn, can transmit the gathered data to a medical center. Therefore, the professionals can constantly monitor the patient's state and take the proper actions according to the observed data. Thus, the use of BSNs can considerably reduce the gap between a medical emergency and the medical response while increasing the autonomy of patients, that is to say, their quality of life.

Body sensors exhibit more constraints regarding size, power, battery availability, and transmission (i.e., the human body is a lossy medium) than those sensors that can be found in conventional wireless sensor networks (WSNs) and, therefore, they require specific solutions. Besides the recent IEEE 802.15.6 standard, already supported by a few commercial devices, several low-power wireless technologies [4–7] suitable for BSNs have emerged during the last years. These technologies define typical transmission rates ranging from several kbps in ANT+ to 6 Mbps in WiFi with the lowest power 802.11b mode.

Lately, there has been increasing concern in incorporating security and privacy mechanisms to medical systems in order to preserve patients' privacy and offer continuous monitoring of their health status. Besides, FDA (Food and Drug Administration) made recently a call for manufacturers to address cybersecurity issues relevant to medical devices for the entire life cycle of the device [8]. Thus, it is expected that these facts will definitely encourage a number of works in this field.

Generally speaking, the following security services should be provided in any medical system.

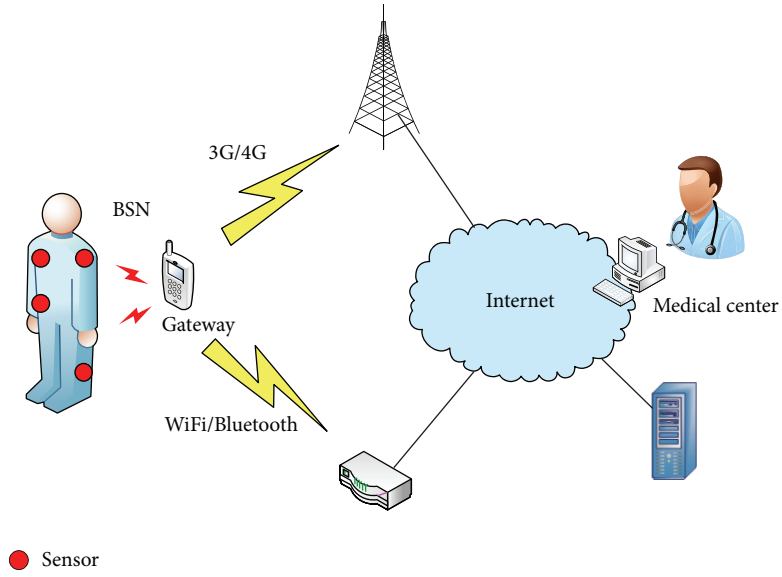


Figure 1: BSN model.

Confidentiality. Data regarding patients' state should be only accessible to authorized entities. In this context, this implies that only the BSN's nodes should be able to interpret the sensed data.

Authentication. The BSN's nodes should be able to verify the source of any received data.

Integrity. Data should not be modified by an unauthorized entity, or at least BSN's nodes should be able to detect that data has been altered.

Availability. Data and device information should be accessible upon request by authorized entities. The human body is a highly dynamic physical environment where wireless channel properties constantly change. Besides, these communications can be severely affected by interferences caused by electronic devices in the proximity of the BSN.

The first three security goals can be easily achieved by means of classical cryptographic tools in conventional networks. However, the limited capabilities of body sensors may prevent from applying them to BSNs. Besides, traditional cryptographic tools cannot prevent disruption of the network services due to interferences, no matter whether they are intentional, for example, a Denial of Service (DoS) attack, or not. Given the relevance of the data sent by body sensors, there is clearly a need for mechanisms to maximize the availability of such networks.

The integration of CR technology [9–11] into BSNs, leading to the concept of cognitive body sensor networks (CBSNs) [12], can significantly improve availability by allowing the nodes to select the best channel at any moment and avoid the harmful effect of interferences. CRs exchange sensed data about channel availability and jointly agree to switch to a new channel when the channel being in use becomes unavailable.

Note that if an attacker manages to eavesdrop channel availability data, it can take advantage of it to perform a new attack on the new channel of operation, thus preventing the network from using an available channel and leading the network to a DoS [13]. Channel switching, if unpredictable, renders DoS attacks more difficult since the attacker must jam every possible transmission channel. Traditional encryption and authentication of exchanged data may help to hide channel switching decisions from external attackers but entail an additional cost that cannot be assumed by heavily constrained devices such as IMDs.

In this paper we present a protocol to protect the process of channel selection in CR-based BSNs. The main goal is to maximize the availability of the network, thus ensuring that patients' data such as blood pressure, heart rate, and temperature will successfully be delivered to a gateway (nonstop monitoring of patients). The protocol makes use of lightweight encryption and authentication primitives specifically suited for constrained devices such as body sensors.

The main contributions of this paper can be summarized as follows.

(i) We apply CR technology into BSNs in order to maximize the availability of services in such networks. Because CRs are able to sense the medium and select the best transmission channel at any moment, the effect of interferences or DoS attacks can be mitigated. In a conventional network, such phenomena would interrupt communications within the BSNs. In a CBSN, the nodes can switch to a new channel whenever the channel in use becomes unavailable.

(ii) We propose a method, suited to constrained devices as body sensors, to secure the exchange of channel availability information and prevent an attacker from eavesdropping such data, thus diminishing the probability of a successful DoS attack.

(iii) We provide a security analysis of the proposed method and derive the time period during which the cryptographic material remains secure.

(iv) The proposed method is compared to other approaches based on traditional cryptographic primitives in terms of energy consumption and CPU usage.

The rest of this document is structured as follows. In Section 2 we review the state of the art on security in BSNs. Section 3 describes the BSN model considered in this work and its potential threats. A lightweight method to secure the process of channel selection in a BSN is presented in Section 4. Sections 5 and 6 present a security analysis of the proposed method and a comparison with existing approaches in terms of resources consumption. Finally, in Section 7 we provide the conclusions of this work.

2. Related Work

To date, research on security in BSNs has mainly focused on protecting data stored at the network nodes from unauthorized access and providing authentication and confidentiality to the communications among the BSN devices. In the following, we provide an overview of the proposals that can be found in the literature.

Many proposed authentication methods are based on biometrics, that is, relying on measurements of physiological values (PVs) [14], such as heart rate, blood pressure, or temperature, in order to establish trust and generate key material. The main idea is ensuring access to sensors only to those devices in physical contact with the patient. The advantage of these methods is that the key source is hard for an attacker to predict without physical access to the patient and also ensures forward-security, because PVs change over time. The main challenge, however, is how to achieve successful authentication among authorized devices when the PV measured by each one is not exactly the same, either due to measurement errors or due to the fact that different devices measure a given PV at different time instants.

Authentication by means of distance-bounding protocols was proposed in several works [15, 16]. This technique provides a very weak mutual authentication between two devices based on measuring the transmission time between them. The rationale behind these protocols is that a legitimate device must be closer than a given distance. As a consequence, they are vulnerable to injection attacks as long as the attacker is close enough to the patient bearing the sensors, for example, by means of a hug.

In [17], the authors presented a protocol based on identity-based encryption (IBE). IBE systems are public key cryptosystems that allow any device to generate a public key from a known identity value such as the sensor ID and require the existence of a trusted third party called the private key generator (PKG) to generate the corresponding private key. To reduce the burden of key generation and encryption/decryption introduced by traditional public key cryptography, the authors proposed to use elliptic curve cryptography (ECC), which provides public key primitives suitable for constrained devices as sensors in BSNs. Despite it, it is still more expensive in terms of resource consumption than approaches based on symmetric cryptography.

In order to preserve user's privacy, a number of works proposed the use of symmetric encryption based on the AES (Advanced Encryption Standard) algorithm [18–20]. Many, such as the one in [19], proposed to use AES with CCM mode of operation, that is to say, AES counter (CTR) mode for data encryption and AES cipher-block-chaining message authentication code (CBC-MAC) for message authentication. The main advantage of this mode is that the same key can be used for authentication and for encryption without compromising security and there is no need for rekeying as long as the number of devices is fixed. As a drawback, the added cost of encryption/decryption and, especially, the costs due to the transmission overheads cannot be neglected in BSNs, where every step forward in resources' saving is of paramount importance. In this line, the authors in [20] presented an in-network mechanism that mimics the AES algorithm and greatly reduces the costs of decryption while they claim achieving the same level of security.

All the above-mentioned proposals approach the problem of protecting patient's data from unauthorized access, modification, or forgery but cannot effectively deal with DoS attacks. Such a protection can be achieved by making use of CR devices that collaboratively switch to another frequency band [11, 21, 22] if the signal-to-noise ratio of the current one is below the required value. Furthermore, it is also necessary to protect the exchanged sensing data in order to prevent an attacker from eavesdropping data and get the next channel to be used in the network. Note that this information may allow an attacker to rapidly perform a DoS attack in the new channel.

In this work, we present a lightweight and secure method that makes use of CR technology for improving the availability of the system, that is, ensuring that the communication between the body sensor nodes will be available even under the presence of unintentional or intentional interferences. The application of CR technology into body sensor networks was already proposed in previous works [23, 24]. However, to the best of our knowledge, none of them addressed security topics.

In [25, 26], several methods for securing spectrum sensing mechanisms were discussed, but they are not suited for heavily constrained devices such as body sensors.

In [27], the authors aimed to improve the availability of a BSN by means of a cross-layer multihop protocol that dealt with routing of data. This scheme, however, can be applied only to multihop BSNs where the path between two given nodes is established according to the connectivity among the nodes. In this approach, nodes make use of several paths but one single channel and thus are more vulnerable to attacks such as jamming than CR-based networks.

3. Network Model and Threats

In this work, we have considered a BSN composed of a set of sensor nodes where all of them can act as sinks, collecting/storing data from other sensors and potentially

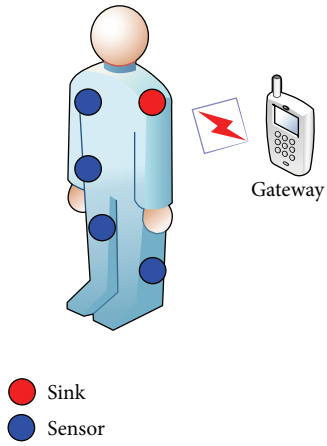


Figure 2: Communication between sensors and the gateway.

transmitting these data to an external gateway if required (see Figure 2). Although this approach introduces some overhead due to the fact that data must be shared among all sensors, it improves network availability and robustness against data loss and fairly distributes energy consumption among all sensors. Also, it makes the process of gathering by the gateway easy, which can connect to any of the BSN nodes to get all the information.

As previously mentioned, we also assume that sensors have cognitive capabilities; that is, they form a CBSN and are able to identify free spectrum bands and adapt their transmission parameters accordingly. Spectrum sensing can be performed by each node on an individual basis or cooperatively. As the latter increases the probability of detection due to space diversity [28], we have adopted such an approach in this work.

In cooperative spectrum sensing, each sensor senses the medium and exchanges its observations with the other members of the network in order to agree on a given channel for data transmission/reception. However, these control data are exposed to many attacks [13], such as packet injection, eavesdropping, or Denial of Service (DoS). Next, we describe the attacker model and the specific attacks that can be executed against CBSNs.

3.1. Attacker Model. In this work we focus on outsiders, that is, external attackers that do not share any cryptographic content with the gateway or the victim's sensor nodes. If the attacker nodes are part of the CBSN, they will have access to the keying material and therefore will be able to successfully eavesdrop and inject data. In any case, the design of a mechanism to counteract this threat is out of the scope of this work.

In the context of CBSNs, we can classify adversaries according to the following criteria:

(i) *Active or passive*: a passive attacker can only eavesdrop data, thus being able to access patient's data and violating his/her privacy. In its turn, an active attacker aims at injecting or modifying data in order to send fake reports on the state of the patient.

(ii) *Type of attack* includes the following:

(a) eavesdropping: unauthorized access to stored data or to transmitted data among the CBSN devices, thus violating the privacy of the patient,

(b) modification/injection: an attacker that may alter the content of a packet transmitted by a sensor or impersonate a sensor by forging a packet; these attacks can be executed due to lack of authentication and violate the integrity of the CBSN communications,

(c) packet replay: an attacker that may capture a packet that was previously sent by a sensor of the network. Regardless of the fact that the CBSN is using authentication mechanisms or not, the packet will be accepted by the networks if antireplay mechanisms are not provided,

(d) jamming: the adversary that disrupts the CBSN communications by generating interfering signals.

(iii) *Intentional or unintentional*: the adversary can be an external entity willing to cause damage to the communications among sensors and the gateway or can be an entity that unintentionally is causing interferences to those communications. As an example, the patient of interest could be near another patient with wearable sensors, which could inject fake reports if data is not properly authenticated. Examples of unintentional attacks could take place in a situation where two patients bearing body sensors are hugging and unconsciously exchange data. Or the patient could be near a relative who is visiting him/her at the hospital and carries any electronic device that causes interferences to the CBSN.

It is important to remark that, in a CBSN where sensor nodes establish communications using different channels over time, these attacks can be extended to the control data exchange among the devices of the CBSN. As an example, an attacker may forge a report regarding the availability of the channels, thus leading the CBSN to select a channel that is suffering from high interferences or that is currently being used by another service. Note that this attack can lead to a DoS and the failure of the system in monitoring the patient's status. In its turn, eavesdropping of the control channel allows an attacker to have knowledge of the channels to be used by the CBSN. The attacker could take advantage of this situation in order to easily disrupt the communications in the network by performing a new DoS attack every time the CBSN switches to a new channel.

The implementation of security mechanisms in a CBSN [12] to counteract these attacks is specially challenging due to the limited capabilities of CBSN's nodes. In the following section, we describe a simple method to secure the process of channel selection in CBSNs. The proposed mechanism is suited for networks with extremely constrained-resources devices, since it makes use of lightweight cryptographic functions and minimizes the added transmission/reception overhead.

4. Securing Sensing Data and Channel Selection in CBSNs

In the following we present a mechanism for securing the exchange of sensing data and the channel selection process in CBSNs. Section 4.1 outlines the assumptions considered in this work regarding the network model and, in Section 4.2, we describe the protocol operation. For ease of understanding, we present the terminology used along this section as follows:

CTR_M: medium-term session counter (m bits),

CTR_S: short-term session counter (m bits),

D_i^u: data sensed by node u during period i (l bits),

ID^u: link-layer identifier of node u (m bits),

K_i^u: keystream to encrypt and authenticate data for node u during period i (r bits),

KM: keying master,

l: length of the data sensed by a given node during a given period,

m: length of the hash output and all the secrets,

N: number of nodes in the network,

p: number of keystreams K_i^u obtained from a S^u ($p = m/r$), defining the number of sensing periods before updating S^u,

r: length of the keystreams K_i^u, which must be a divisor of m,

S_L: long-term globally shared secret (m-bits),

S_M: medium-term globally shared secret (m-bits),

$S_{s,i}$: long-term secret shared between the KM and node i; it is used to update S_L in case it is compromised,

S^u: short-term shared secret with node u.

4.1. Assumptions. Although the proposed protocol is designed to be implemented in heavily constrained devices, we work under the assumption that such devices have at least the following capabilities:

(i) Compute a hash function with an output length of m bits.

(ii) Temporally store in its random access memory at least $m \cdot (N + 3)$ bits, with N the number of nodes in the network. As we detail later in Section 4.2, each node must keep a short-term shared secret for each of the N nodes in the network (including itself) and three more long-term and medium-term secrets, each one with length of m bits.

(iii) Sensor nodes use a synchronization protocol that will be used to share a global short-term session counter and a medium-term session counter among all nodes (see Section 4.2). Given the low transmission rate of sensor networks, existing synchronization schemes [29] provide enough precision for this purpose. We assume that the chosen protocol provides recovery methods upon loss of synchronization. How synchronization is achieved will strongly depend on the chosen protocol, but if the latter requires a master node for providing synchronization, the gateway of the BSN could play this role.

To the best of our knowledge, the former requirement can be assumed even in very constrained devices. As shown in [30], there are several lightweight hash functions that can be integrated into a sensor mote. The latter may not be harder to achieve. As detailed in Section 4.2, during every sensing period each node stores one secret per member of the network, a globally shared secret, and two counters, all of them with the same length m as the hash output. If we consider a typical hash function with an output of 128 or 256 bits and a network with tens to hundreds of sensors, the RAM requirements for sensor nodes are just bounded to a few tens of kilobytes.

4.2. Protocol Operation. Before deploying the CBSN, every sensor node must be preloaded by a keying master (KM) with the following data:

(1) The set of channels that the sensor will have to sense in the cooperative sensing process.

(2) A long-term and globally shared secret S_L of m bits (the hash output length).

(3) A long-term secret $S_{s,i}$ shared between the KM and node i that will be used to update the globally shared secret S_L in case it is compromised.

The KM is an external device, which is not a member of the BSN. Typically, this role is played by the device responsible for gathering data from the sensors or gateway (e.g., a smart phone or a tablet).

Upon deployment of the network, every node derives a medium-term globally shared secret S_M by hashing the XOR of the long-term secret S_L and a counter. The generation process of S_M is clearly depicted in Figure 3. This process is periodically repeated with an updated value of the medium-term counter in order to protect the secret against a potential attacker. Details about how often this process should be carried out and the attacker capabilities are provided in Section 5.

As shown in Figure 4, each node generates a set of random sequences of m bits: one for the node itself and one for each other node in the network. These random sequences, S^u, with u the node identifier, are obtained by hashing the XOR of the link-layer identifier of the node ID^u, the medium-term shared secret S_M, and a short-term session counter CTR_S.

Therefore, our proposal makes use of three types of shared secrets:

(i) A short-term per-node shared secret S^u (one per each node in the network) used for encryption, decryption, and authentication of data.

(ii) A medium-term globally shared secret S_M that is used to derive the short-term per-node shared secrets S^u.

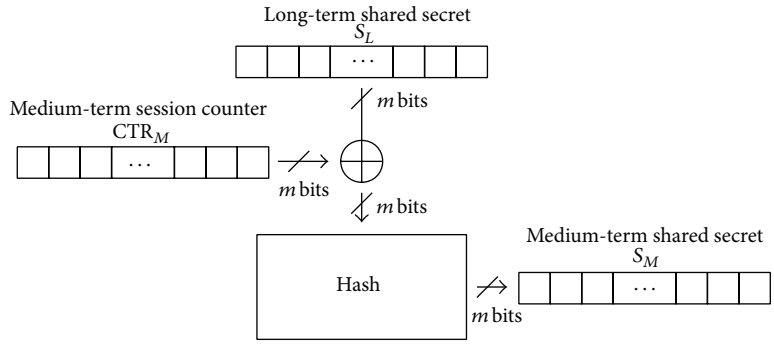


Figure 3: Generation of the medium-term globally shared secret S_M.

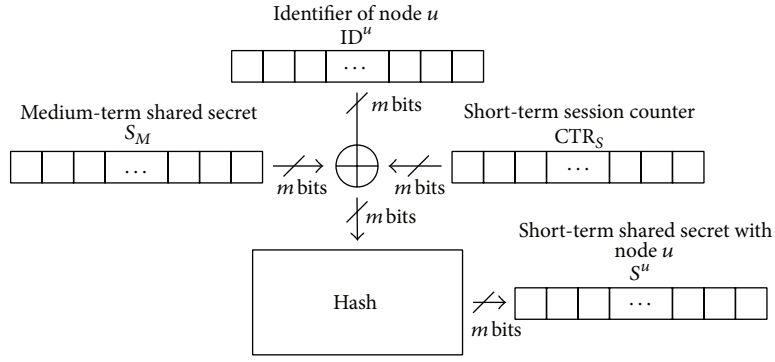


Figure 4: Generation of the short-term shared secret S^u for node u.

(iii) A long-term globally shared secret that is used to derive a new S_M when the current one is about to expire.

As clearly denoted in Figure 5, each sequence S^u is divided into p fragments of r bits, which we will be denoted as K_i^u, each one being used as keystream to encrypt and authenticate data for node u in period i. As per this behavior, a new short-term shared secret must be derived every p sensing period.

When a node performs spectrum sensing, it generates a binary sequence D_i^u of l bits that stores the availability of the different channels. The length of such sequence l will depend on the number of bits used to code the state of each channel and the number of channels. As an example, the simplest way would be to use just a single bit for coding each channel, with value "0" if the channel is occupied and "1" otherwise. If more precise information about the quality of channels is needed (i.e., high, medium, low, and very low quality), more bits can be used to code the channel state.

During a sensing period i, each node must send to its neighbors its own sensing information but also it must process the information received from its neighbors to reach a joint decision.

In order to send its own sensing information, node u will make use of the corresponding keystream K_i^u: the first l bits of the keystream will be used to encrypt channel information D_i^u by means of a XOR addition; the remaining $r - l$ bits are left unchanged and will be used to provide message authentication, as illustrated in Figure 5. The resulting sequence C_i^u will be sent to all the other nodes.

To verify the authenticity and decrypt the content of the packets that have been sent by a given neighbor u, a node will XOR the sequence C_i^u of the received packet with the keystream K_u^i, as depicted in Figure 6. If the last $r - l$ bits of the resulting sequence are not all 0 s, the authentication fails and the entire packet is discarded. Otherwise, channel information can be recovered from the first l bits resulting from the XOR addition.

The above described process is applied for each neighboring node u. Then, the channel reported by a larger number of neighbors will be selected for the operation of the network. Note that because more than one channel may be reported by the same amount of nodes, a tie-break mechanism is needed to guarantee that the process leads to equal results in all nodes. One simple approach that could be used is to select the channel with the highest identifier. However, this would lead to a lower usage of channels with lower identifiers and therefore to providing the attacker with valuable information about channel usage in the CBSN. As a consequence, we propose to use a tie-break method that relies on the format of D_i^u.

Recall that a fundamental characteristic of this protocol is that there is no central entity that is known and trusted by all sensors. This makes the protocol suitable for unattended scenarios, and it also makes it more efficient in terms of data transmitted through the network, because no information is sent regarding which channels have to be sensed or which channel is finally selected. Instead, sensors are deployed with all the information needed to perform the sensing in

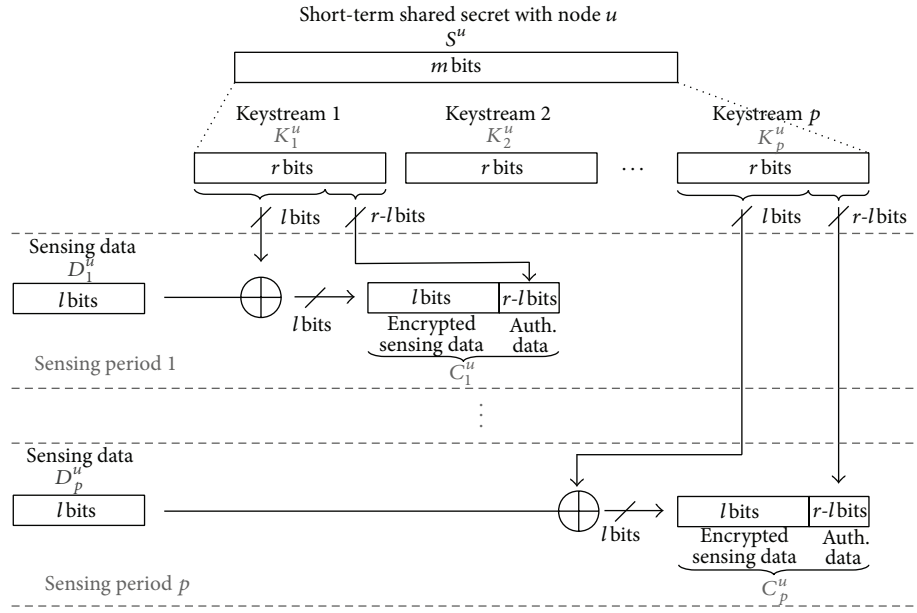


Figure 5: Encrypting and authenticating sensing data.

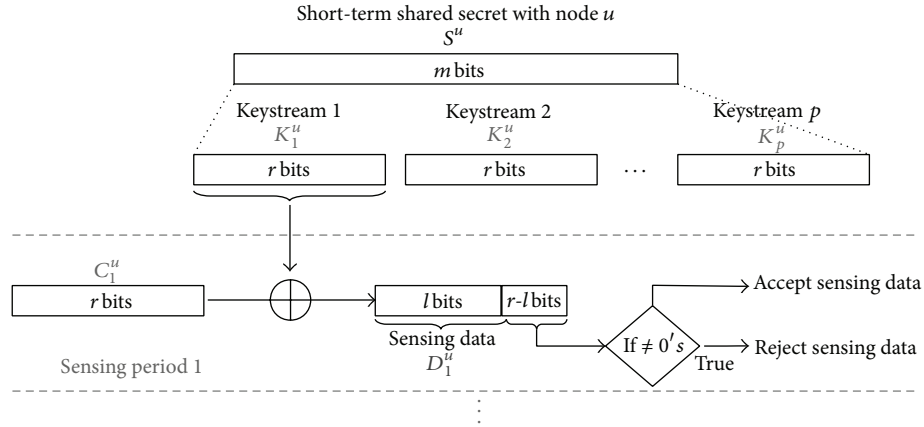


Figure 6: Decrypting sensing data.

a distributed way and make a joint decision autonomously. Thus, there is no need for additional mechanisms to be used when a new node joins the network. In this case, the new node needs to synchronize with the rest of the members to get the proper value of the session counters by making use of the corresponding protocol. However, when a node is expelled from the network because it has been compromised, new cryptographic material must be generated and distributed among the remaining nodes. The KM is responsible for triggering this process and communicates with each sensor node to update the shared long-term secret S_L. Note that because the KM shares a different secret $S_{s,i}$ with each node i, it can securely distribute the new value of S_L. Upon reception of S_L, each node should perform again the initialization process described at the beginning of this section.

5. Security Analysis

The security of the proposed method relies on the shared secrets used to derive the keys and perform encryption and authentication of channel availability data. As long as these secrets are not compromised, data confidentiality can be ensured; that is, an attacker might not be able to get the list of channels to be used in the CBSN. Besides, the method must prevent an attacker from injecting fake data into the system. These issues are discussed as follows. In Section 5.1, we analyze how often the shared secrets should be updated in order to guarantee a proper protection against cryptanalysis; next, in Section 5.2, we evaluate the packet authentication method used in our proposal in terms of probability of bypassing the authentication check.

5.1. Shared Secrets Lifetime. As previously mentioned in Section 3.1, for this analysis, we are assuming that attacks come from external entities and therefore attackers are not able to obtain the cryptographic material that is stored in the body sensors. In the context of this proposal, the lifetime of each of the shared secrets is the interval in which these secrets are considered computationally safe against cryptanalysis, that is, their cryptoperiod.

The cryptoperiod straightly depends on the chosen cryptographic protocols, the length of the secrets themselves, and the amount of times they are used. The more a given secret is used, the shorter its cryptoperiod is, as an attacker gets more information about this secret and therefore the probability of a successful cryptanalysis increases. In fact, cryptoperiod is defined more in terms of the number of times a given secret or key is reused (the amount of ciphertext exposed to an attacker for a given secret/key) than as a given time period, which strongly depends on the transmission rate of the sensor nodes.

Recall the three types of shared secrets used in the proposed method:

(i) *Short-term per-node shared secrets*: one secret S^u per source node that is used to lightweight encrypt, decrypt, and authenticate the channels' sensed data.

(ii) *Medium-term globally shared secrets*: globally shared secret S_M that is used to derive the short-term per-node shared secrets S^u.

(iii) *Long-term globally shared secret*: this being the initially preloaded secret S_L that is used to derive a new medium-term globally shared secret S_M when the current one is about to expire.

As clearly denoted in Figure 5, our approach operates, in some manner, as an additive stream cipher. It is well known that stream ciphers are considered to be secure as long as the key is never reused and, thus, our cipher will be secure if a given value S^u is not repeated. As a result, S^u must be updated every $p = m/r$ sensing period, with p the renewal period, m the length of the shared secret S^u, and r the amount of transmitted bits (sensing data) in a sensing period that are encrypted with S^u.

Recall that, in our proposal, the per-node key used for encryption S^u is generated by means of a hash function. A second requirement is that this function must be cryptographically secure. Note that if the hash function does not accomplish it, an attacker might be able to reverse it, that is, to get the input of the hash function given an output, meaning that, in our proposal, an attacker would be able to recover the value of the medium-term globally shared secret S_M (see Figure 4).

A cryptographically secure hash function with an output of m bits can offer a security level of 2^m operations against preimage attacks and $2^{m/2}$ against collision attacks. Generally speaking, a minimum output of 128 bits is required in order to provide a high level of security for most applications but shorter lengths are accepted if the number of generated messages in a given period is limited, as it is the case of low-rate networks. In Section 6, we propose several lightweight hash candidates with an output of 128 bits; that is to say, we can assume that it is computationally unfeasible for an attacker to invert the hash function and thus to predict the value of S^M as long as it is updated before exceeding its cryptoperiod, which has an upper bound of $2^{m/2} = 2^{64}$ uses.

The long-term globally shared secret S_L is only used to update the current medium-term globally shared secret S_M. Because S_M is not updated very often, it is very unlikely that an attacker manages to obtain several values of S_M to reverse the hash function and recover S_L. As a result, we can assume that the S_L cryptoperiod is long enough and there is no need to update the secret during the nodes' lifetime.

5.2. Authentication. A cryptogram C_i^u of sensing data contains an authentication field of 16 bits that is checked upon reception (see Figure 6). Consequently, an attacker has a chance of 1 in 2^{16} of guessing the next authentication field, which allows it to forge a valid authentication field and inject fake data. Note that this attack can lead the CBSN to wrong decisions about the availability of the spectrum.

If the attacker repeatedly attempts to send valid ciphertexts, it may succeed after 2^{15} attempts, in average. Because the attacker does not know S^u, the authentication field appears to it as a random stream and therefore it must select a fake authentication field at random. Besides, the attacker cannot determine whether a given ciphertext has been accepted or rejected because the receiver does not acknowledge the reception of such packets to the emitter. Otherwise, the attacker could take advantage of this information in order to guess a valid authentication field in a faster way.

In conventional networks, 2^{15} packets may seem an extremely low number but it may provide an adequate level of security in CBSNs. In these networks, the attacker can only send fake packets during the sensing periods, which is in the order of a few milliseconds in most cognitive scenarios [31]. Moreover, as previously stated in Section 1, transmission rates in BSNs are considerably low, with values usually ranging from tens to a few hundred of kilobits per second.

As an example, let us consider a 1 Mbps link, a sensing period of 10 ms, and a packet size of 10 bytes (which is clearly bigger than the typical packet size in sensor networks). Given these parameters, an attacker would only be able to send 125 packets at most in every sensing period. That is to say, the attacker would need an average of 262.144 sensing periods to send a fake packet and pass the authentication check.

6. Cost Evaluation and Comparison with Other Approaches

In this section, we evaluate the cost of our proposal in terms of energy consumption due to transmission overhead and computational cost and compare its performance with the most common approach adopted in sensor networks [32], which is providing authentication and/or encryption of the channel sensing data by means of using standard block ciphers. As is well known, block ciphers have as input the message to be encrypted or authenticated, which is divided into several blocks of fix length and a key. Both the block

length and the key length depend on the algorithm being used. Regardless of the algorithm, block ciphers can be used in several modes of operation depending on the service to be provided, that is, encryption only, authentication only, or encryption/authentication. Generally, the following modes of operation are applied.

Authentication. CBC-MAC is a block cipher mode for generating message authentication codes. The message to be authenticated is divided into several blocks of equal size, and each block is encrypted so that the value of a given block depends on the encryption of the previous block. The final output of the cipher, that is, the message authentication code or CBC-MAC, is the result of encrypting the last block of the message. When the input of the cipher is shorter than the block size (as it is usually the case in sensor networks), the CBC-MAC can be obtained by directly encrypting a single block, padded until the block size of the cipher is reached.

Encryption. CTR mode of operation turns a block cipher into a stream cipher, meaning that the resulting ciphertext has the same size as the input or plain text. Thus, it does not force the output length to be a multiple of the block size, as it is the case of other modes such as CBC-MAC. This property makes this mode of operation suitable for encryption in sensor networks where devices usually exchange short-length messages.

Authentication+Encryption. CCM (CTR + CBC-MAC) is a common choice for providing both encryption (CTR) and authentication (CBC-MAC) [19]. A minor variation of CCM, called CCM*, is used in the ZigBee standard [7].

In this work, we assume that Advanced Encryption Standard (AES) in CTR mode is used for encryption and AES CBC-MAC for authentication, as it is the current standard for symmetric cryptography, even in sensor nodes [33]. Currently, there are efficient hardware implementations of AES that are highly affordable.

Regarding hardware platforms, the vast majority of previous works on BSNs have used the 16-bit Texas Instruments' (TI) MSP430 and CC2540 families of microcontrollers [34]. Built around a 16-bit CPU, ultra-low-power MSP430 microcontrollers are designed for low cost and, specifically, low-power consumption embedded applications. As an example, TI's CC2540 family [35] enable robust Bluetooth low energy (BLE) network nodes to be built with low total bill-of-material (BOM) costs. BLE operates in the same spectrum range (2.400 GHz–2.4835 GHz ISM band) as classic Bluetooth technology but uses a different set of channels; instead of 79 1 MHz channels, BLE offers 40 2 MHz channels, 3 for advertising purposes and 37 for data exchange.

6.1. Transmission/Reception Overhead. In this section we analyze the overhead introduced by our proposal in terms of transmission/reception of channel availability data and compare it with the overhead exhibited when conventional approaches are used for data encryption/authentication, as explained above. We assume that all sensors are capable of sensing a given set of channels and report information about their state.

With our proposal, the minimum number of transmitted bits will depend on the number of channels that a given sensor is reporting, the number of bits used to code the state of each channel, and the length of the authentication code. As explained in Section 5.2, a length of 16 bits is enough to secure most applications in WSNs and, thus, we have assumed this value for the authentication field. This leads to a total amount of $\text{Bits}_{tx} = l + 16$ of transmitted bits, where l represents the total number of bits used to code all possible channels, and $\text{Bits}_{tx} = (n-1)\text{Bits}_{tx}$ received bits, representing the number of bits received by a given sensor from its neighbors.

Aiming to provide a fair comparison, we choose the same key length for block ciphers and for our proposal, that is to say, a 128-bit key. The transmitted bits overhead added by AES CBC-MAC authentication is 128 bits (for a semantically secure implementation also an IV or nonce must be shared between emitter and receiver, so that the overhead can be higher). Regarding encryption, the number of transmitted bits is equal to the number of bits l used to code the state of the channels, but it also requires the use of a nonce, with a length equal to half of the key length, that is, 64 bits per message.

During every sensing period, every node must transmit a packet with sensing information but also must process the packets received from its neighbors. Table 1 and Figure 7, respectively, show the transmission and reception overhead due to the secure sharing of sensing information using both standard block ciphers and our proposal. The values are provided as a function of the number of bits l used to code the state of the channels and the number of nodes N, ranging from 5 to 30. Given that the considered scenario is a body sensor network, this is more than a reasonable value, since a patient wearing more than 30 sensors may be an unlikely situation.

The reader may notice that the overhead introduced by this mechanism increases linearly with the number of nodes for both approaches. However, with the proposed method the transmission/reception overhead is considerably reduced with respect to the use of standard block ciphers while still maintaining an acceptable level of security. In fact, the more the nodes in the CBSN, the bigger the improvement introduced by the former. As we will show later, the transmission/reception savings lead to a huge saving also in energy consumption.

6.2. Computational Cost. In this section, we provide a comparison of the CPU cost in cycles due to the implementation of the cryptographic functions.

If AES is used, the total cryptographic cost per node for securing the exchange of sensing data equals the cost of one encryption and $N - 1$ decryptions. Assuming the Texas Instruments' reference AES-implementation for CC2540 microcontrollers [36], AES encryption needs 6600 cycles/block and AES decryption 8400 cycles/block.

With our proposal, the energy consumption has three components: the computation of the different sequences S_i^u with the hash function before the sensing period begins, the XOR of the keystream K_i^u with the sequence D_i^u that signals the availability of channels, and the XOR of the sequences C_i^u received from neighbors with the precomputed S_i^u. Therefore,

Table 1: Transmission overhead.

	l (bits)	Overhead (bits)
Authentication only (CBC-MAC)	16	128
	32	128
	64	128
Encryption only (CTR)	16	80
	32	96
	64	128
Authentication and encryption (CCM)	16	208
	32	224
	64	256
Authentication and encryption (our proposal)	16	32
	32	48
	64	80

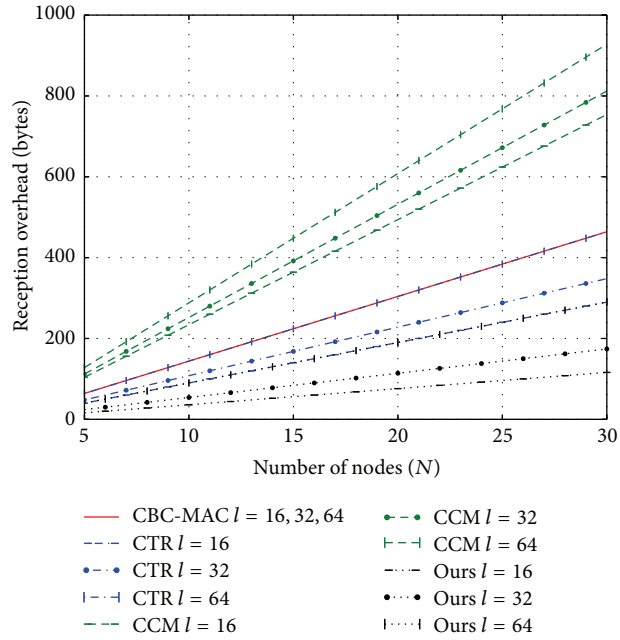


Figure 7: Reception overhead for a varying number of nodes N.

a node must compute N hashes and perform N XORs to send channel information and process the reports received from its neighbors.

As per [37] XOR operation with a MSP430 accounts for 4-5 cycles/byte. Assuming a 128-bit hash function and the worst case, every XOR in our proposals accounts for $5 \cdot 16 = 80$ cycles. As previously explained in Section 5.1 we suggest the use of a lightweight cryptographic hash function specifically suited for low-end devices with an output of 128 bits. Table 2 depicts the number of CPU cycles per block needed [38] for two potential candidates. As clearly seen in the table, computing one of these hash functions requires only a few tens of cycles/block. In the following, for this analysis we will consider the (stripped) MAME hash function, as it is a pure hash function that does not rely on a symmetric cipher and requires more CPU cycles (worst case).

Table 2: Cycles per block for different cryptographic hash functions.

Algorithm	Hash output size	Cycles/block
(Stripped) MAME	128	96
H-PRESENT-128	128	32

Taking into account the previous data, Figure 8 shows the CPU cycles consumed with both our proposal (with a MAME hash function) and standard AES-128 security. It can be clearly seen that our proposal scales much better with the number of nodes while still providing an appropriate level of security. We do not provide values for the process time, that is, the time needed for key generation, encryption, decryption, and data authentication, but the number of CPU cycles required to execute each function. In this way, time values can be obtained for a particular sensor node according to its CPU features.

6.3. Total Energy Cost. Table 3 provides the transmission and reception energy consumption of a TI's CC2540 microcontroller for different modes and values of transmission power. The displayed values have been tested under 25°C. We do not have values for in-body conditions (≈38°C) but we present these data for reference purposes. In any case, this fact only affects the energy consumption for receiving/transmitting. Note that the total cost in terms of energy is much higher, since it should also account for duty cycles, state changes, and other parameters [39].

There is no single specific "energy per CPU cycle" value since the cycle consumption depends on the type of CPU operation. Anyway, in [34], the authors measured that the TI's MSP430F1611 consumes energy at an average of 0.72 nJ per clock cycle, and we have adopted such value in our study.

Figure 9 shows the total average energy consumption, as a function of the number of neighboring sensor nodes and the number l of bits used to code the channels, for the proposed mechanism and standard approaches: CCM (authentication and encryption), CTR (encryption only), and CBC-MAC (authentication only). We have assumed standard reception and short-range transmission of −6 dBm (see Table 3).

As clearly denoted in the figure, our method only requires a few tens of μJ regardless of the number of sensor nodes, while AES-based security requires higher values of energy ranging from 35 μJ to almost 240 μJ when encryption and authentication are provided and for 30 sensor nodes. The more the number of sensor nodes, the bigger the improvement introduced by our proposal.

It must be remarked, however, that the purpose of this figure is to provide reference values to be taken into account for future implementations. Besides, the level of security provided by our method is lower than AES-based methods but still is more than adequate given the features of CBSNs (transmission rate, number of sent messages, etc.) and given the fact that the data we are trying to protect are just a limited number of potential channels to be used for operation of the network.

Table 3: Current/energy consumption for RX/TX tested on Texas Instruments CC2540 EM with $T_A = 25^{\circ}$C with no peripherals active and low MCU activity at 250 kHz.

Test conditions	Current	Energy/byte
RX standard	19.6 mA	58.8 nJ
RX high gain	22.1 mA	66.3 nJ
TX −23 dBm	21.1 mA	63.3 nJ
TX −6 dBm	23.8 mA	71.4 nJ
TX 0 dBm	27 mA	81 nJ
TX 4 dBm	31.6 mA	94.8 nJ

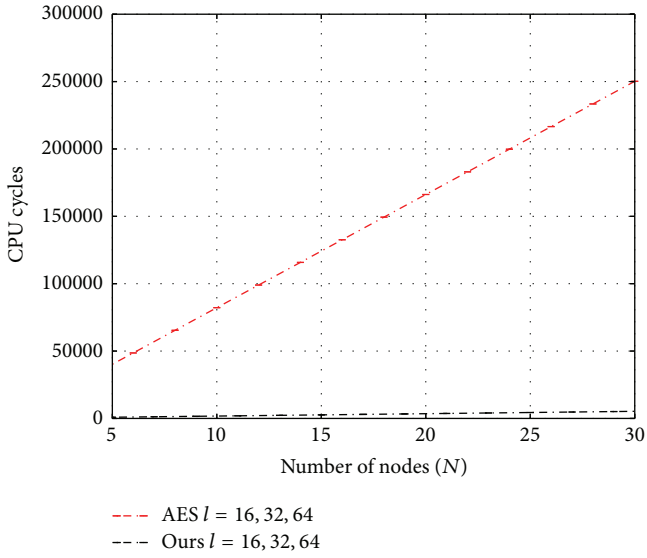


Figure 8: Added CPU cycles for a secure exchange of sensing data.

Indeed, this mechanism introduces some overhead due to spectrum sensing and sharing of channel information and, as we pointed out above, the overhead increases linearly with the number of nodes in the network. The synchronization protocol adds some overhead too, but the increase will strongly depend on the chosen protocol. In [29], some protocols with high energy efficiency are referenced, which could be used in our proposal.

Despite it, we claim that it is definitely worth introducing this overhead to increase the availability of the network and make it robust to potential interferences and DoS attacks. Under these undesired situations, the current channel used by the CBSN may become unavailable, but the proposed method allows the nodes to securely agree on a new channel of operation and rapidly resume their transmissions. It must be remarked that securing channel availability information may prevent or at least diminished the effect of further DoS attacks when switching to a new channel.

We do not quantify the benefits of applying our method in terms of attack mitigation because it strongly depends on the capabilities of the attacker (time required for sensing each channel, number of channels that can sense, etc.). As a future work, it would be interesting to estimate the improvement achieved by our approach in terms of throughput of the

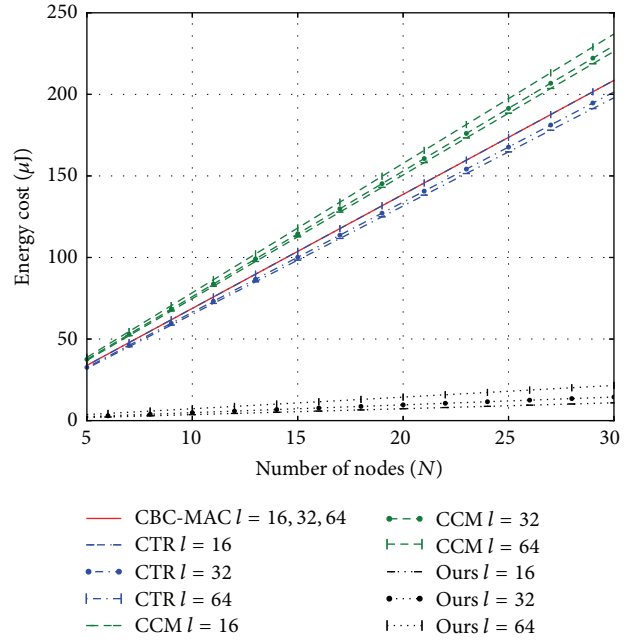


Figure 9: Added energy costs for a TI's MSP430F1611 with a TI's CC2540 microcontroller.

CBSNs connections and the tradeoff between benefits and overhead.

7. Conclusions

Body sensor networks (BSNs) emerge as an optimal solution for ensuring constant and remote monitoring of the health status in patients. Recent advances in technology have made it possible to deploy a network of tiny sensors over the human body, and even in body, which can measure vital signs such as temperature, heart rate, or the level of glucose and report these data to medical personnel.

Guaranteeing the availability of such communications is a must as long as connectivity losses during emergency situations may prevent a patient from immediately receiving medical assistance and may end up in catastrophic results.

A new network paradigm, known as cognitive body sensor networks (CBSNs), could mitigate this threat by allowing body sensors to operate in a wide range of frequencies and adapt its transmission parameters according to highly dynamic environment conditions. However, this would come at the expense of implementing cooperative spectrum sensing mechanisms that allow sensors to exchange information about channel quality and availability. As a consequence, CBSNs might become vulnerable to specific attacks that are targeted to these mechanisms.

In this paper we presented a novel and simple method to secure the sensing process in a CBSN and improve its availability. The method relies on cryptographic primitives that require a minimum amount of memory and low energy consumption, thus being more suited for devices with limited resources than traditional approaches. It offers authentication

and encryption of control data shared by the sensors in the CBSN to agree on a given channel.

Our proposal was analyzed in terms of security and we showed that although it does not provide the same level of security as AES-based encryption and authentication, it is still sufficient for low packet rate networks such as CBSNs. The provided results also showed that our method outperforms existing approaches in terms of transmission/reception overhead and number of CPU cycles needed, particularly as the number of sensor nodes increases. For typical microcontrollers as CC2540 and MSP430, the improvement in energy consumption clearly justifies the use of the proposed method against AES-based mechanisms in constrained networks such as CBSNs, in which maximizing the network life is extremely important.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work has been partially supported by the spanish government under grant TEC2011-22746 "TAMESIS" and by the Ministry of Economy and Competitiveness through the projects CO-PRIVACY (TIN2011-27076-C03-02) and SMARTGLACIS (TIN2014-57364-C2-2-R).

References

[1] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[2] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[3] 802.15.6-2012—IEEE Standard for Local and metropolitan area networks—Part 15.6: Wireless Body Area Networks, 2012, http://standards.ieee.org/getieee802/download/802.15.6-2012.pdf.

[4] Bluetooth Low Energy (LE), June 2014, http://www.bluetooth.com/Pages/low-energy-tech-info.aspx.

[5] The ANT+ Alliance, 2014, http://www.thisisant.com.

[6] Wi-Fi Alliance, June 2014, http://www.wi-fi.org/.

[7] Zigbee Alliance, June 2014, http://www.zigbee.org/.

[8] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: security and privacy in implantable medical devices and body area networks," in *Proceedings of the 35th IEEE Symposium on Security and Privacy (SP '14)*, pp. 524–539, San Jose, Calif , USA, May 2014.

[9] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[10] B. Wang and K. J. R. Liu, "Advances in cognitive radio networks: a survey," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 5–23, 2011.

[11] Y. Xu, J. Wang, Q. Wu, A. Anpalagan, and Y.-D. Yao, "Opportunistic spectrum access in unknown dynamic environment: a game-theoretic stochastic learning solution," *IEEE Transactions on Wireless Communications*, vol. 11, no. 4, pp. 1380–1391, 2012.

[12] D. Cavalcanti, S. Das, J. Wang, and K. Challapali, "Cognitive radio based wireless sensor networks," in *Proceedings of the 17th International Conference on Computer Communications and Networks (ICCCN '08)*, pp. 1–6, August 2008.

[13] O. León, J. Hernández-Serrano, and M. Soriano, "Securing cognitive radio networks," *International Journal of Communication Systems*, vol. 23, no. 5, pp. 633–652, 2010.

[14] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-Heart (H2H): authentication for implanted medical devices," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '13)*, pp. 1099–1111, ACM, Berlin, Germany, November 2013.

[15] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, pp. 410–419, Chicago, Ill, USA, November 2009.

[16] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: body area network authentication exploiting channel characteristics," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1803–1816, 2013.

[17] C. C. Tan, S. Zhong, H. Wang, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in *Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec '08)*, pp. 148–153, April 2008.

[18] O. Garcia-Morchon, T. Falck, T. Heer, and K. Wehrle, "Security for pervasive medical sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '09)*, pp. 1–10, Toronto, Canada, July 2009.

[19] G. Selimis, L. Huang, F. Massé et al., "A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design," *Journal of Medical Systems*, vol. 35, no. 5, pp. 1289–1298, 2011.

[20] Y. Yan and T. Shu, "Energy-efficient In-network encryption/decryption for wireless body area sensor networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '14)*, pp. 2442–2447, IEEE, Austin, Tex, USA, December 2014.

[21] Y. Xu, A. Anpalagan, Q. Wu, L. Shen, Z. Gao, and J. Wang, "Decision-theoretic distributed channel selection for opportunistic spectrum access: strategies, challenges and solutions," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 1689–1713, 2013.

[22] Y. Xu, J. Wang, Q. Wu, A. Anpalagan, and Y.-D. Yao, "Opportunistic spectrum access in cognitive radio networks: global optimization using local interaction games," *IEEE Journal on Selected Topics in Signal Processing*, vol. 6, no. 2, pp. 180–194, 2012.

[23] R. Chavez-Santiago, K. E. Nolan, O. Holland et al., "Cognitive radio for medical body area networks using ultra wideband," *IEEE Wireless Communications*, vol. 19, no. 4, pp. 74–81, 2012.

[24] A. R. Syed and K.-L. A. Yau, "On cognitive radio-based wireless body area networks for medical applications," in *Prceedings of the 1st IEEE Symposium on Computational Intelligence in Healthcare and e-Health (CICARE '13)*, pp. 51–57, Singapore, April 2013.

[25] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08)*, pp. 1876–1884, IEEE, Phoenix, Ariz, USA, April 2008.

[26] H. Rifà-Pous, M. J. Blasco, and C. Garrigues, "Review of robust cooperative spectrum sensing techniques for cognitive radio networks," *Wireless Personal Communications*, vol. 67, no. 2, pp. 175–198, 2012.

[27] B. Braem, B. Latré, C. Blondia, I. Moerman, and P. Demeester, "Analyzing and improving reliability in multi-hop body sensor networks," *International Journal on Advances in Internet Technology*, vol. 2, no. 1, pp. 152–161, 2009.

[28] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: a survey," *Physical Communication*, vol. 4, no. 1, pp. 40–62, 2011.

[29] B. Sundararaman, U. Buy, and A. D. Kshemkalyani, "Clock synchronization for wireless sensor networks: a survey," *Ad Hoc Networks*, vol. 3, no. 3, pp. 281–323, 2005.

[30] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, and Y. Seurin, "Hash functions and RFID tags: mind the gap," in *Cryptographic Hardware and Embedded Systems—CHES 2008: 10th International Workshop, Washington, D.C., USA, August 10–13, 2008. Proceedings*, vol. 5154 of *Lecture Notes in Computer Science*, pp. 283–299, Springer, Berlin, Germany, 2008.

[31] C. Cordeiro, K. Challapali, D. Birru, and N. Sai Shankar, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05)*, pp. 328–337, Baltimore, Md, USA, November 2005.

[32] S. Ullah, H. Higgins, B. Braem et al., "A comprehensive survey of wireless body area networks on PHY, MAC, and network layers solutions," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[33] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proceedings of the ACM Workshop on Wireless Security (WiSe '04)*, pp. 32–42, Philadelphia, Pa, USA, October 2004.

[34] M. Pajic, Z. Jiang, I. Lee, O. Sokolsky, and R. Mangharam, "From verification to implementation: a model translation tool and a pacemaker case study," in *Proceedings of the 18th IEEE Real Time and Embedded Technology and Applications Symposium (RTAS '12)*, pp. 173–184, Beijing, China, April 2012.

[35] CC2540 2.4-GHz Bluetooth low energy System-on-Chip, 2013, http://www.ti.com/lit/ds/symlink/cc2540.pdf.

[36] U. Kretzschmar, "AES128—a C implementation for encryption and decryption. MSP430 systems. ECCN 5E002 TSPA—technology/software publicly," Application Report SLAA397A, Texas Instruments, Dallas, Tex, USA, 2009, http://www.ti.com.cn/cn/lit/an/slaa397a/slaa397a.pdf.

[37] El Barquero, *Aqueronte: MSP430: Cycles and Instructions*, edited by: Aqueronte, 2011, http://unbarquero.blogspot.com.es/2011/05/msp430-cycles-and-instructions.html.

[38] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, and Y. Seurin, "Hash functions and RFID tags: mind the gap," in *Cryptographic Hardware and Embedded Systems—HES 2008*, vol. 5154 of *Lecture Notes in Computer Science*, pp. 283–299, Springer, Berlin, Germany, 2008.

[39] S. Kamath and J. Lindh, "Measuring bluetooth low energy power consumption," Application Note AN092, Texas Instruments, Dallas, TEx, USA, 2012, Version SWRA347a, http://www.ti.com/lit/an/swra347a/swra347a.pdf.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 138328, 12 pages
http://dx.doi.org/10.1155/2015/138328

Research Article

Energy-Efficient Layered Video Multicast over OFDM-Based Cognitive Radio Systems

Wenjun Xu, Shengyu Li, Yue Xu, Zhiyong Feng, and Jiaru Lin

Key Lab of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China

Correspondence should be addressed to Wenjun Xu; wjxu@bupt.edu.cn

Received 10 July 2015; Accepted 17 September 2015

Academic Editor: Miao Pan

An energy-efficient layered video multicast (LVM) scheme for "*bandwidth-hungry*" video services is studied in OFDM-based cognitive radio (CR) systems, where the video data is encoded into a base layer and several enhancement layers with the former intended for all subscribers to guarantee the basic quality of reconstructed video and the latter aiming at the quality improvement for the promising users with good channel conditions. Moreover, in order to balance user experience maximization and power consumption minimization, a novel performance metric *energy utility* (EU) is proposed to measure the sum achieved quality of reconstructed video at all subscribers when unit transmit power is consumed. Our objective is to maximize the system EU by jointly optimizing the intersession/interlayer subcarrier assignment and subsequent power allocation. For this purpose, we first perform subcarrier assignment for base layer and enhancement layers using greedy algorithm and then present an optimal power allocation algorithm to maximize the achievable EU using fractional programming. Simulation results show that the proposed algorithms can adaptively capture the state variations of licensed spectrum and dynamically adjust the video transmission to exploit the scarce spectrum and energy resources adequately. Meanwhile, the system EU obtained in our algorithms is greatly improved over traditional spectrum efficiency (SE) and energy efficiency (EE) optimization models.

1. Introduction

Recently, the fifth generation (5G) mobile wireless system has been under heated discussion [1, 2]. It is reported that the wireless traffic volume will increase by 1000-fold over the next decade [3], and hence there is an urgent need to design novel spectrum-efficient transmission paradigms. Cognitive radio (CR) [4] is one of the best technologies to improve the spectrum efficiency (SE) and has attracted many researchers' attention. The basic idea of CR is to bear data transmission among secondary users (SUs) by reusing licensed spectrum without harming the benefits of authorized users (also known as primary users, PUs). Orthogonal frequency division multiplexing (OFDM) supports a flexible spectrum management by dividing the available spectrum into fine-granularity subcarriers and hence is recognized as a promising technology for spectrum reusing [5]. As a result, it is meaningful to combine CR and OFDM together and investigate new transmission paradigm in OFDM-based CR systems.

Meanwhile, energy efficiency (EE) is also a key metric for 5G, in which energy consumption needs to be reduced on the order of several magnitudes [6]. Note that extra power consumption incurred by spectrum sensing makes the power saving issue more critical in CR systems [7, 8]. Until now, large amounts of researches have been conducted to study energy-efficient transmission in OFDM-based CR systems. For example, in our early work [9], the EE metric measured by the achieved transmission bits per Joule is adopted, and the optimal power allocation for EE maximization is derived using *fractional programming*. Subsequently, the model is improved with the minimum rate guarantee and subcarrier assignment taken into account in [10, 11], respectively. Then, the authors in [12] further consider channel uncertainty and study the EE maximization problem with a probabilistic interference control policy.

However, all these researches mentioned above focus on unicast transmission. Along with the proliferation of smart phones, mobile multimedia services, especially mobile video services, have been in the explosive growth [13]. CR can effectively alleviate the more and more serious spectrum scarcity issue and is one of the key candidate technologies in 5G. Hence, it is almost an inevitable trend to deliver the increasing popular video services in the future communication system without licensed spectrum. Even for networks which have already been allocated with some spectrum bands, integrating CR function into the networks, for example, Licensed-Assisted Access (LAA) [14], can provide more competent video transmission, improving the user experience greatly. Moreover, as secondary networks can only access the authorized spectrum opportunistically, its transmission capacity is limited by the prioritized access mode. Hence, it is more challenging to transmit "*bandwidth-hungry*" video services with QoS guarantee in CR networks. The achieved results can provide a good guidance for how to bear other types of services in CR networks.

Video multicast has become an indispensable part for wireless networks, and hence it is of great significance to study how to scalably multicast video in CR systems. Several kinds of multicast schemes have been proposed for video transmission in the literature, including conventional multicast (CM) [13, 15], multiple description coding multicast (MDCM) [16, 17], and layered video multicast (LVM) [18, 19]. In CM [15], all subscribers in a multicast group receive the intended content with the identical quality, and the transmission rate is limited by the least channel gain of all subscribers. To cope with this issue, MDCM and LVM introduce source coding to support distinguished video transmission for different subscribers. In MDCM [16, 17], the video data is encoded into multiple descriptions and transmitted at different rates. For subscribers of various channel conditions, different sets of descriptions are received to jointly recover video with different resolutions. Despite being attractive in terms of system throughput, MDCM cannot guarantee the successful reception of key information and hence applies poorly in practice. By comparison, in LVM [18, 19], the video data is encoded into a base layer (BL) and several enhancement layers (ELs). The BL is intended to all subscribers at a low rate and hence can guarantee a basic recovered video quality, while the ELs are transmitted at incremental rates and opportunistically received by subscribers with promising channel conditions to persistently improve the video quality.

To the best our knowledge, existing researches on video multicast in OFDM-based CR systems mainly focus on CM [13, 15] or MDCM [16, 17], and what is more, only SE maximization model is studied. In this paper, joint intersession/interlayer subcarrier assignment and power allocation problem for energy-efficient LVM are studied in OFDM-based CR systems. For existing energy-efficient transmission models [9–12], *full-buffer* traffic model is assumed; that is, there is always infinite data waiting for transmission, and EE maximization is studied with no consideration of service characteristic. For LVM, the final recovered video quality is not linear with the receiving rate. Therefore, a utility function is introduced in our model to depict the relationship between the user experience, that is, recovered video quality, and its receiving rate, and a more accurate performance metric, *energy utility* (EU), is designed to measure the sum user experience achieved per Joule.

In detail, the main contributions of this paper can be summarized as follows.

(1) *EU-Based Optimization Model*. A novel optimization model is established for energy-efficient LVM in OFDM-based CR systems which aims at maximizing the system EU to balance the total recovered video quality and power consumption while guaranteeing multiple interference constraints for PUs.

(2) *Spectrum Assignment Method for LVM*. Both BL and EL subcarrier assignment algorithms are proposed to execute the intersession/interlayer subcarrier assignment in LVM. The BL subcarrier assignment aims at guaranteeing the basic video qualities for all multicast sessions with as fewer subcarriers as possible, while the EL subcarrier assignment tries to optimize the system EU by assigning subcarriers to the proper subscribers.

(3) *Optimal Power Allocation Method for EU Maximization*. For the multiconstrained EU-maximization problem, an optimal power allocation algorithm is presented by jointly utilizing fractional programming and subgradient method, which can be considered as the framework of optimizing energy-aware video multicast in OFDM-based CR systems.

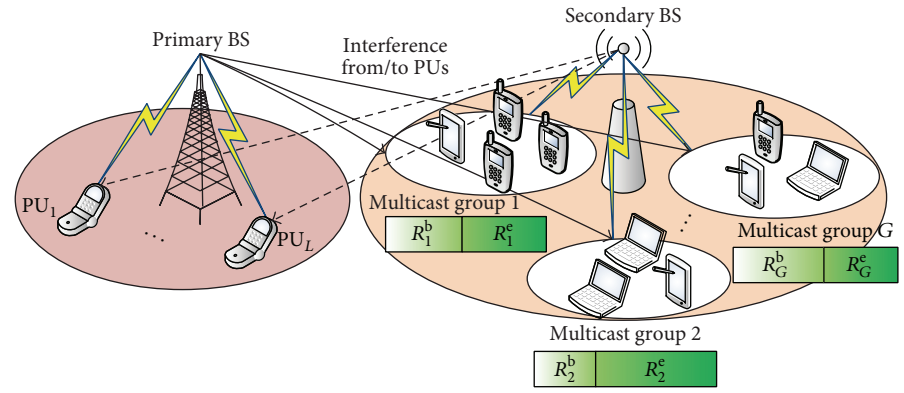
The rest of the paper is organized as follows. In Section 2, we build the EU-based optimization model for LVM over OFDM-based CR systems. The subcarrier assignment for BL as well as EL and the EU-based power allocation are proposed and discussed by Section 3. Finally, simulation results are shown in Section 4, and conclusions are drawn in Section 5.

2. System Model and Problem Formulation

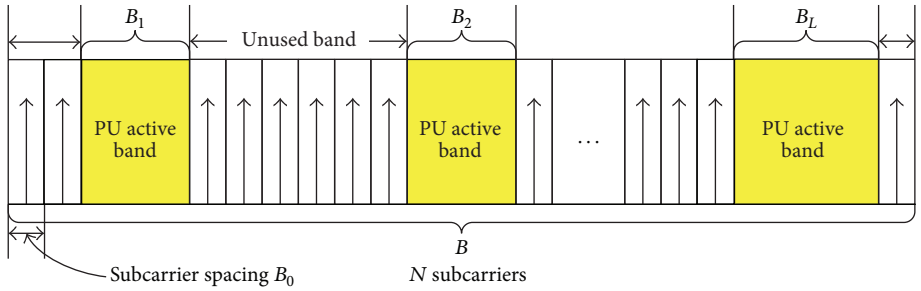
In this section, the spectrum division manner and the mutual-interference model are depicted firstly, and then the energy-efficient LVM transmission model is formulated with the objective of EU maximization.

2.1. OFDM-Based CR System. The considered CR system is composed of a primary network and a CR network, which are both deployed in a cellular fashion. The primary network consists of a primary base station (BS) and L PUs, while the CR network is made up of a secondary BS and K SUs. The whole licensed spectrum spans B Hz, and each PU occupies a disjoint fraction of the spectrum, denoted as B_l. For the finer-grained spectrum utilization, the OFDM technology is adopted to divide the whole sensed spectrum B into N subcarriers, with each subcarrier spanning $B_0 = B/N$ Hz [5, 9]. Figure 1 illustrates the details of CR system and spectrum distribution.

Since the sensed spectrum by CR network is licensed to the primary network, the privilege of PUs to use the spectrum must be guaranteed, which typically necessitates



(a) CR system: a primary network and a CR network coexist



(b) Spectrum division by OFDM and spectrum occupation of PUs

Figure 1: System scenario and spectrum distribution.

the interference control. Therefore, a common interference evaluation model is introduced from [20].

In [19], the power spectrum density (PSD) of subcarrier n is written as

$$\varphi_n(f) = p_n T_s \left(\frac{\sin \pi f T_s}{\pi f T_s} \right)^2, \tag{1}$$

where p_n is the transmitted power of signal on subcarrier n and T_s is the duration of OFDM symbol. Then, the interference introduced by the signal on subcarrier n into PU l can be expressed as

$$\widetilde{I}_{l,n}^{\mathrm{SP}} = G_l^{\mathrm{SP}} \int_{d_{l,n}-B_l/2}^{d_{l,n}+B_l/2} \varphi_n(f)\, df = I_{l,n} p_n, \tag{2}$$

where $d_{l,n}$ denotes the spectral distance between subcarrier n and the center frequency of PU l, G_l^{SP} denotes the channel gain from the secondary BS to PU l, and $I_{l,n}$ represents the interference caused by the normalized power on subcarrier n to PU l.

Meanwhile, the interference caused by the primary BS to SU k on subcarrier n is calculated as [20]

$$\widetilde{I}_{k,n}^{\mathrm{PS}} = \sum_{l=1}^{L} G_{k,n}^{\mathrm{PS}} \int_{d_{l,n}-\Delta f/2}^{d_{l,n}+\Delta f/2} E\left[I_l(\omega)\right] d\omega, \tag{3}$$

where $G_{k,n}^{\mathrm{PS}}$ denotes the channel gain from primary BS to SU k on subcarrier n, and $E[\cdot]$ is the expectation operator. $E[I_l(\omega)]$ is the signal PSD of PU l after N-Fast-Fourier-transform (FFT) processing, and it is represented as

$$E\left[I_l(\omega)\right] = \frac{1}{2\pi N} \int_{-\pi}^{\pi} \Phi_l\left(e^{j\phi}\right) \left(\frac{\sin\left(\omega-\phi\right) N/2}{\sin\left(\omega-\phi\right)/2} \right)^2 d\phi, \tag{4}$$

where $\Phi_l(e^{j\phi})$ is the PSD of the transmitted signal by the primary BS to PU l, which is generally modeled as an elliptically filtered white noise process [20].

2.2. LVM Transmission Model. As shown in Figure 1(a), all K users are partitioned into G multicast groups according to the video contents they are interested in. The set and number of SUs in group g are denoted as $\mathcal{K}_g$ and $|\mathcal{K}_g|$, respectively. Let $H_{k|g,n}^{\mathrm{SS}}$ denote the channel gain between the secondary BS and SU k in group g, and the corresponding channel gain to interference-plus-noise ratio (CINR) can be expressed as

$$\gamma_{k|g,n} = \frac{H_{k|g,n}^{\mathrm{SS}}}{\sigma_n^2 + \widetilde{I}_{k|g,n}^{\mathrm{PS}}}, \tag{5}$$

where σ_n^2 is the noise power on subcarrier n and $\widetilde{I}_{k|g,n}^{\mathrm{PS}}$ is calculated according to (3) with an index mapping from $k \mid g$

to k. Based on the Shannon formula, the achievable data rate of SU k in group g on subcarrier n is calculated by

$$r_{k|g,n} = B_0 \log_2 \left(1 + p_n \gamma_{k|g,n}\right). \quad (6)$$

For CM, the lowest rate of SUs in a group is conservatively adopted to ensure the correct data reception of all SUs [15]. Thus, the data transmission rate of group g on subcarrier n is expressed as

$$r^{\mathrm{c}}_{g,n} = \min_{k \in \mathcal{K}_g} r_{k|g,n} = B_0 \log_2 \left(1 + p_n \min_{k \in \mathcal{K}_g} \gamma_{k|g,n}\right). \quad (7)$$

In wireless transmission, the heterogeneity of the receiving channels for different SUs will seriously limit the performance for CM. In order to overcome the shortcomings, LVM [18, 19] is introduced and modeled in this paper. In LVM, video data are transmitted resiliently on different subcarriers to adapt to the diverse channel conditions. This is accomplished by coding the source data into a BL and several ELs, and as long as the BL is received, SU can decode the video stream with the basic quality. If more ELs are received, the decoded video quality is increasingly improved [21]. The essential difference between CM and LVM lies in that the former requires that all SUs in a group receive the video with the identical quality, whilst the latter allows the differential reception, depending on the individual channel quality. Therefore, LVM provides a new degree of freedom, that is, the transmission rates on subcarriers, to exploit different channel conditions.

Specifically, it is assumed that each video g, which is received by group g, is encoded into one BL with rate R^{b}_g and one EL with rate R^{e}_g (see Figure 1(a)). $R^{\max}_g = R^{\mathrm{b}}_g + R^{\mathrm{e}}_g$ denotes the maximal rate for video g. As in [19], we also assume that the fine grained scalability (FGS) coding technique is adopted, so that the EL can be truncated at any bit location with all the remaining bits still being useful at the decoder [22].

In LVM, the BL data is of great importance to reconstruct the source video, and it is imperative that the BL can be received by all the SUs in a group. Hence, if subcarrier n is used by group g for the BL transmission, the transmission rate is equal to that of CM; that is,

$$r^{\mathrm{b}}_{g,n} = r^{\mathrm{c}}_{g,n}. \quad (8)$$

If subcarrier n is used by group g for the EL transmission at a rate of $r^{\mathrm{e}}_{g,n}$, the receiving rate of SU $k, k \in \mathcal{K}_g$ on subcarrier n is written as

$$\sigma\left(r_{k|g,n} \geq r^{\mathrm{e}}_{g,n}\right) r^{\mathrm{e}}_{g,n}, \quad (9)$$

where $\sigma(T)$ is 1 if T is true, otherwise 0. Define two indicators $\rho_{g,n}$ and s_n to perform the intersession and interlayer subcarrier assignment as follows. $\rho_{g,n} \in \{1, 0\}$ denotes whether subcarrier n is assigned to group g or not, and s_n denotes whether subcarrier n is used for the BL transmission ($s_n = 1$) or the EL transmission ($s_n = 0$). The achieved rate of SU $k, k \in \mathcal{K}_g$ is calculated as

$$R_k = \sum_{n=1}^{N} \rho_{g,n} \left[(1 - s_n)\, \sigma\left(r_{k|g,n} \geq r^{\mathrm{e}}_{g,n}\right) r^{\mathrm{e}}_{g,n} + s_n r^{\mathrm{b}}_{g,n}\right]. \quad (10)$$

2.3. EU-Based Problem Formulation. In LVM, the achieved rate cannot reflect the quality directly, and some metrics, such as peak signal to noise ratio (PSNR) and mean square error (MSE), may be more accurate to evaluate the received video quality. For generalizing the expression, the utility function $U_k(R_k)$ is defined to denote the change relationship of reconstructed video quality with the achieved rate. Moreover, $U_k(R_k)$ is assumed to be nondecreasing and concave according to the measured or theoretical results [18, 19]. Then, the total weighted-utility is summed as

$$U_{\mathrm{total}} = \sum_{k=1}^{K} w_k U_k\left(R_k\right), \quad (11)$$

where w_k ($w_k > 0$) is the weight of SU k and can be used to reflect the relative priorities among SUs.

Apart from the video quality, the energy cost of video transmission over OFDM-based CR systems should be also considered. The total energy consumption in a timeslot includes three parts: the sense energy P_{s}, that is, the energy consumed to sense the available spectrum, the transmission energy P_{t}, that is, the energy consumed to transmit data on the sensed spectrum, and the circuit energy P_{c}. Note that the concepts of "*energy*" and "*power*" are not strictly distinguished in this paper, since only the constant duration is multiplied or not. The total energy consumption is accumulated as

$$E_{\mathrm{total}} = P_{\mathrm{t}} + P_{\mathrm{s}} + P_{\mathrm{c}} = \sum_{n=1}^{N} p_n + \xi \sum_{n=1}^{N} p_n + P_{\mathrm{c}}, \quad (12)$$

where ξ denotes the ratio of the sense energy P_{s} to the transmission energy P_{t} [15]. The formula accounts for the required energy consumption for downlink (DL) video multicast in OFDM-based CRNs. In practice, the total system power consumption includes the power consumption at both BS and end device sides. The power consumption of end devices during DL transmission mainly results from multiple active circuit modules, such as the channel estimation and feedback module and the baseband signal processing module. However, the aggregate value is relatively small compared with the power consumption of BS, whose radio frequency (RF) transmit power is often very large due to the large-scale pathloss fading. As a result, the power consumption of end devices is not considered in formula (12), in which the total system energy consumption is approximated as the power consumption at the secondary BS [7, 9–12].

In the existing work, EE is maximized to optimize the achieved rate by the unit energy consumption [9–12]. For the video transmission, it makes more sense to shift EE to

EU. Therefore, the EU-based video transmission problem is formulated as

$$\begin{aligned}
\mathcal{OP}_0: \quad & \max_{\rho_{g,n},p_n,s_n,r^{\mathrm{e}}_{g,n},r^{\mathrm{b}}_{g,n}} \eta_{\mathrm{EU}} = \frac{U_{\mathrm{total}}}{E_{\mathrm{total}}} \\
& C_1: \sum_{n=1}^{N} p_n \le P_{\mathrm{total}} \\
& C_2: \sum_{n=1}^{N} I_{l,n} p_n \le I^l_{\mathrm{th}}, \quad 1 \le l \le L \\
& C_3: p_n \ge 0, \quad 1 \le n \le N \\
& C_4: \sum_{n=1}^{N} \rho_{g,n} s_n r^{\mathrm{b}}_{g,n} \ge R^{\mathrm{b}}_g, \quad 1 \le g \le G \\
& C_5: \sum_{g=1}^{G} \rho_{g,n} \le 1, \quad 1 \le n \le N \\
& C_6: \rho_{g,n} \in \{0,1\}, \quad 1 \le n \le N,\ 1 \le g \le G \\
& C_7: s_n \in \{0,1\}, \quad 1 \le n \le N,
\end{aligned} \tag{13}$$

where P_{total} is the total transmitted power by the secondary BS and I^l_{th} is the interference threshold for PU l. In $\mathcal{OP}_0$, C_2 denotes the total interference constraint from each PU, C_4 requires that the BL data can be received by all the SUs in each group to guarantee the basic quality of reconstructed video, and C_5 and C_6 restrict that one subcarrier is exclusively used by only one group, since different groups may be interested in distinct video contents from the secondary BS. It is assumed that the secondary BS has the perfect knowledge of multicast grouping, the bandwidth of B, channel gains, and interference coefficients.

3. Optimized Video Multicast Transmission

In order to achieve the optimal performance, spectrum assignment $\rho_{g,n}$, s_n, power allocation p_n, and the data transmission rate selection $r^{\mathrm{e}}_{g,n}$, $r^{\mathrm{b}}_{g,n}$ should be jointly determined. Nevertheless, the tight coupling among these variables will incur a prohibitively high computation complexity. Therefore, allowing for the features of LVM and CRN, we decompose $\mathcal{OP}_0$ into three steps, that is, BL subcarrier assignment, EL subcarrier assignment, and power allocation. Additionally, how to deal with the spectrum scarcity is also discussed.

3.1. BL Subcarrier Assignment. For unifying the expression, let $I_{0,n} = 1$, $1 \le n \le N$, $I^0_{\mathrm{th}} = P_{\mathrm{total}}$. In the traditional OFDM systems, where no primary network exists, equal power P_{total}/N is generally assumed for subcarrier assignment [23]. In OFDM-based CRNs, the interference to PUs has to be considered, and the interference coefficient $I_{l,n}$ varies from one subcarrier to another. The coarse assumption of equal power deviates from the actual situations and may degrade the performance. Instead, the ladder-profile power is assumed in this paper:

$$p_n = \min\left(\frac{I^0_{\mathrm{th}}}{NI_{0,n}}, \frac{I^1_{\mathrm{th}}}{NI_{1,n}}, \ldots, \frac{I^L_{\mathrm{th}}}{NI_{L,n}}\right). \tag{14}$$

This idea is borrowed from [24], which supposes that each subcarrier produces the identical amount of interference to PUs. Obviously, the power p_n in (14) rests with the interference coefficients and may differ among subcarrier individuals. It can be verified that all the power and interference constraints C_1 and C_2 are satisfied by (14); that is, $\sum_{n=1}^{N} I_{l,n} p_n \le \sum_{n=1}^{N} I_{l,n}(I^l_{\mathrm{th}}/NI_{l,n}) \le I^l_{\mathrm{th}}$ for $0 \le l \le L$. Furthermore, a factor $\beta \le 1$ is calculated to scale the power p_n as

$$\beta = \max_{0 \le l \le L} \frac{\sum_{n=1}^{N} I_{l,n} p_n}{I^l_{\mathrm{th}}}, \quad p_n = \frac{p_n}{\beta}, \tag{15}$$

such that at least one constraint in C_1, C_2 is active for maintaining the reasonable power level.

With (14) and (15), the achievable rate $r^{\mathrm{b}}_{g,n}$ of BL is readily computed according to (7) and (8). The details of BL subcarrier assignment are provided in Algorithm 1. The objective of Algorithm 1 is to meet the BL rate requirements with as small number of subcarriers as possible. At each iteration, the most unsatisfied group g with the largest gap from the BL rate requirement is selected, and then the best subcarrier n with the largest achievable rate is assigned to this group. Subsequently, the state of whether the rate requirement is fulfilled or not is inspected for group g, and if satisfied, it is immediately removed from the set of unsatisfied groups $\mathcal{G}$ to save more subcarriers for EL data transmission.

Either $\mathcal{A} = \varnothing$ or $\mathcal{G} = \varnothing$ will terminate Algorithm 1. However, only when $\mathcal{A} \ne \varnothing$, that is, there is a surplus of subcarriers, EL subcarrier assignment is needed, which progressively improves the quality of video.

3.2. EL Subcarrier Assignment. For EL subcarrier assignment, besides the task of assigning subcarriers to the appropriate groups, the data transmission rate $r^{\mathrm{e}}_{g,n}$ should also be determined jointly. In $\mathcal{OP}_0$, $r^{\mathrm{e}}_{g,n}$ is limited to be a nonnegative real number. It seems that the derivative method has to be adopted to obtain the optimal $r^{\mathrm{e}}_{g,n}$ as the value of $r^{\mathrm{e}}_{g,n}$ is continuous. However, by a close observation, $r^{\mathrm{e}}_{g,n}$ can only take finite $K + 1$ values. Specifically, the following theorem is presented to reduce the complexity of subcarrier assignment for EL.

Theorem 1. *With the nondecreasing utility functions, for any subcarrier n assigned to transmit the EL data, the optimal rate $r^{e}_{g,n}$ is equal to* 0 *or $r^{e}_{g,n} \in \mathcal{B}_n = \{r_{m|g,n} \mid 1 \le g \le G,\ m \in \mathcal{K}_g\}$; that is, $r^{e}_{g,n}$ must be zero or one of the K achievable rates in $\mathcal{B}_n$.*

Proof. See Appendix A. □

Theorem 1 indicates that if subcarrier n is assigned to group g, then only the $|\mathcal{K}_g|$ achievable rates may be the

Input:
(1) P_{total}, $\gamma_{m|g,n}$ for $m \in \mathscr{K}_g$, $1 \le g \le G$, p_n for $1 \le n \le N$, $I_{l,n}$ for $1 \le l \le L$, $1 \le n \le N$, I_{th}^l for $1 \le l \le L$, and R_g^{b} for $1 \le g \le G$;
Initialization:
(2) Initialize the set of BL-rate-unsatisfied groups $\mathscr{G} = \{1, 2, \ldots, G\}$, the set of unassigned subcarriers $\mathscr{A} = \{1, 2, \ldots, N\}$, the achieved rate $\widetilde{R}_g = 0$ for group g, the set of assigned subcarriers $\Omega_k = \varnothing$ for SU k, the assignment indicator $\rho_{g,n} = 0$, $1 \le n \le N$, $1 \le g \le G$;
Iteration:
(3) **while** $\mathscr{A} \neq \varnothing$ **and** $\mathscr{G} \neq \varnothing$ **do**
(4) Find group $g \in \mathscr{G}$ satisfying $\widetilde{R}_g - R_g^{\text{b}} \le \widetilde{R}_i - R_i^{\text{b}}$, $\forall i \in \mathscr{G}$;
(5) Select subcarrier n to maximize the achieved rate as $n = \arg\max_j r_{g,j}^{\text{b}}$, $j \in \mathscr{A}$;
(6) Assign subcarrier n to group g for BL data transmission as $\rho_{g,n} = 1$, $\mathscr{A} = \mathscr{A} - \{n\}$, $s_n = 1$, and update $\widetilde{R}_g$, Ω_k as $\widetilde{R}_g = \widetilde{R}_g + r_{g,n}^{\text{b}}$, $\Omega_k = \Omega_k \cup \{n\}$, $\forall k \in \mathscr{K}_g$;
(7) **if** $\widetilde{R}_g \ge R_g^{\text{b}}$ **then**
(8) Delete group g as $\mathscr{G} = \mathscr{G} - \{g\}$;
(9) **end if**
(10) **end while**
Output:
(11) $\mathscr{G}, \mathscr{A}, \widetilde{R}_g, \Omega_k, \rho_{g,n}, s_n$.

Algorithm 1: Algorithm for BL subcarrier assignment.

Input:
(1) $w_k, \xi, P_c, P_{\text{total}}, \gamma_{m|g,n}$ for $m \in \mathscr{K}_g$, $1 \le g \le G, n \in \mathscr{A}$, p_n for $n \in \mathscr{A}$, $I_{l,n}$ for $1 \le l \le L, n \in \mathscr{A}$ and I_{th}^l for $1 \le l \le L$;
Initialization:
(2) Initialize the set of unassigned subcarriers $\mathscr{A}$, the set of assigned subcarriers Ω_k for SU k, and the assignment indicator $\rho_{g,n}, n \notin \mathscr{A}, 1 \le g \le G$ according to the output of Algorithm 1. Set $\rho_{g,n} = 0$, $n \in \mathscr{A}$, $1 \le g \le G$, and the achieved rate $R_k = \widetilde{R}_g$ for SU k, $k \in \mathscr{K}_g$;
Iteration:
(3) **while** $\mathscr{A} \neq \varnothing$ **do**
(4) Select subcarrier $n, n \in \mathscr{A}$ in order, and find group g and BU m to maximize the achieved EU as $(g, m) = \arg\max_{\rho_{i,n}, r_{j|i,n}} \eta_{\text{EU}}$, $1 \le i \le G$, $j \in \mathscr{K}_g$;
(5) Assign subcarrier n to group g for EL data transmission as $\rho_{g,n} = 1$, $\mathscr{A} = \mathscr{A} - \{n\}$, $s_n = 0$, and update R_k, Ω_k as $R_k = R_k + \sigma(r_{k|g,n} \ge r_{m|g,n}) r_{m|g,n}$ for $k \in \mathscr{K}_g$, $\Omega_k = \Omega_k \cup \{n\}$ for $r_{k|g,n} \ge r_{m|g,n}$, $k \in \mathscr{K}_g$;
(6) **end while**
Output:
(7) $\Omega_k, \rho_{g,n}, s_n, r_{m|g,n}$.

Algorithm 2: Algorithm for EL subcarrier assignment.

optimal solution. In total, all $K = \sum_{g=1}^{G} |\mathscr{K}_g|$ achievable rates constitute the candidates for the optimal solution if subcarrier n is not assigned yet. This contracts the domain of $r_{g,n}^{\text{e}}$ from the nonnegative real number to $K + 1$ discrete values and thereby eases the determination process of $r_{g,n}^{\text{e}}$. Define SU m as the barrier user (BU) on subcarrier n if its achievable rate is selected for data transmission, that is, $r_{g,n}^{\text{e}} = r_{m|g,n}$, since its rate marks the watershed between the success and failure in data reception. According to Theorem 1, the rate of SU k in (10) is rewritten as

$$R_k = \sum_{n=1}^{N} \rho_{g,n} \left[(1 - s_n)\, \sigma\left(r_{k|g,n} \ge r_{m|g,n}\right) r_{m|g,n} + s_n r_{g,n}^{\text{b}} \right], \tag{16}$$

where BU m may be different among subcarriers and needs to be decided by Algorithm 2.

The objective of Algorithm 2 is to maximize the EU via subcarrier assignment for EL. At each iteration, subcarrier n is selected in order, and then, based on Theorem 1, the traversal of $K + 1$ values for $r_{g,n}^{\text{e}}$ is carried out in order to achieve the maximal EU η_{EU}. In Algorithm 2, for $1 \le i \le G$, $j \in \mathscr{K}_g$, to maximize η_{EU} is equivalent to maximizing the total utility as

$$\arg \max_{\rho_{i,n}, r_{j|i,n}} \eta_{\text{EU}} = \arg \max_{\rho_{i,n}, r_{j|i,n}} \sum_{k=1}^{K} w_k U_k\left(R_k\right), \tag{17}$$

since the power consumption values are equal for the denominator of η_{EU} when determining which group subcarrier n is assigned to and which SU is selected as the BU.

3.3. EU-Based Power Allocation. With the determined subcarrier assignment, the rate of SU $k, k \in \mathscr{K}_g$ in (16) can be further expressed as

$$\begin{aligned} R_k &= \sum_{n\in\Omega_k}\left[(1-s_n)\, r_{m|g,n} + s_n r^{\mathrm{b}}_{g,n}\right] = \sum_{n\in\Omega_k} r_n \\ &= \sum_{n\in\Omega_k} B_0 \log_2\left(1+p_n\gamma_n\right), \end{aligned} \tag{18}$$

where r_n and γ_n are the achievable rate and CINR, respectively, for the BU related to subcarrier n in group g. Note that if subcarrier n is used for EL, the BU is specified in Algorithm 2. Otherwise, for BL, the BU is the SU in group g with the worst channel condition on subcarrier n.

When determining subcarrier assignment, the ladder-profile power is simply assumed in (14) and (15) to evaluate the rate or utility in Algorithms 1 and 2. Thus, the power needs to be reallocated to maximize the EU for multicast video transmission, which is formulated as

$$\begin{aligned} \mathscr{OP}_1\colon\quad & \max_{p_n} \eta_{\mathrm{EU}}(\mathbf{p}) = \frac{U_{\mathrm{total}}(\mathbf{p})}{E_{\mathrm{total}}(\mathbf{p})} \\ & C_1\colon \sum_{n=1}^{N} p_n \le P_{\mathrm{total}} \\ & C_2\colon \sum_{n=1}^{N} I_{l,n} p_n \le I^l_{\mathrm{th}}, \quad 1\le l\le L \\ & C_3\colon p_n \ge 0, \quad 1\le n\le N \\ & C_4\colon \sum_{n\in\Theta^{\mathrm{b}}_g} r_n \ge R^{\mathrm{b}}_g, \quad 1\le g\le G, \end{aligned} \tag{19}$$

where Θ^{b}_g is the set of subcarriers assigned to group g for the BL transmission and $\mathbf{p}$ denotes the vector of p_n, $1 \le n \le N$. Even though the optimization variables associated with subcarrier assignment in $\mathscr{OP}_0$ have been settled, $\mathscr{OP}_1$ is still intractable due to the fractional objective function as well as a large number of constraints on the power and BL rate.

As in our previous work [9], *fractional programming* [25] is employed to deal with the objective function issue. With the positive parameter α, a new function $g(\mathbf{p},\alpha)$ is defined as

$$g(\mathbf{p},\alpha) = E_{\mathrm{total}}(\mathbf{p}) - \alpha U_{\mathrm{total}}(\mathbf{p}). \tag{20}$$

Then, another problem is formulated as

$$\begin{aligned} \mathscr{OP}_2\colon\quad & \min_{p_n} g(\mathbf{p},\alpha) \\ & C_1, C_2, C_3, C_4. \end{aligned} \tag{21}$$

Let S denote the feasible region of $\mathscr{OP}_1$ and $\mathscr{OP}_2$, and define the optimal value and solution of $\mathscr{OP}_2$ as

$$\begin{aligned} F(\alpha) &= \min_{\mathbf{p}} \{g(\mathbf{p},\alpha) \mid \mathbf{p}\in S\}, \\ \mathbf{f}(\alpha) &= \arg\min_{\mathbf{p}} \{g(\mathbf{p},\alpha) \mid \mathbf{p}\in S\}. \end{aligned} \tag{22}$$

The following lemma can relate $\mathscr{OP}_1$ and $\mathscr{OP}_2$, and the detailed proof of Lemma 2 can be found in [25].

Lemma 2. *$\mathbf{p}^*$ and $1/\alpha^*$ correspond to the optimal solution and value of problem $\mathscr{OP}_1$ in (19); that is, $1/\alpha^* = U_{total}(\mathbf{p}^*)/E_{total}(\mathbf{p}^*) = \max_{\mathbf{p}}\{\eta_{EU}(\mathbf{p}) \mid \mathbf{p}\in S\}$, if and only if*

$$\begin{aligned} F(\alpha^*) &= 0, \\ \mathbf{f}(\alpha^*) &= \mathbf{p}^*. \end{aligned} \tag{23}$$

Lemma 2 indicates that the optimal solution to $\mathscr{OP}_2$ is also the optimal solution to $\mathscr{OP}_1$, provided that (23) is satisfied. Hence, solving $\mathscr{OP}_1$ can be realized by finding the optimal power allocation of $\mathscr{OP}_2$ for a given α, and then update α until (23) is established. The problem at hand is how to achieve the optimal power allocation for $\mathscr{OP}_2$ with a given α. To this end, the following theorem is presented.

Theorem 3. *If the utility function is nondecreasing and concave for each SU, problem $\mathscr{OP}_2$ with a fixed α belongs to convex optimization ones.*

Proof. See Appendix B. □

The convexity of $\mathscr{OP}_2$ with a fixed α enables the solution in the dual domain without the dual gap [26]. Namely, the optimal solution to the dual problem is exactly the optimal solution to the primal problem $\mathscr{OP}_2$. The Lagrangian of $\mathscr{OP}_2$ is defined as

$$\begin{aligned} L = {} & E_{\mathrm{total}}(\mathbf{p}) - \alpha U_{\mathrm{total}}(\mathbf{p}) + \sum_{l=0}^{L}\lambda_l\left(\sum_{n=1}^{N} I_{l,n}p_n - I^l_{\mathrm{th}}\right) \\ & + \sum_{g=1}^{G}\upsilon_g\left(R^{\mathrm{b}}_g - \sum_{n\in\Theta^{\mathrm{b}}_g} r_n\right), \end{aligned} \tag{24}$$

where $\boldsymbol{\lambda} = [\lambda_0, \lambda_1, \ldots, \lambda_L] \succeq \mathbf{0}$ and $\boldsymbol{\upsilon} = [\upsilon_1, \ldots, \upsilon_G] \succeq \mathbf{0}$ are vectors of dual variables. Therefore, its dual function is defined as

$$h(\boldsymbol{\lambda}, \boldsymbol{\upsilon}, \alpha) = \min_{p_n} L. \tag{25}$$

According to the Karush-Kuhn-Tucker (KKT) conditions [26], the optimal power allocation should satisfy

$$\begin{aligned} \frac{\partial L}{\partial p_n} = {} & \left[-\alpha\sum_{k\in\Phi_n} w_k \frac{dU_k(R_k)}{dR_k} - s_n\upsilon_g\right]\frac{B_0}{\ln 2}\frac{\gamma_n}{1+p_n\gamma_n} \\ & + \sum_{l=0}^{L}\lambda_l I_{l,n} + \xi + 1 = 0, \end{aligned} \tag{26}$$

where Φ_n denotes the set of SUs who can receive data from subcarrier n. By some manipulations, the optimal p_n is derived as

$$\begin{aligned} p_n = {} & \left[\frac{B_0}{\ln 2}\frac{\alpha\sum_{k\in\Phi_n} w_k\left(dU_k(R_k)/dR_k\right) + s_n\upsilon_g}{\sum_{l=0}^{L}\lambda_l I_{l,n} + \xi + 1}\right. \\ & \left. - \frac{1}{\gamma_n}\right]^+, \end{aligned} \tag{27}$$

Input:
(1) $w_k, \xi, P_c, P_{\text{total}}, \gamma_{m|g,n}$ for $m \in \mathcal{K}_g$, $1 \le g \le G$, $1 \le n \le N$, $I_{l,n}$ for $1 \le l \le L$, $1 \le n \le N$, I_{th}^l for $1 \le l \le L$, Ω_k for $1 \le k \le K$, Φ_n, s_n for $1 \le n \le N$ and $\Theta_g^{\text{b}}, R_g^{\text{b}}$ for $1 \le g \le G$;
Initialization:
(2) Initialize α, and the tolerable error ϵ. Set $F(\alpha) = \infty$;
Iteration:
(3) **while** $|F(\alpha)| > \epsilon$ **do**
(4) Initialize the tolerable error $\widetilde{\epsilon}$, the dual variables λ_l, $0 \le l \le L$, υ_g, $1 \le g \le G$, and $e = \infty$;
(5) **while** $e > \widetilde{\epsilon}$ **do**
(6) Calculate p_n according to (26) or (27);
(7) Update λ_l, υ_g according to (29);
(8) Compute e as $e = \|\Delta\boldsymbol{\lambda}/\boldsymbol{\lambda}(t)\| + \|\Delta\boldsymbol{\upsilon}/\boldsymbol{\upsilon}(t)\|$ with $\Delta\boldsymbol{\lambda} = \boldsymbol{\lambda}(t+1) - \boldsymbol{\lambda}(t)$, $\Delta\boldsymbol{\upsilon} = \boldsymbol{\upsilon}(t+1) - \boldsymbol{\upsilon}(t)$;
(9) **end while**
(10) Compute $F(\alpha)$, and update $\alpha = E_{\text{total}}(\mathbf{p})/U_{\text{total}}(\mathbf{p})$;
(11) **end while**
Output:
(12) p_n and the final EU $\eta_{\text{EU}} = 1/\alpha$.

Algorithm 3: EU-based power allocation.

where $[x]^+$ denotes $\max\{0, x\}$. In general, the analytical expression of p_n is unavailable, except that $U_k(R_k)$ is linear with R_k for any SU k. In such cases, $dU_k(R_k)/dR_k$ is independent of p_n. Otherwise, n nonlinear equations with n unknowns in (26) have to be solved numerically to find the optimal p_n.

Once the optimal p_n is achieved, the dual function $h(\boldsymbol{\lambda}, \boldsymbol{\upsilon}, \alpha)$ in (25) can be computed for the fixed tuple $(\boldsymbol{\lambda}, \boldsymbol{\upsilon})$. Now, the dual problem needs to be solved as

$$\max_{\boldsymbol{\lambda} \ge \mathbf{0}, \boldsymbol{\upsilon} \ge \mathbf{0}} h(\boldsymbol{\lambda}, \boldsymbol{\upsilon}, \alpha). \tag{28}$$

The optimal solution to (28) can be steadily obtained in a subgradient method [27], which iteratively updates the dual variables $(\boldsymbol{\lambda}, \boldsymbol{\upsilon})$ in the subgradient direction until they converge. Specifically, the updates for (28) can be performed as

$$\begin{aligned} \lambda_l(t+1) &= \left[\lambda_l(t) - \varepsilon_t\left(I_{\text{th}}^l - \sum_{n=1}^{N} I_{l,n} p_n\right)\right]^+, \quad 0 \le l \le L, \\ \upsilon_g(t+1) &= \left[\upsilon_g(t) - \omega_t\left(\sum_{n \in \Theta_g^{\text{b}}} r_n - R_g^{\text{b}}\right)\right]^+, \quad 1 \le g \le G, \end{aligned} \tag{29}$$

where $\varepsilon_t, \omega_t > 0$ form two sequences of step sizes. In general, the step size ε_t, ω_t can be selected as κ/t or $\kappa/\sqrt{t}$ based on the diminishing rules [27], where $\kappa > 0$ is a constant, and t is the number of iterations. The subgradient method can guarantee that $(\boldsymbol{\lambda}, \boldsymbol{\upsilon})$ converges to the optimal point as long as ε_t and ω_t are sufficiently small [27]. Due to the convexity depicted by Theorem 3, the optimal solution to $\mathcal{OP}_2$ can be achieved according to (26) or (27) once the dual optimal solution $(\boldsymbol{\lambda}^*, \boldsymbol{\upsilon}^*)$ is reached.

With the optimal power allocation $\mathbf{p}$ for the given α, update $\alpha = E_{\text{total}}(\mathbf{p})/U_{\text{total}}(\mathbf{p})$ and solve problem $\mathcal{OP}_2$ again. The process is repeated until the condition of Lemma 2 is satisfied. The iteration convergence of α update is proved in [24]. The details of power allocation are provided in Algorithm 3, where $\|\mathbf{x}\|$ denotes the 2-norm of vector $\mathbf{x}$.

The objective of Algorithm 3 is to maximize the EU by allocating power among subcarriers, whilst guaranteeing the BL rate requirements. In the inner loop, power allocation $\mathbf{p}$ and dual variables $(\boldsymbol{\lambda}, \boldsymbol{\upsilon})$ are alternately updated to attain the optimal solution for a fixed α. In the outer loop, α is repeatedly updated until it converges. It can be asserted that Algorithm 3 can reap the optimal power for $\mathcal{OP}_1$, owing to the factor that both the inner-loop and outer-loop iterations can converge to the respective optimal solutions.

In a practical system, the video is encoded into data layers at first, and then the BL data is mapped onto subcarriers by Algorithm 1. Sequentially, the EL data is arranged on the unused subcarriers by Algorithm 2, and the power, corresponding to the transmission rate, for each subcarrier is ultimately settled by Algorithm 3. Through all three algorithms, the EU is consecutively optimized to deliver the video to diverse receivers with the detected spectrum and limited energy.

3.4. Spectrum Scarcity Discussion. Typically, the video service is "*bandwidth-hungry,*" and wireless network states, including channel quality, service requests, and the numbers of SUs and PUs, remain ever-changing. Sometimes the sensed spectrum is not enough for supporting the BL rates of all the groups. For example, the available bandwidth is overly narrow due to the full occupation of the primary network, or the interference threshold is excessively tight because the CR network is geographically close to the primary network. For such cases, problem $\mathcal{OP}_0$ has no feasible solutions, which is usually reflected by the phenomenon that Algorithm 1 stops with $\mathcal{A} = \varnothing$.

In order to address the issue, the *aggressive* solution is to drop some SUs according to the service emergency or the requested rate of BL data, and in the next timeslot, more transmission opportunities are offered to these sacrificed SUs. The *conservative* solution is to relax the BL rate constraint C_4 in $\mathcal{OP}_0$ and adaptively determine the transmission rates of each SU by its contribution to the EU η_{EU}; that is, the SU who can increase the total utility most by the unit energy consumption will achieve the transmission opportunity. This solution can restrain parts of SUs from data transmission in an "*EU-competitive*" fashion.

4. Simulation Results

In this section, channel fading gains from the secondary BS to SUs and PUs are modeled as consisting of six independent Rayleigh multipaths with an average channel power gain of 0 dB. The sensed spectrum is divided into $N = 64$ subcarriers with the subcarrier spacing $B_0 = 15$ KHz in frequency band. $L = 4$ PUs are assumed to be active in the primary network, and each PU occupies a fraction of spectrum with an equal bandwidth of $2B_0$. The locations of PU bands are assumed to evenly span the whole frequency band.

The noise power plus the interference power is identically set as σ_0^2 for each subcarrier, and the total transmission power is $P_{\mathrm{total}} = 1$ W. The average signal to interference-plus-noise ratio (SINR), which is defined as $P_{\mathrm{total}}/(N\sigma_0^2)$, ranges from 8 dB to 28 dB. The interference threshold of each PU $I_{\mathrm{th}}^l = 0.5$ mW for $1 \le l \le L$. The weight $w_k = 1$, $1 \le k \le K$, is designated to maximize the system sum-utility. The circuit energy consumption $P_{\mathrm{c}} = 0.1$ W, and the ratio of the sense energy to the transmission energy is set as $\xi = 0.1$.

In the CR network, two video sequences, that is, *Foreman* and *Harbour* in [18], are dedicated to $G = 2$ groups. The piecewise linear utility function [18] is selected to evaluate the PSNR performance as

$$U_k(r) = \begin{cases} U_g^0 + \chi_g\left(r - R_g^{\mathrm{b}}\right) & r \le R_g^{\mathrm{b}} \\ U_g^0 + \tau_g\left(r - R_g^{\mathrm{b}}\right) & R_g^{\mathrm{b}} < r \le R_g^{\max} \\ U_g^0 + \tau_g\left(R_g^{\max} - R_g^{\mathrm{b}}\right) & r > R_g^{\max}, \end{cases} \tag{30}$$

where U_g^0, $k \in \mathcal{K}_g$, denotes the PSNR when only the BL data is received and χ_g and τ_g are the slopes of the two pieces. The parameters U_g^0, R_g^{b}, $R_g^{\max}$, χ_g, and τ_g are set according to the video sequences *Foreman* and *Harbour* in [18]. With the specific utility function (30), the optimal p_n in (27) can be rewritten as

$$p_n = \left[\frac{B_0}{\ln 2}\frac{\alpha\left(\sum_{k\in\Phi_n^{\mathrm{L}}} w_k\chi_g + \sum_{k\in\Phi_n^{\mathrm{M}}} w_k\tau_g\right) + s_n\upsilon_g}{\sum_{l=0}^{L}\lambda_l I_{l,n} + \xi + 1} - \frac{1}{\gamma_n}\right]^+, \tag{31}$$

where Φ_n^{L} and Φ_n^{M} are the subsets of Φ_n and denote the sets of SUs in Φ_n, whose total rate R_k, respectively, satisfies $R_k \le R_g^{\mathrm{b}}$ and $R_g^{\mathrm{b}} < R_k \le R_g^{\max}$. For comparison, another utility function $U_k(r) = r$ is also simulated to maximize the weighted-rate. All simulation results are averaged over 1000 channel realizations.

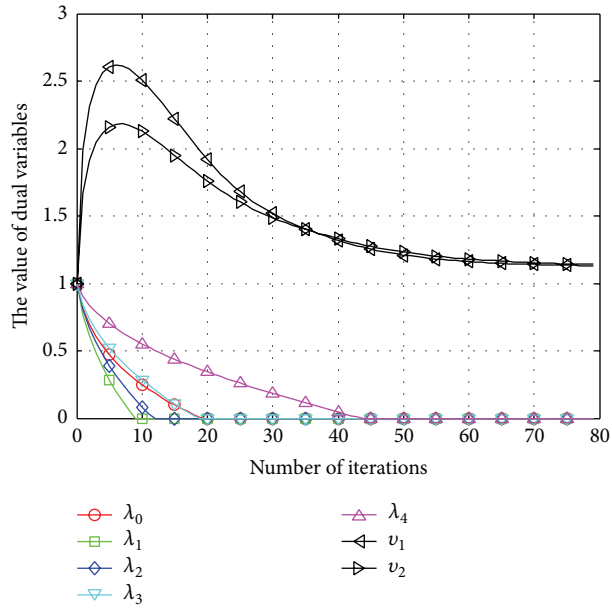


Figure 2: The convergence process of dual variables in the energy-utility-based power allocation algorithm.

Table 1: Average number of iterations for auxiliary variable α.

Optimization objective function	Weighted-PSNR	Weighted-rate
Average number of iterations	2.1	3.6

Figure 2 shows the convergence process of dual variables λ_l, $l = 0, 1, 2, 3, 4$, and υ_g, $g = 1, 2$, in the EU-based power allocation algorithm, where the number of SUs is 4 in each group, and the average SINR is equal to 12 dB. It can be observed that the dual variables rapidly converge to the stable points within 10~80 iterations. Table 1 lists the average iteration numbers of auxiliary variable α. No matter which objective function is optimized, weighted-PSNR or weighted-rate, approximately 2~4 iterations are sufficient to achieve the converged α, which indicates that the high convergence rate of α is little impacted by the objective function. Combining Figure 2 with Table 1, it is concluded that the EU-based power allocation algorithm possesses the favourable iteration complexity.

In Figure 3, the EEs of the CM [14] and LVM are demonstrated with the increase of the SU number in each group. That is, the utility function is chosen as $U_k(r) = r$. As the number of SUs increases, both multicast methods are capable of achieving the higher EE, due to the fact that more SUs can benefit from a single transmission. In the meantime, the EE gap between them continuously enlarges, because the LVM enables the differential data reception and breaks through the worst channel restraint in CM. For example, with

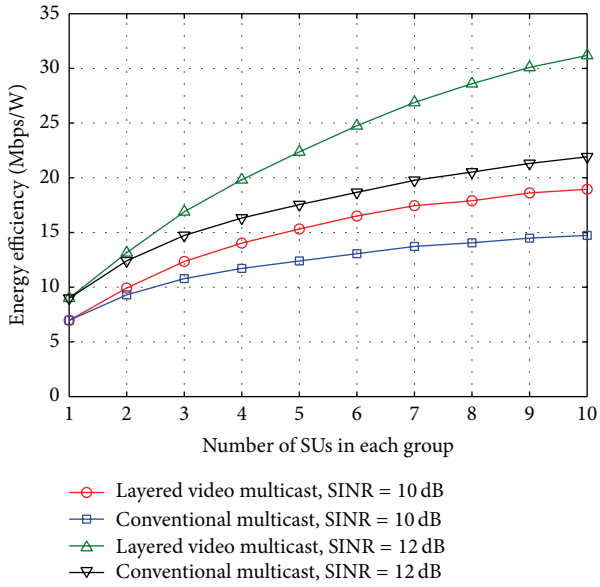


Figure 3: The energy efficiency comparison between the conventional multicast and layered video multicast.

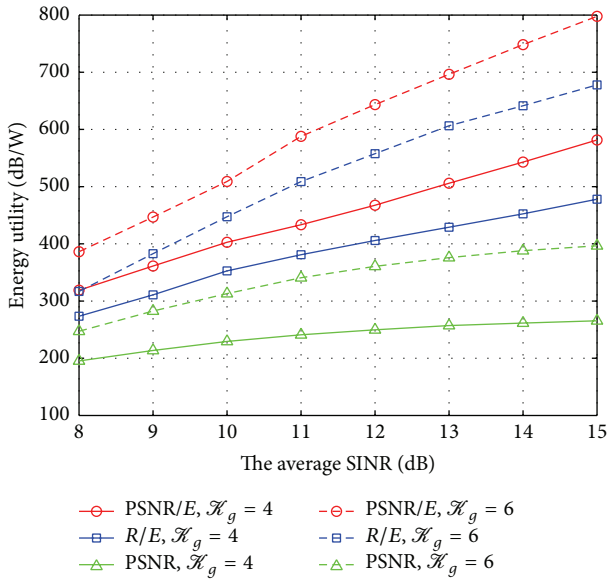


Figure 4: The energy utility comparison among different optimization objective functions.

SINR = 12 dB, when the number of SUs is 10 in each group, the EE gain is nearly up to 40%.

In Figure 4, we compare three optimization objective functions, that is, the EU (the weighted-PSNR divided by the total energy consumption), the EE (the weighted-rate divided by the total energy consumption) [9–12], and the weighted-PSNR [18, 19], for the video transmission in terms of the achieved PSNR by the unit energy consumption. From Figure 4, it can be seen that because of integrating the energy cost into consideration the EE optimization achieves a significant performance gain over the weighted-PSNR optimization. Moreover, the EU optimization is considerably superior

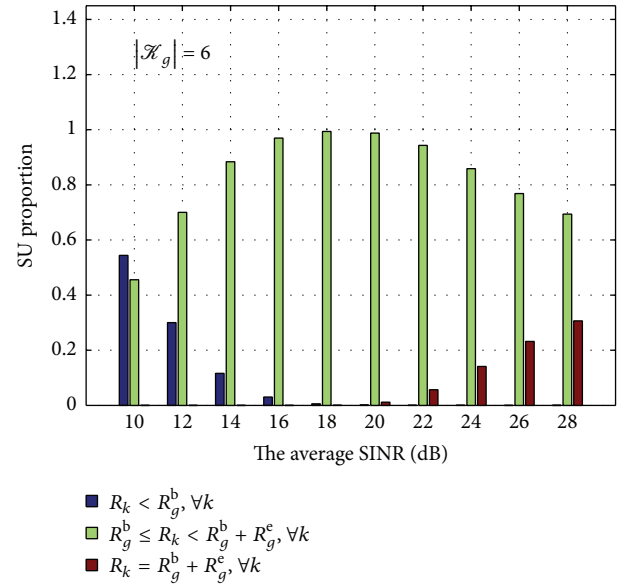


Figure 5: The proportion distribution of SUs within three rate ranges.

to the EE optimization thanks to the direct PSNR metric for the video quality. For example, with SINR = 15 dB, when the number of SUs is 4 in each group, the EU optimization can achieve about 120% and 20% performance gain compared to the weighted-PSNR and EE optimizations, respectively. It means that the selection of EU as the optimization objective is much qualified for green video transmission over OFDM-based CR systems.

The proportion distribution is shown in Figure 5 for the SUs, who are classified into three categories according to the total received rate; that is, $R_k < R_g^b$, $R_g^b \le R_k < R_g^b + R_g^e$, and $R_k = R_g^b + R_g^e$, $k \in \mathcal{K}_g$. As the average SINR rises, the proportion of SUs, whose rates are lower than the BL rate, decreases evidently, while the proportion of SUs, who achieve the saturated rate $R_g^b + R_g^e$, increases remarkably. It indicates that the "*bandwidth-hungry*" video services can fully utilize the sensed spectrum by our proposed algorithms. In addition, the proportion (the middle green bars) of the SUs, whose rates satisfy $R_g^b \le R_k < R_g^b + R_g^e$, always dominates the proportion distribution except when the average SINR equals 10 dB, which reveals that the relative fairness among SUs can be ensured as a result of the BL rate requirements and the selected PSNR utility function.

5. Conclusion

This paper studies LVM transmission over OFDM-based CR systems, where multiple interference constraints are necessitated to carry out the performance protection for PUs. An EU-based optimization model, which is well tailored for green video delivery, is formulated, and then the BL and EL spectrum assignments are separately proposed for the complexity reduction. Furthermore, the EU-based power allocation algorithm is also proposed by jointly employing fractional programming and subgradient method. Simulation results show that the proposed power allocation algorithm

can converge to the optimal solution rapidly, and LVM greatly outperforms CM, which is attributed to allowing the elastic data reception. Via the proposed algorithms, the sensed spectrum can be fully exploited by "*bandwidth-hungry*" video services, and the EU-based optimization notably surpasses the EE-based optimization in considering the video quality and energy consumption simultaneously. As the future work, multi-EL modeling and the sequential receiving issue for the video transmission will be considered to further explore the video multicast potential over OFDM-based CR systems.

Appendices

A. Proof of Theorem 1

When the optimal solution is obtained and subcarrier n is assigned to group g, if $p_n = 0$, then $r^{\mathrm{e}}_{g,n} = 0$. Otherwise, if $p_n > 0$, $r^{\mathrm{e}}_{g,n} > 0$, and $r^{\mathrm{e}}_{g,n} \notin \mathscr{B}_n$, then sort the K elements of $\mathscr{B}_n$ in descending order and divide the elements in $\mathscr{B}_n$ into two subsets $\mathscr{B}_n^-, \mathscr{B}_n^+$ according to $r^{\mathrm{e}}_{g,n}$, where $\mathscr{B}_n^+$ is defined as $\{x \mid x \in \mathscr{B}_n, x > r^{\mathrm{e}}_{g,n}\}$ and $\mathscr{B}_n^- = \mathscr{B}_n - \mathscr{B}_n^+$. Actually, the elements of $\mathscr{B}_n^+$ correspond to the achievable rates of SUs who can receive the EL data from subcarrier n. For the optimal solution, $p_n > 0$ requires that $\mathscr{B}_n^+$ must be nonempty, because the empty $\mathscr{B}_n^+$ means $r^{\mathrm{e}}_{g,n}$ is greater than all K achievable rates $r_{m|g,n}$ for $1 \le g \le G, m \in \mathscr{K}_g$, and results in the zero receiving rate on subcarrier n for all SUs.

Supposing that the smallest element in $\mathscr{B}_n^+$ is $r^*_{g,n}$, if $r^*_{g,n}$ is selected as the data transmission rate, then all SUs, who are originally able to receive the data from subcarrier n, can reach a higher receiving rate; that is, $r^{\mathrm{e}}_{g,n} \to r^*_{g,n}$, without harming the receiving rate of other SUs. With the nondecreasing utility functions, the substitution of $r^*_{g,n}$ for $r^{\mathrm{e}}_{g,n}$ will increase the total utility while maintaining the power p_n unchanged. This indicates that the EU can be further improved, which contradicts the optimality assumption. Thus, for $p_n > 0$, $r^{\mathrm{e}}_{g,n}$ must be one of the K achievable rates in $\mathscr{B}_n$.

B. Proof of Theorem 3

The constraints C_1, C_2, and C_3 are linear and thereby convex. In addition, the constraint C_4 can be rewritten as $-\sum_{n\in\Theta_g^{\mathrm{b}}} r_n + R_g^{\mathrm{b}} \le 0$, $1 \le g \le G$. The left-hand side of C_4 is also convex since it is the sum of $-r_n$, which is calculated by a convex function, that is, a negative logarithmic function. The remaining task is to prove that $g(\mathbf{p}, \alpha)$ is convex over the feasible region of p_n, $1 \le n \le N$. To do so, a lemma is introduced as follows.

Lemma B.1. *If a function $g(x)$ is concave, a function $h(x)$ is concave, and the function $\widetilde{h}(x)$ is nondecreasing, then the composition function $f(x) = h(g(x))$ is concave as well.*

In Lemma B.1, with $\mathrm{dom}\, h$ denoting the domain of the function $h(x)$, $\widetilde{h}(x)$ is defined as

$$\widetilde{h}(x) = \begin{cases} h(x) & x \in \mathrm{dom}\, h, \\ -\infty & x \notin \mathrm{dom}\, h. \end{cases} \tag{B.1}$$

The proof can be found in Section 3.2.4 of [26].

Recall the expression of R_k; it is the aggregate rate of all the subcarriers which are occupied by SU k; that is, $R_k = \sum_{n\in\Omega_k} B_0 \log_2(1 + p_n\gamma_n)$. As mentioned above, the rate of each item is a logarithmic function with p_n, and therefore R_k is a concave function with p_n. With $U_k(x)$ being nondecreasing and concave, according to Lemma B.1, $U_k(R_k)$ is concave as well, provided that $\widetilde{U}_k(x)$ is nondecreasing. The additional condition on $\widetilde{U}_k(x)$ can be easily satisfied in practice, due to the fact that the utility function $U_k(x)$ is generally defined over the domain of $\{x \mid x \ge 0\}$, and the nondecreasing feature will be preserved during the extension of $U_k(x)$ to $\widetilde{U}_k(x)$. Thus, $-\alpha U_{\mathrm{total}}(\mathbf{p})$ is convex. In combination with the fact that $E_{\mathrm{total}}(\mathbf{p})$ is linear and convex, $g(\mathbf{p}, \alpha)$ is convex over the feasible region of p_n, $1 \le n \le N$, and consequently problem $\mathscr{OP}_2$ belongs to convex optimization ones.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61471059), National High-Tech R&D Program (863 Program 2015AA01A705), Fundamental Research Funds for Central Universities (2014ZD03-01), Special Youth Science Foundation of Jiangxi (20133ACB21007), National Key Scientific and Technological Project of China (2013ZX03003012), and Postgraduate Innovation Fund of SICE for BUPT 2015.

References

[1] P. Pirinen, "A brief overview of 5G research activities," in *Proceedings of the 1st IEEE International Conference on 5G for Ubiquitous Connectivity (5GU '14)*, pp. 17–22, IEEE, Äkäslompolo, Finland, November 2014.

[2] E. Hossain and M. Hasan, "5G cellular: key enabling technologies and research challenges," *IEEE Instrumentation & Measurement Magazine*, vol. 18, no. 3, pp. 11–21, 2015.

[3] A. Osseiran, F. Boccardi, V. Braun et al., "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, 2014.

[4] J. Mitola and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[5] Y.-C. Liang, K.-C. Chen, G. Y. Li, and P. Mähönen, "Cognitive radio networking and communications: an overview," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 7, pp. 3386–3407, 2011.

[6] S. Chen and J. Zhao, "The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 36–43, 2014.

[7] Y. Gao, W. Xu, K. Yang, K. Niu, and J. Lin, "Energy-efficient transmission with cooperative spectrum sensing in cognitive radio networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 7–12, Shanghai, China, April 2013.

[8] T. Zhang and D. H. Tsang, "Cooperative sensing scheduling for energy-efficient cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2648–2662, 2015.

[9] Y. Wang, W. Xu, K. Yang, and J. Lin, "Optimal energy-efficient power allocation for OFDM-based cognitive radio networks," *IEEE Communications Letters*, vol. 16, no. 9, pp. 1420–1423, 2012.

[10] J. Mao, G. Xie, J. Gao, and Y. Liu, "Energy efficiency optimization for ofdm-based cognitive radio systems: a water-filling factor aided search method," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2366–2375, 2013.

[11] S. Wang, M. Ge, and W. Zhao, "Energy-efficient resource allocation for OFDM-based cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3181–3191, 2013.

[12] S. Wang, W. Shi, and C. Wang, "Energy-efficient resource management in OFDM-based cognitive radio networks under channel uncertainty," *IEEE Transactions on Communications*, vol. 63, no. 9, pp. 3092–3102, 2015.

[13] R. O. Afolabi, A. Dadlani, and K. Kim, "Multicast scheduling and resource allocation algorithms for OFDMA-based systems: a survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 240–254, 2013.

[14] N. Rupasinghe and I. Guvenc, "Licensed-assisted access for WiFi-LTE coexistence in the unlicensed spectrum," in *Proceedings of the IEEE Globecom Workshops (GC Wkshps '14)*, pp. 894–899, Austin, Tex, USA, December 2014.

[15] D. T. Ngo, C. Tellambura, and H. H. Nguyen, "Resource allocation for OFDMA-based cognitive radio multicast networks with primary user activity consideration," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1668–1679, 2010.

[16] K. Yang, W. Xu, S. Li, and J. Lin, "A distributed multiple description coding multicast resource allocation scheme in OFDM-based cognitive radio networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 210–215, IEEE, Shanghai, China, April 2013.

[17] K. Yang, W. Xu, S. Li, J. Lin, and W. Wu, "A statistical-CSI-based scheme for multiple description coding multicast in CRNs," *IEEE Signal Processing Letters*, vol. 21, no. 2, pp. 213–216, 2014.

[18] H. Zhang, Y. Zheng, M. A. Khojastepour, and S. Rangarajan, "Cross-layer optimization for streaming scalable video over fading wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 3, pp. 344–353, 2010.

[19] D. Hu, S. Mao, Y. T. Hou, and J. H. Reed, "Scalable video multicast in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 3, pp. 434–444, 2010.

[20] T. Weiss, J. Hillenbrand, A. Krohn, and F. K. Jondral, "Mutual interference in OFDM-based spectrum pooling systems," in *Proceedings of the IEEE 59th Vehicular Technology Conference. VTC 2004-Spring*, vol. 4, pp. 1873–1877, IEEE, May 2004.

[21] H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H.264/AVC standard," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 9, pp. 1103–1120, 2007.

[22] H. M. Radha, M. Van der Schaar, and Y. Chen, "The MPEG-4 fine-grained scalable video coding method for multimedia streaming over IP," *IEEE Transactions on Multimedia*, vol. 3, no. 1, pp. 53–68, 2001.

[23] Z. Shen, J. G. Andrews, and B. L. Evans, "Adaptive resource allocation in multiuser OFDM systems with proportional rate constraints," *IEEE Transactions on Wireless Communications*, vol. 4, no. 6, pp. 2726–2737, 2005.

[24] G. Bansal, M. J. Hossain, and V. K. Bhargava, "Adaptive power loading for OFDM-based cognitive radio systems with statistical interference constraint," *IEEE Transactions on Wireless Communications*, vol. 10, no. 9, pp. 2786–2791, 2011.

[25] W. Dinkelbach, "On nonlinear fractional programming," *Management Science*, vol. 13, no. 7, pp. 492–498, 1967.

[26] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[27] D. P. Bertsekas, *Nonlinear Programming*, Athena Scientific, 1999.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 938191, 7 pages
http://dx.doi.org/10.1155/2015/938191

Research Article

A Cross-Layer-Based Routing Protocol for Ad Hoc Cognitive Radio Networks

Gyanendra Prasad Joshi,[1] Seung Yeob Nam,[1] Chang-Su Kim,[2] and Sung Won Kim[1]

[1] *Department of Information and Communication Engineering, Yeungnam University, 280 Daehak-ro, Gyeongsan-si, Gyeongbuk-do 38541, Republic of Korea*
[2] *School of Business, Yeungnam University, 280 Daehak-ro, Gyeongsan-si, Gyeongbuk-do 38541, Republic of Korea*

Correspondence should be addressed to Sung Won Kim; swon@yu.ac.kr

Received 20 July 2015; Accepted 13 September 2015

Academic Editor: Amiya Nayak

This paper proposes a cross-layer-based routing protocol for mobile ad hoc cognitive radio networks. The routing layer receives the spectrum-availability-related information from the medium access control layer and selects the next hop node on the route according to the spectrum information. This paper examines the expectation of channel switching in a range of scenarios and proposes a novel route selection method to mitigate the frequent channel switching. The proposed protocol distributes the routing overheads among secondary users in the network and prolongs the network lifetime. An extensive simulation was performed to evaluate the proposed approach, and the results showed that the proposed protocol extends the network lifetime and maintains a higher data delivery ratio.

1. Introduction

Protection of the primary user (PU) is the primary concern in cognitive radio (CR) networks. Therefore, secondary users (SUs) need to evacuate the channel immediately whenever the PU arrives on the channel. From the prospective of the routing layer, if a SU is in the active PU's area, it does not necessarily detour the route. Instead, the SU can change the channel, retaining the same route. Rerouting is only necessary whenever a link breaks between two nodes on the route and the link-break condition occurs when there is no common channel between the tagged node and next hop node.

Indeed, changing the channel according to the presence or absence of the PU is a medium access control (MAC) layer issue. The routing layer should focus on selecting the next hop node or complete the route to the destination. Some of the current routing protocols in the literature have not distinguished the routing and MAC layer issues clearly [1–3]. For example, in [1], Challenge-2 and Challenge-3, the author argued that if the PUs arrive on the channel, then the SUs also need to change the established route. However, this argument is partially true. First of all, the number of common channels available can be one of the factors affecting the selection of the next hop node for routing; it is not solely a routing layer issue. The route is not invalid (or the route is not broken) if a PU arrives on a channel currently used by a SU. If a PU is detected on the channel, the node (MAC layer) simply changes the channels. The route is invalid if the PUs occupy all the common channels between two nodes on the route. Cacciapuoti et al. [2] and Talay and Altilar [3] performed a similar assumption for the route invalidation.

In ad hoc cognitive radio networks (CRNs), the spectrum availability has a geospatial correlation. The incumbent spectrum available in a single geographical location might not be available in another geographical location. Therefore, it is necessary for cognitive radio ad hoc routing (CRAR) protocols to obtain the spectrum information from the MAC layer to calculate the route cost. To elaborate, the simplest scenario is described here.

Assume that there are four SUs in a single plane, the sender node (A), intermediate nodes (I_1, I_2), and destination node (B), as shown in Figure 1. Each node has only one idle common channel. When I_1 receives a packet from node A on channel C_1, it needs to tune its transceiver to channel C_2 to forward the packet to I_2. Again, I_1 needs to switch back to channel C_1 to receive another packet. Switching a channel for

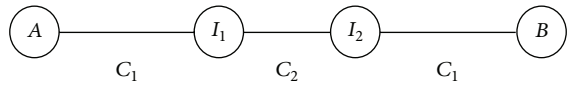


Figure 1: Simple scenario of four-node ad hoc cognitive radio network.

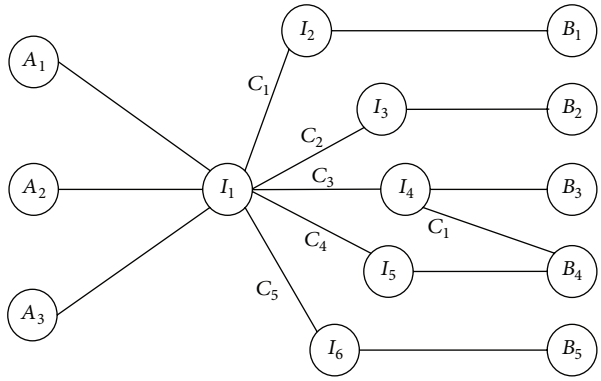


Figure 2: Multiple sources and destination scenarios.

each packet is more expensive in terms of the delay, particularly to the CR node, which has only one or two transceivers.

This situation can be bad if the intermediate node needs to forward the packets for different destinations in different channels, as shown in Figure 2. The transceiver of node, I_1, needs to switch the channel several times to send packets in different channels and a delay may increase exponentially, leading to a channel bottleneck problem.

Therefore, the channel switching delay due to frequent channel hopping can be mitigated if the spectrum-availability-related parameter can be included in the route cost.

2. Related Work

The reports of CR in the literature focused mainly on the physical (PHY) or MAC layer issues. The routing protocols for cognitive radio ad hoc networks have received less attention than other areas. Most routing protocols in the literature are an extension of multichannel routing protocols for ad hoc networks with the spectrum availability parameter. Nevertheless, there are several prospects, reviews, and position papers in the literature [4–7]. Cesana et al. [5] discussed the challenges and solutions in routing for cognitive radio networks. The authors categorized the cognitive radio routing schemes into full spectrum knowledge-based routing and local spectrum knowledge-based routing. They discussed several aspects of cognitive radio routing. Al-Rawi and Yau [6] discussed the challenges and categorized some of the cognitive radio routing schemes. Zhang et al. [7] classified and analyzed some of the existing routing protocols and compared their characteristics. Joshi et al. [8] also described some of the routing-related issues in cognitive radio wireless sensor networks.

Although many authors have not mentioned that their routing protocol is a cross-layer protocol [2–5], network layer receives information of available common channel from the MAC layer. Cacciapuoti et al. [2] proposed two versions of cognitive ad hoc on-demand distance vector (CAODV) protocols, which are an extension of AODV [9]. The first approach, called intEr-Route dIversity CAODV (ERI-CAODV), uses different channels for different routes, but each route is restricted to evolve through the same channel. The second approach is called intrA-Route dIversity (ARI-CAODV), which relaxes the constraint in ERI-CAODV that the same channel must be available in the entire route. In ARI-CAODV, intermediate SU sends the route a request (RREQ) in every idle channel.

Both approaches have several drawbacks. In both protocols, rerouting is initiated whenever a PU arrives on the channel. CAODV has a route error packet called the primary user route error (PU-RERR) packet, which is generated whenever a PU is detected on the channel currently used by SUs. The PU-RERR is broadcasted to the neighbors through the same channel occupied by the PU, which is a contradiction of the original principle of cognitive radio networks. CAODV does not take energy consumption into consideration. Further, in ERI-CAODV, finding the same channel in each link is not always possible. In ARI-AODV, sending RREQ in every idle channel is the waste of bandwidth resources.

Talay and Altilar [3] proposed a self-adaptive routing (SAR) protocol by extending the protocol by Cheng et al. [10] based on AODV. This protocol is an underlay approach that adjusts the transmission range of a SU whenever required and possible. This protocol assumes that all SUs are in the proximity of the minimum transmission range. The SAR assumes route failure if a PU is detected and attempts to calculate the distance between the PU and SU and adapts the transmission range. However, adapting the transmission range is difficult in a heterogeneous network. Therefore, this study compared the proposed protocol with the abovementioned ARI-AODV and SAR.

Most of the papers mentioned above did not consider the temporal variations of the spectrum availability. In some studies [11–14], the authors discussed the common control channel for routing-related packets (e.g., RREQ/RREP/RERR/RREP, etc.), but they did not mention clearly whether there should be an additional common control channel (CCC) compared to the general CCC used for the MAC layer control packets or the same CCC can be used for the routing packets. Generally, in CRNs, the CCC is necessary to inform of the arrival of the PU and negotiate for the data channels, which is a MAC layer issue. Some of the papers discussed above invalidate the route if the PU arrives on the channel. Invalidating the route is not really necessary upon the arrival of the PU on the channel, because there may be other idle channels available. This essentially is an MAC layer issue.

The remainder of the paper is organized as follows. Section 3 analyzes the estimated number of channel switching. The section validates one of the design parameters and explains why the selection of a common channel in the last hop and the next hop is necessary. Section 4 details the proposed protocol. Section 5 verifies the validity of the proposed protocol and Section 6 concludes the paper.

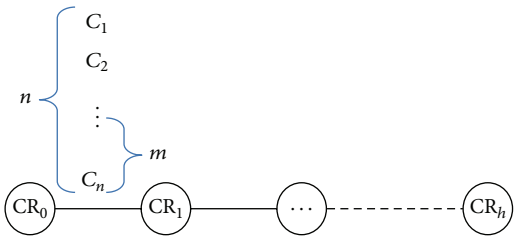


Figure 3: Scenario for the analysis.

3. Analysis of Estimated Number of Channel Switching

To estimate the number of channel switching, the simplest scenario shown in Figure 3 was considered. Let h be the number of hops between the source and destination (end-to-end hops) and n the number of data channels for each link. This study assumed that all the channels were idle on each link for this case. The aim was to calculate the average number of switches needed to transmit a packet from the source to the destination. Let S denote the number of switches required. The term "smart-selection" refers to a method to select the same channel in each link to minimize the number of channel switches.

Case 1.

Smart-Selection. If the same channel is selected in each link with the *smart-selection* on each link to minimize the number of switches, then

$$E[S_s] = 0, \tag{1}$$

where S_s means the number of channel switches required when the channels are selected in a smart manner.

Random Selection. If the channels are selected randomly on each link, then $E[S_r]$ can be calculated in the following manner:

$$\begin{aligned} E[S_r] &= \sum_{i=2}^{h} 1 \cdot \Pr(\text{switching on link } i) \\ &= \sum_{i=2}^{h} 1 \\ &\quad \cdot \Pr(\text{channel on link } i-1 \neq \text{channel on link } i) \\ &= \sum_{i=2}^{h} \left(1 - \frac{1}{n}\right) = (h-1)\left(1 - \frac{1}{n}\right), \end{aligned} \tag{2}$$

where

$$\begin{aligned} &\Pr(\text{switching on link } i) \\ &= \Pr(\text{channel on link } i-1 \neq \text{channel on link } i) + \Pr(\text{channel on link } i-1 \text{ is not in use on link } i) \\ &\quad \times \Pr(\text{link } i \text{ uses a different channel } (\textit{Independence assumption.}) \mid \text{channel on link } i-1 \text{ is not in use on link } i) \end{aligned} \tag{5}$$

$$= \frac{m}{n} + \left(1 - \frac{m}{n}\right)\left(1 - \frac{1}{n-m}\right) = \frac{m}{n} + \frac{n-m-1}{n} = 1 - \frac{1}{n}.$$

where S_r means the number of channel switches required when the channels are randomly selected. Because channel switching is related directly to the delay; (2) shows that the random channel selection strategy is more expensive in terms of channel switching even in a very simple scenario.

Case 2. Assume that among n channels, m channels are occupied by the PUs (i.e., the channels are busy or in use). That is, there are $n-m$ idle channels on each link. m channels are selected randomly among n channels.

Smart-Selection. The channel on each link is selected so that the same channel can be used on as many hops as possible from the source node. Let X be the maximum number of hops that can go without switching.

Let us consider the range of X for the proposed scheme. If the number of hops between the source and the destination is h, then X has an upper bond of h. X will have the minimum value when m channels on the ith link are selected to minimize the overlapping between the channels on the ith link and the set of channels selected in the previous links. Thus the lower bound of X can be represented as

$$X \geq \left\lceil \frac{n}{m} \right\rceil - 1. \tag{3}$$

$\lceil X \rceil$ means the smallest number, which is greater than or equal to X. Therefore, $\lceil n/m \rceil - 1$ becomes a lower bound of X. Then, it is possible to show that

$$S_s \leq \left\lceil \frac{h}{\lceil n/m \rceil - 1} \right\rceil - 1. \tag{4}$$

Random Selection. If the channels are selected randomly on each link, then $E[S_r]$ can be calculated as follows:

Thus, the following can be obtained:

$$E[S_r] = \sum_{i=2}^{h} 1 \cdot \Pr(\text{switching on link } i) = \sum_{i=2}^{h} \left(1 - \frac{1}{n}\right) = (h-1)\left(1 - \frac{1}{n}\right). \quad (6)$$

It can be observed that (6) is identical to (2). The reason is that if m busy channels are selected randomly on each link and one channel for a new connection is selected randomly from the remaining $n - m$ channels, then the situation is not different from the case where one channel is selected randomly without any preoccupied channel. This is valid because of the randomization of m busy channels.

Let us compare (4) and (5) for large n and small m, particularly when $m = 1$. If an algorithm that can select a channel in such a smart way that every node on the route selects the same channel whenever possible (i.e., smart-selection) can be used, then the expected number of switching on a given path is obtained as from (4):

$$E[S_s] \leq \left\lceil \frac{h}{n-1} \right\rceil - 1, \quad (7)$$

where S_s is the number of switching for the case where the channels are selected in a smart way:

$$E[S_r] = (h-1)\left(1 - \frac{1}{n}\right) \approx h - 1, \quad (8)$$

where S_r is the number of switches for the case where the channels are selected randomly on each link. Therefore, $E[S_s]$ can be much smaller than $E[S_r]$ in this case.

Equation (8) means that when the channels are selected randomly, switching is likely to occur on every link as the number of channels (n) becomes large.

Equation (7) is a special case of (4), obtained especially for $m = 1$. An interesting result can be obtained when $m = 1$. If $n = h + 1$,

$$E[S_s] \leq \left\lceil \frac{h}{(h+1)-1} \right\rceil - 1 = 0. \quad (9)$$

That is, $E[S_s] = 0$ when $n = h + 1$. This means that if the number of channels (n) is sufficiently large compared to the number of hops (h) and $m = 1$, then the number of switches in the proposed scheme can be reduced to zero. Figure 4 illustrates this case, particularly when $h = 4$.

4. Proposed Routing Protocol

From the analysis, it was observed that channel switching can be mitigated considerably with the smart-selection. Therefore, this study proposes a cross-layer-based cognitive radio routing (CLC-routing) protocol. The proposed protocol hereafter is called *CLC-routing*. This protocol receives channel availability-related information from the MAC layer and selects the next hop node, which has a common channel as the previous link. The proposed protocol also prolongs the network lifetime by distributing the routing workload among the SUs.

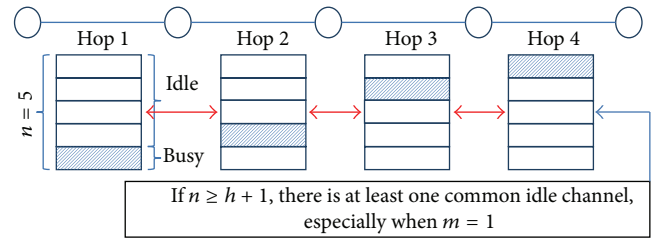


Figure 4: Illustration of the condition that guarantees no switching on an end-to-end path under the proposed channel selection scheme.

The Proposed Protocol Has the following Properties

(i) It does not detour if the PU arrives on the channel; rather it tries to hop the channel and invalids the link only if all the channels are occupied by the PU.

(ii) It tries to select the same channel that is selected in the previous link, so that no channel switching is needed to receive and forward a packet.

(iii) It selects a route with the cost considering spectrum availability, battery capacity of SUs, and length of the route.

(iv) It distributes the routing overload among the nodes in the networks by invaliding the route.

Advantages of the Proposed Protocol

(i) Extending the network lifetime.

(ii) Decreasing the MAC layer delay.

(iii) Mitigating frequent rerouting.

4.1. Protocol Description. In this work, the well-known dynamic source routing protocol for multihop wireless ad hoc networks is extended [15], and a cross-layer protocol that obtains the spectrum-related parameter from the MAC layer and selects the next hop is proposed. The predictive MAC (PMAC) protocol [16] was used to receive the channel information. The PMAC maintains the channel status table and predicts the PU's arrival on the channel. The protocol also ranks the channel from the best channel to the worst channel according to a range of factors. The proposed protocol calculates the cost of the route considering (i) the number of available common channels, (ii) the residual battery of the SU, and (iii) the number of hops. The cost of a node according to the residual battery can be calculated as in the following:

$$\text{Cb}_{\text{CR}_i} = \left(\frac{b_{\text{CR}_i}^{\max}}{b_{\text{CR}_i}^{\text{res}}(t)} \right)^{\beta}, \quad (10)$$

where Cb_{CR_i} is the cost due to the battery capacity of the cognitive radio node, CR_i, $b_{\text{CR}_i}^{\max}$ is the full capacity of the battery of node, i, $b_{\text{CR}_i}^{\text{res}}(t)$ is the residual battery capacity of the CR_i, and β is the weighting factor.

4.2. Route Discovery. A SU node that has packets to send begins broadcasting a route request (RREQ) packet. The RREQ contains channel information of the link $i - 1$. The MAC attempts to select the same channel for link i as selected in the link $i - 1$ if the channel is available for the SUs.

Once an intermediate SU receives a RREQ packet, the SU rebroadcasts the packet if (a) the SU has no route to the destination in its cache, and (b) it has not already broadcast the RREQ with the same sequence number and sender ID. Otherwise, the SU drops the RREQ. Each intermediate SU calculates the link cost from its own $\mathrm{Cb}_{\mathrm{CR}_i}$ and the cost due to the available common channels (C_i), as expressed in the following:

$$C_l = \alpha \cdot C_i + \mathrm{Cb}_{\mathrm{CR}_i}, \tag{11}$$

where C_l is the link cost and α is the weighting factor. C_i is a factor of total number of available channels that can be utilized by the SUs and number of common channels. The intermediate SU nodes add this to the path cost in the header of the RREQ packet.

When an intermediate SU node receives a RREQ packet, it starts a timer and keeps the cost in the header of that packet as the minimum cost ($C_{\min}$). If additional RREQs arrive with the same destination and sequence number, the cost of the newly arriving RREQ packet is compared with the $C_{\min}$. If the new packet has a lower cost, $C_{\min}$ is changed to this new value and the new RREQ packet is forwarded. Otherwise, the new RREQ packet is dropped.

4.3. At the Destination SU Node. After the first packet destined to it is received, the SU starts the timer and waits for the other RREQs. After the timer expires, the destination SU compares the route. The SU generates a route reply (RREP) with the route with the minimal cost. The route cost is calculated using the following:

$$C_{\mathrm{Rt}} = \sum_{i \in \mathrm{Rt}} C_l + \delta \cdot H, \tag{12}$$

where C_{Rt} is the route cost, H is the number of hops, and δ is the weighting factor.

4.4. Route Maintenance. The route in the CR ad hoc networks is more prone to breaking than ad hoc networks because the PUs can occupy the channel anytime. When all common channels are occupied by PUs and no common channel is available between two intermediate nodes, the node has to generate a route error (RERR) packet. The other reasons to start the route maintenance are energy depletion and node mobility, as in the conventional ad hoc networks.

SUs generate RERR message immediately if the number of common channels available is zero for the next hop. On the other hand, if the cost difference between current cost $\mathrm{Cb}_{\mathrm{CR}_i}$ and the cost at the route discovery time is higher than the given threshold value, the SU generates a RERR packet after time t to inform the source that the route is invalid. This is because the frequent route invalidation is expensive in terms of delay and throughput. After receiving the RERR packet, the source begins rerouting by broadcasting a RREQ packet.

This strategy of generating a RERR considering the difference between the current cost $\mathrm{Cb}_{\mathrm{CR}_i}$ and the cost at the route discovery time balances load among SU nodes by enforcing a change in route. Therefore, it distributes the workload and extends the network lifetime.

5. Simulation Results

In the present work, for the simulation, the ns-2 [17] was extended for ad hoc cognitive radio network scenario. The network consists of 80 SUs and 20 PUs confined in 1000 × 1000 m^2 area. The transmission range of each node is assumed to be 50 m. Six flows of CBR traffic are generated over the UDP at various data transmission rates from 100 kbps to 1 Mbps. The packet size is 512 bytes. A limited node mobility of 5 m/sec was used to evaluate the protocol's performance. The number of licensed channels available for the opportunistic use was set to 10 and one additional control channel (i.e., CCC) for the MAC layer control packets exists. The additional CCC is free from PUs packets and is only used for the MAC control packets of SUs. PUs use an ON/OFF arrival model. As described in the protocol description, the PMAC was used as a MAC layer protocol. PMAC requires two transceivers: one for the data channels and one for CCC. Most of the MAC layer parameters from the PMAC were used. The time is divided into beacon intervals of 100 ms, where 20 ms is for channel negotiation and 80 ms is for the data packets. The simulation runs for 10,000 seconds. Each simulation is run 10 times and the averaged values are presented in the graphs.

The SU lifetime, packet delivery ratio, throughput, and end-to-end delay were examined as the quantitative metrics for evaluating the performance of the proposed protocol. No de facto standard routing protocol exists for cognitive radio networks to compare with the proposed protocol. Therefore, this study compared the proposed CLC-routing protocol with the *CLC-routing* without selecting the channels randomly in each link (we call it *CLC-routing-random*), ARI-AODV [2], and SAR [3]. Although ARI-AODV and SAR both were cross-layer approaches, they did not mention details of the MAC protocols they used. This was modified slightly to make it compatible. Therefore, the result can be different from the original paper.

Figure 5 shows the number of dead nodes with and without spectrum information. In the evaluation, a node is dead if it has a battery power less than five percent of $b_{\mathrm{CR}_i}^{\max}$. In the simulation, the first node of CLC-routing, CLC-routing-random, SAR, and ARI-AODV dies at 5492, 4751, 3498, and 3449 seconds, respectively, after the simulation begins. SAR and ARI-AODV do not consider the network lifetime as a primary concern. A SU node on the route works actively until the SU node has remaining battery. Therefore, SUs are exhausted and die soon, leading to network partitioning and rerouting. On the other hand, in the CLC-routing protocol, the node changes route according to the current energy of the node. CLC-routing-random switches the channel more frequently than CLC-routing and it consumes more energy. Throughout the simulation, fewer nodes died in the proposed

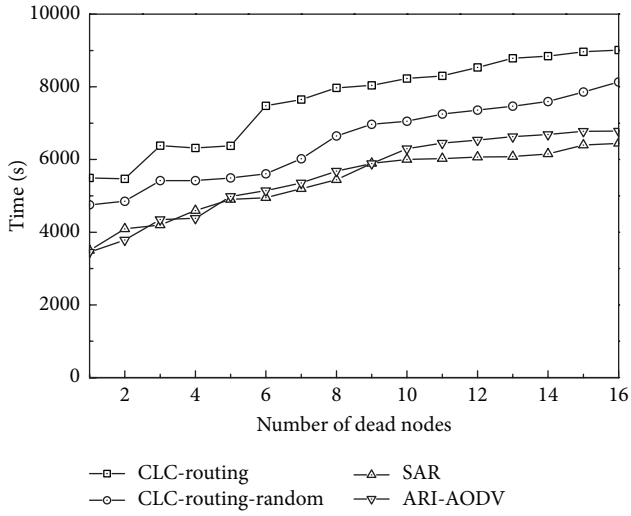


Figure 5: Number of dead nodes with and without spectrum information.

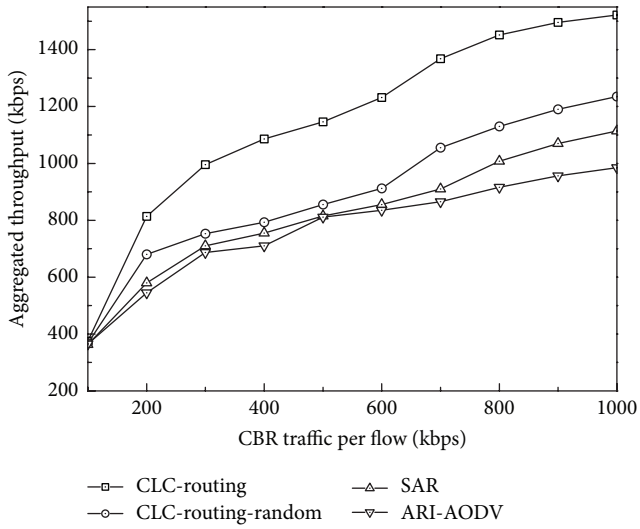


Figure 7: Network throughput in various traffic rates.

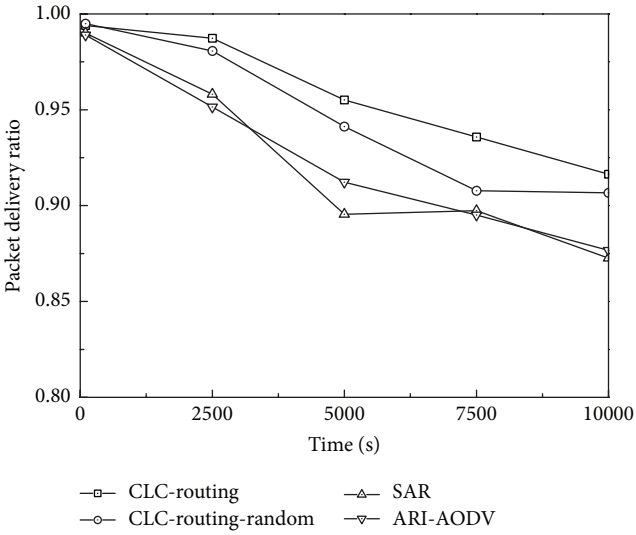


Figure 6: Packet delivery ratio.

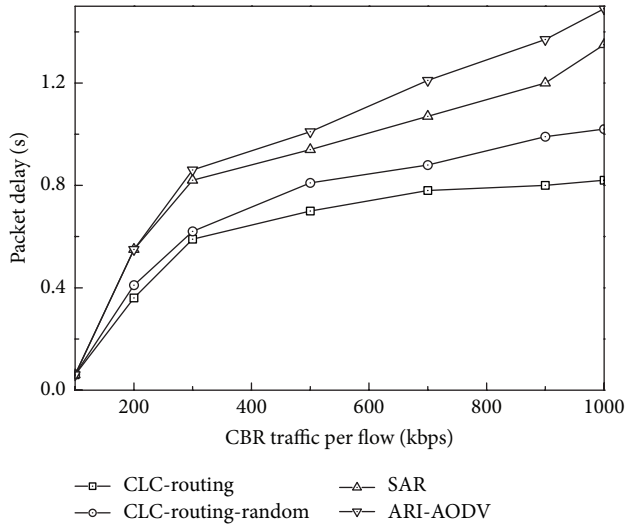


Figure 8: Average end-to-end delay in various traffic flows.

approach. This shows that the energy depletion rate can be mitigated with the proposed strategy.

Figure 6 shows the packet delivery ratio. This was calculated as the number of packets received by the destination divided by the number of packets that originated from the source. The results show that CLC-routing achieves a higher packet delivery ratio than the remaining simulated protocols. The reasons include frequent rerouting because of the network partitioning caused by energy depletion, route invalidation, even if channels are available in the intermediate nodes in SAR and ARI-AODV, frequent channel switching in CLC-routing-random due to random channel selection, and a lack of cooperation with the MAC in a cross-layer approach.

Figure 7 shows the aggregated throughput of the *CLC-routing*, *CLC-routing-random*, SAR, and ARI-AODV. Aggregated throughput was calculated as the average rate of successful packet delivery over six communication flows. Because of the less rerouting, less network partitioning, and less channel switching, CLC-routing achieved a higher throughput than the remaining three approaches. Because the size of outgoing packet queue is fixed in the simulation, SUs cannot deliver all the packets generated with higher traffic flow. Therefore, the protocols with higher network partitioning and frequent channel switching achieve a lower aggregated throughput.

Figure 8 compares the average end-to-end delay. The average end-to-end delay was calculated as the average time between the transmission of data packets at the source SU and the successful reception of the packet at the destination SU. This is because higher CBR traffic rate generates more interference, so the end-to-end delay increases. SAR and ARI-AODV have a higher average end-to-end delay because they invalidate the route and reroute frequently. Although

this study considered two transceivers, one transceiver was dedicated to the CCC and the other transceiver (called data transceiver) was only used for data transfer. If the data receiving channel and data sending channel are different, then the average end-to-end delay increases because of the frequent mandatory channel switching.

6. Conclusion and Future Works

This paper presented a cross-layer-based cognitive radio routing protocol for cognitive radio networks. Because rerouting is expensive in terms of energy, delay, and throughput, it is better to select a route in such a way that requires less channel switching. Excessive workload on a particular node causes network partitioning and induces repeated rerouting. The proposed protocol incorporated power awareness and spectrum information with a cross-layer approach. Future work will introduce fuzzy-logic-based channel selection.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the 2015 Yeungnam University Research Grant.

References

[1] P. Bandyopadhyay, "Routing in cognitive radio ad-hoc networks," Tech. Rep., University of Helsinki, Helsinki, Finland, http://www.hiit.fi/u/bayhan/uh/StudentReports/Payel_Bandyopadhyay_RA_finalreport.pdf.

[2] A. S. Cacciapuoti, M. Caleffi, and L. Paura, "Reactive routing for mobile cognitive radio ad hoc networks," *Ad Hoc Networks*, vol. 10, no. 5, pp. 803–815, 2012.

[3] A. C. Talay and D. T. Altilar, "Self adaptive routing for dynamic spectrum access in cognitive radio networks," *Journal of Network and Computer Applications*, vol. 36, no. 4, pp. 1140–1151, 2013.

[4] Y. X. Chen, "Application and research of routing protocol based on AODV in cognitive radio," *Applied Mechanics and Materials*, vol. 336–338, pp. 1776–1780, 2013.

[5] M. Cesana, F. Cuomo, and E. Ekici, "Routing in cognitive radio networks: challenges and solutions," *Ad Hoc Networks*, vol. 9, no. 3, pp. 228–248, 2011.

[6] H. A. A. Al-Rawi and K.-L. A. Yau, "Routing in distributed cognitive radio networks: a survey," *Wireless Personal Communications*, vol. 69, no. 4, pp. 1983–2020, 2013.

[7] L. Zhang, X.-W. Zhou, and J.-P. Wang, "Routing protocols for cognitive radio networks: a survey," *Journal of Chinese Computer Systems*, vol. 31, no. 7, pp. 1254–1260, 2010.

[8] G. P. Joshi, S. Y. Nam, and S. W. Kim, "Cognitive radio wireless sensor networks: applications, challenges and research trends," *Sensors*, vol. 13, no. 9, pp. 11196–11228, 2013.

[9] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, New Orleans, LA, USA, February 1999.

[10] G. Cheng, W. Liu, Y. Li, and W. Cheng, "Spectrum aware on-demand routing in cognitive radio networks," in *Proceedings of the 2nd IEEE international symposium on new frontiers in dynamic spectrum access networks (DySPAN '07)*, pp. 571–574, Dublin, Ireland, April 2007.

[11] R. D. Pochhi, R. P. Deshmukh, and P. D. Dorge, "An efficient multipath routing protocol for cognitive ad hoc networks," *International Journal of Advanced Electrical and Electronics Engineering*, vol. 1, no. 3, pp. 57–62, 2012.

[12] C. Xin, B. Xie, and C.-C. Shen, "A novel layered graph model for topology formation and routing in dynamic spectrum access networks," in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05)*, pp. 308–317, Baltimore, Md, USA, November 2005.

[13] R. Pal, "Efficient routing algorithms for multi-channel dynamic spectrum access networks," in *Proceedings of the 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '07)*, pp. 288–291, IEEE, Dublin, Ireland, April 2007.

[14] G. Cheng, W. Liu, Y. Li, and W. Cheng, "Joint on-demand routing and spectrum assignment in cognitive radio networks," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, pp. 6499–6503, Glasgow, UK, June 2007.

[15] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks," in *Ad Hoc Networking*, chapter 5, pp. 139–172, Addison-Wesley, 2001.

[16] G. P. Joshi, S. Y. Nam, and S. W. Kim, "Decentralized predictive MAC protocol for Ad Hoc cognitive radio networks," *Wireless Personal Communications*, vol. 74, no. 2, pp. 803–821, 2014.

[17] The network simulator, http://www.isi.edu/nsnam/ns/.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 730762, 10 pages
http://dx.doi.org/10.1155/2015/730762

Research Article

Sensor Virtualization Module: Virtualizing IoT Devices on Mobile Smartphones for Effective Sensor Data Management

JeongGil Ko,[1] Byung-Bog Lee,[2] Kyesun Lee,[2] Sang Gi Hong,[2] Naesoo Kim,[2] and Jeongyeup Paek[3]

[1]*Department of Software Convergence Technology, Ajou University, Suwon 16499, Republic of Korea*
[2]*Electronics and Telecommunications Research Institute (ETRI), Daejeon 34129, Republic of Korea*
[3]*School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, Republic of Korea*

Correspondence should be addressed to Jeongyeup Paek; jpaek@cau.ac.kr

Received 15 May 2015; Accepted 3 August 2015

Academic Editor: Sung Won Kim

The vision of the *Internet of Things (IoT)* is coming closer to reality as a large number of embedded devices are introduced to our everyday environments. For many commercial IoT devices, ubiquitously connected mobile platforms can provide global connectivity and enable various applications. Nevertheless, the types of IoT resource-utilizing applications are still limited due to the traditional stovepipe software architecture, where the vendors provide supporting software on an end-to-end basis. This paper tries to address this issue by introducing the *Sensor Virtualization Module (SVM)*, which provides a software abstraction for external IoT objects and allows applications to easily utilize various IoT resources through open APIs. We implement the SVM on both Android and iOS and show that the SVM architecture can lead to easy development of applications. We envision that this simplification in application development will catalyze the development of various IoT services.

1. Introduction

Low-power embedded sensor networking platforms will soon be deployed for various application purposes in our everyday environments. On large scale, applications such as smart power-grids [1–3], smart city management [4], home and building automation [5, 6], wireless sensor networks [7, 8], and the newly proposed concept of Industry-4.0 [9, 10] will quickly increase the number of embedded computing platforms dramatically. Embedded computing platforms for these applications will be deployed in a way such that the nodes or networks that consist of these systems will have a way to interconnect themselves with the larger Internet architecture [11, 12]. With such advances in embedded devices and networks, increase of computational power, and the ability to interconnect with other devices, the concept of *Internet of Things (IoT)* has emerged. These IoT devices will mostly utilize standard protocols and mechanisms to communicate with the Internet and transport their data to consumers and services in the cloud [13]. To access these IoT devices, a service providing component on the cloud will advertise the resources of these devices for applications to discover and utilize. The ability to connect, communicate with, and remotely manage millions of networked, automated devices via the Internet has opened the potentials for the development of various applications that impact our everyday lives.

Nevertheless, the concept of IoT means more than just devices connecting to the global Internet. There will be another class of IoT devices with *some* radio connectivity that can connect to nearby devices for local communication but not to the global Internet by itself. Not only will miniature sized IoT devices be deployed as network-scale services but we will also enjoy many personalized IoT services which involve only a small number of devices with such limited connectivity. As numerous interconnected devices that can sense and control are embedded closely to our living environments, we envision that there will be a larger number of these "connection-limited" devices that allow more local and personalized applications to be designed. Examples of such

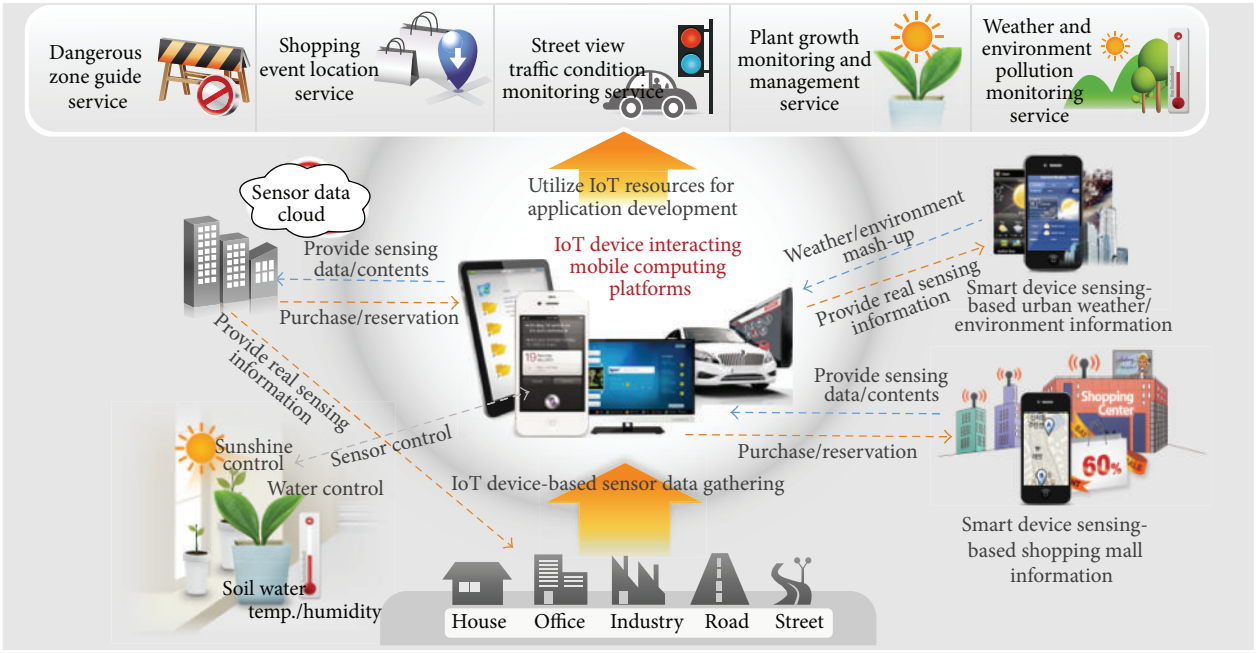


FIGURE 1: Example applications where IoT platforms are interacting with mobile computing platforms.

include IoT devices for personal health exercise management and home monitoring and control.

Due to their size, scale, and resource constraints, devices manufactured for these services are unlikely to provide global connectivity by themselves. Luckily we can easily find many ubiquitously connected mobile computing platforms (e.g., smartphones, tablets) [14]. Furthermore, many of the low-resource IoT devices are designed so that they interact with and through these mobile platforms. Recent work by Park et al. shows that the computational power of current-day smartphones is capable of supporting an even more diverse set of wireless standards using cognitive or software radios [15]; thus, we will soon be seeing such mobile platforms interact heavily with sensing systems using various wireless standards. By connecting IoT devices to these mobile computing platforms, we can quickly realize various mobile platform-based IoT applications. And with the mobile computing platforms' global connectivity, we can easily expose IoT resources globally to allow remote platforms and services to utilize local IoT devices. Figure 1 illustrates examples of such application scenarios where individual IoT devices are connected to user-controlled mobile devices and an associated cloud service takes the role of exposing the IoT resources for other services to reuse. These IoT devices exploit the ubiquitous connectivity of a mobile platform to gain the always-on connectivity required to reach other destinations on the Internet.

While being an attractive scenario, however, many of these IoT devices interacting with mobile devices today can only interface with a software stack that is designed by the manufacturer because the software architecture of these devices mostly takes a "stovepipe" approach, where the vendor of the IoT device provides a complete stack of (closed) software implementation to fully exploit their functionalities [16]. In such a software design, it is difficult for various third-party applications to fully utilize the IoT devices since vendor-provided APIs are usually limited. Furthermore, this restricts resource sharing among different applications, not only for applications internal to a single mobile platform, but also for external applications running in the cloud or on remote smartphones. By breaking down the bricks of the software "stovepipe" and by gaining the ability to handle such information in a more uniform manner, we can allow the same set of IoT devices to be shared, used, and managed in a more flexible way. This will increase their usability in various scenarios, and a more diverse set of applications can be developed and distributed.

This paper introduces the *Sensor Virtualization Module (SVM)*, designed to provide an abstraction for accessing, managing, and sharing the data and resources provided by embedded IoT devices. The proposed *SVM* not only provides global connectivity and service exposure to the Internet for IoT devices but also provides a set of open APIs for mobile applications to utilize and provides ways to design an application server on the cloud for mobile computing platforms or Internet-based services to access remote IoT resources. Furthermore, the *SVM* also allows conflict resolution between different IoT resource requests to allow efficient sharing of IoT resources across multiple IoT applications and also provides a feature that allows creating virtual IoT devices using sensor data mash-up. Finally, *SVM* includes software reprogramming capability that supports software update of both the IoT device and also the mobile computing platform to which local IoT devices are connected.

Using a prototype *SVM* implementation, this paper also introduces a number of applications that can benefit from the resource sharing functionality that the *SVM* provides.

The remainder of this paper is structured as follows. In Section 2 we describe the *SVM* architecture and explain the two important features of *SVM*: creating virtual IoT device for sensor data mash-up and software reprogramming. Then in Section 3, we present two application case studies that make use of and benefit from the *SVM* architecture: sensor data management application and the home appliance management application. Finally, we summarize our work and discuss future research directions in Section 5.

2. Architecture

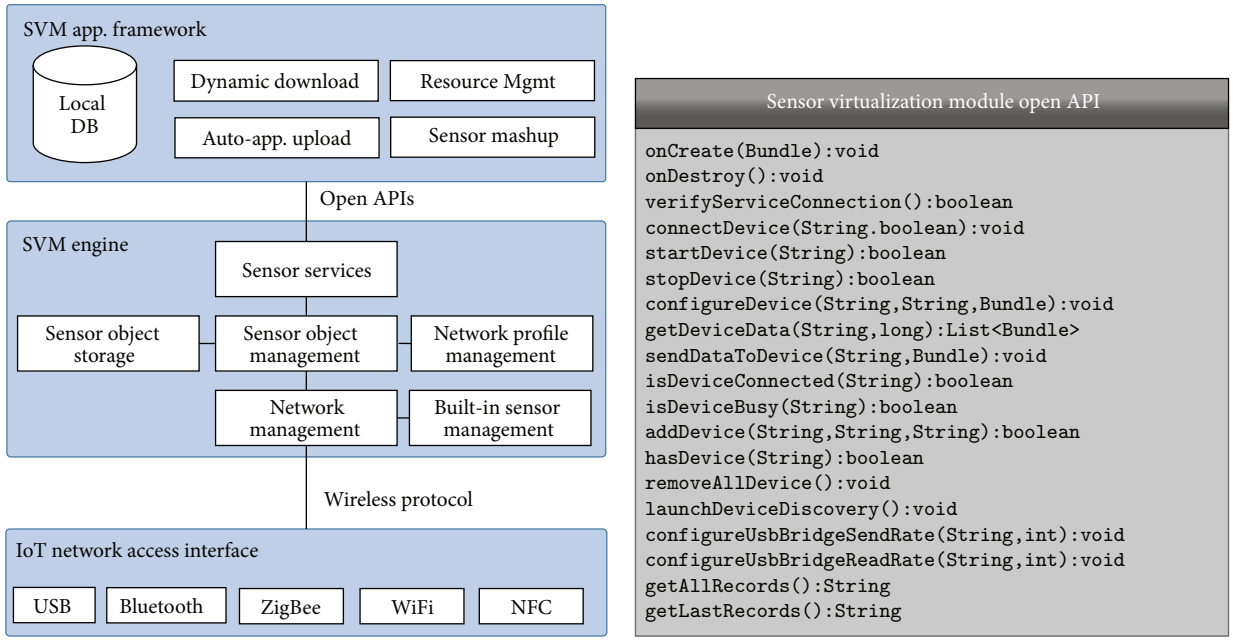
To address the aforementioned challenges, this section introduces the architecture of the *Sensor Virtualization Module (SVM)*, which is designed to provide individual external IoT devices with the connectivity, exposure, and management features required to be effectively utilized over various applications. By external IoT devices, we mean embedded devices such as sensor, actuators, and home appliances with some form of networking and computation capabilities to interconnect and communicate with other local devices, but without direct global connectivity to the Internet and not internal to a mobile device with global connectivity.

2.1. Sensor Virtualization Module. Even in the market today, we see a variety of IoT devices that report their data to services on the Internet using the connectivity of a mobile computing platform. With the proliferation of user-friendly mobile and web applications, this trend will increase. In scenarios where a mobile device takes a significant role for IoT platforms, it is important that the mobile device manages its "reachable" resources efficiently so that the resources provided by IoT devices can be easily accessed, controlled, and shared by various applications.

To address this issue, we design *SVM*, which takes on the role of providing an abstraction for IoT resources that a mobile computing platform can access in its local network. Specifically, *SVM* provides support for applications to access the external IoT resources by first abstracting the network interfaces. For this, upon request from upper-layer applications, the *SVM* engine starts a device discovery phase in which it activates all possible network interfaces to search profiles of IoT devices within reach. Based on the result of this device discovery, the *SVM* engine formulates device object handlers for each identified IoT device. These handlers include information on the name of the device, networking interface, network address, and other device specific profiles. The object handlers are then advertised to the applications, allowing them to select the devices they wish to connect with. As a result of this process, applications can access external IoT devices without knowing how the devices are physically connected. We illustrate the software architecture of our proposed *SVM* in Figure 2(a).

SVM simplifies application development by providing an abstraction of the IoT devices that are present in the local field. In other words, *SVM* makes it look as if the external devices are on-board sensor components such as accelerometer, gyro, GPS, or camera. When applications interconnect with the *SVM* layer, a set of open APIs are provided, as exemplified in Figure 2(b), to the applications for them to interact with the *SVM* layer and to easily access these resources. For example, `launchSensorDiscovery()` API searches for all the external physical sensors that can be connected to the smart device via any of the network access interfaces (e.g., Bluetooth, WiFi, and ZigBee) on the smart device and provides a list of those sensors. `connectDevice(string)` API takes the identifier (e.g., MAC address) as an argument and connects to the external sensor and creates an object within the memory of the smart device. Also, `getDeviceData(string,long):List<bundle>` API takes the sensor identifier and the maximum number of data readings to take as the arguments, reads the sensor data from the external sensors as a list of data items, and inserts them into the internal memory within the sensor data object at the smart devices. (Full API documentation list can be found in the ETRI internal technical report and can be given upon request.) While we expect the application to already understand the format of the incoming data from the external IoT device, an additional data translating module in *SVM* can be used to convert device specific data format to a common XML format. In other words, this allows the users to freely design and utilize their own application layer protocol, such as CoAP. The focus on the *SVM* design was to minimize restrictions to the application system developers while freeing them from the fuss of dealing with low-level communication and networking details in designing an IoT application system. Overall, the use of the *SVM* makes the development process of smart device applications that utilize external IoT devices easier.

Although this process allows easy access to external IoT devices via mobile platform from various applications, the increase in the number of interacting applications can result in conflicts among resource requests. For example, applications *A* and *B* can each ask for data from the same IoT device but ask for it to be retrieved at different time intervals or may potentially request the device to be actuated in different ways. However, since such application level algorithms are not enforced by any standardization body, we cannot assure that these conflicts will be properly processed at the end-device level. As a result, besides managing the connectivity, another major role of the *SVM* engine is to resolve such conflicts caused by multiple requests from different applications. When multiple applications make conflicting requests, *SVM* runs its rule-engine within the `Sensor Object Management` module to select the best option to satisfy most of the incoming requests. The conflict manager of the `Sensor Object Management` operates based on a policy which an administrator user can input at runtime. For example, application *A* may ask for sensor readings every 10 minutes, and a different application *B* may ask for sensor readings every 5 minutes, both from the same external IoT device. In this case, the external sensor can read out sensor samples every 5 minutes but send it to application *A* only for every other reading while sending



(a) *SVM* architecture (b) *SVM* open APIs

Figure 2: *SVM* software architecture and summary of *SVM*'s open APIs.

all readings to application *B*. In this case, the rule-engine is given a policy to take the greatest common factor for meeting the schedule of multiple applications. Also similarly, when multiple applications request different duty-cycle operations on an IoT device for energy management, given the goal of providing a satisfactory QoS for all connected applications, the larger operation duty-cycle which may consume more energy but assure performance level QoS on all applications is used.

We point out that the *SVM* operates as a background process on Android and operates only with an explicit request from the application process in iOS. While managing both on-board and external sensors, the *SVM* does not operate until an application sends a request so that it can minimize the additional power draw that a hardware controlling module introduces. The size of the SVM software on a smartphone is ~1.20 MB on Android and ~2.30 MB on iOS and requires ~50 kB of memory while running with an additional ~20 kB of extra memory per each external sensor connected to the smart device. The SVM operates on Android version 4.3 (API Level 18) and iOS 5 or higher to support BLE connections.

As a way to open these local IoT resources to even more applications beyond a device's internal applications, the APIs provided by *SVM* and the data resources from the *SVM* application framework are shared using a Google App Engine-based service. As an identifier for each mobile computing platform, we use a tuple ID of `[GPS-location,mobile-platform-ID]`, where the associated phone number of the mobile platform or the MAC address is used as the `mobile-platform-ID`. This tuple ID is associated with the APIs that the mobile platform provides (Figure 2(b)) and allows other mobile platforms to access a remote mobile platform's local IoT resources when properly authenticated.

Finally, Figure 3 shows the overall architecture and usage scenario that we envision; the *SVM* on a mobile device manages its local IoT devices and exposes them to the cloud via the *SVM* application server. These IoT devices as well as virtual IoT devices (which we explain below) can be accessed not only by multiple applications running on that mobile device but also by remote applications running on various Internet-connected platforms.

2.2. Creating Virtual IoT Device: Sensor Data Mash-Up. The capability to easily access data from various external IoT devices, both locally and remotely, opens the possibilities to generate new information from the original data. For example, the capability to access temperature and humidity levels from two different sensors allows the generation of a new data type called "comfort level." Although it is possible to implement a dedicated application on a smartphone to read individual local sensors and calculate this comfort level, *SVM* takes a different approach where a virtual IoT device with "comfort level" sensor is created. The advantage of this approach is that any application running on a mobile device or on the Internet can access this shared information without dedicated connections to the physical sensors or individual knowledge of how they are retrieved or how the new information is calculated. Our *SVM*'s open APIs allow the generation of such new types of information sources by providing an `addDevice()` function. Using this functionality, as Figure 4 shows, data from different IoT devices can be "mashed up" to generate new custom data using a user

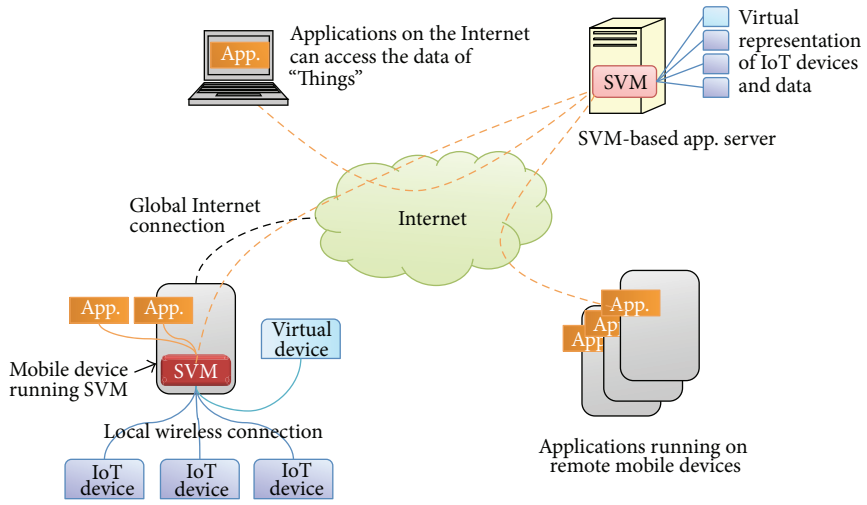


Figure 3: *SVM* usage scenario.

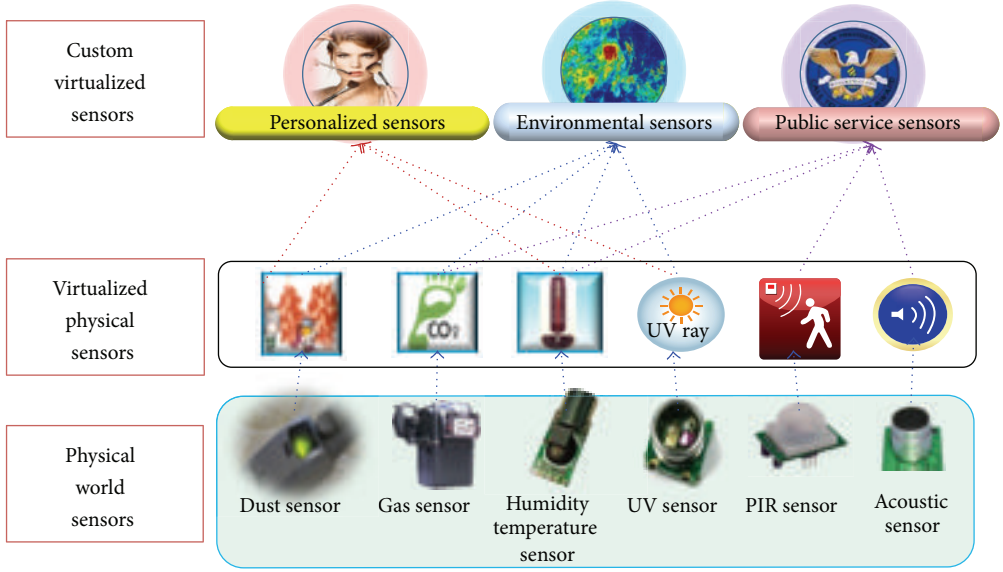


Figure 4: Custom virtualized device generation process using data from physical world sensors.

defined fusion function. Furthermore, as we illustrate in Figure 5, this new data resource can also be exposed as a separate customized virtual IoT device using the open APIs for various remote applications to access. For example, if a mobile or web application wishes to access environmental information from a specific location, it can access a virtual environment sensor instead of trying to connect to several physical sensors individually and reimplement the fusion function.

2.3. Software Reprogramming. The management of IoT devices from mobile platforms offers opportunity for any software updates required by the IoT devices to be achieved through the mobile platform. Furthermore, when a mobile device first enters a field of IoT devices, a new installation of software may be required on the mobile device to fully manage or utilize the features of the IoT devices required by the target application. For this purpose, *SVM* provides support for updating software on a target IoT device and also for installing required software on the mobile platform to utilize the IoT devices that are connected to themselves.

(i) IoT Device Software Update. *SVM* supports reprogramming of the external IoT devices as follows. First step, which occurs during the application development and packaging phase, is to combine the executable binaries generated for the IoT devices into a single smartphone application installation package. Fortunately, both Android and iOS development environments provide directories where raw files can be packaged as a single application installation file. Specifically, these designated folders are the `res/raw/` folder within Android IDE and the `documents/` directory for iOS. Once the IoT devices' binaries and the smartphone installation

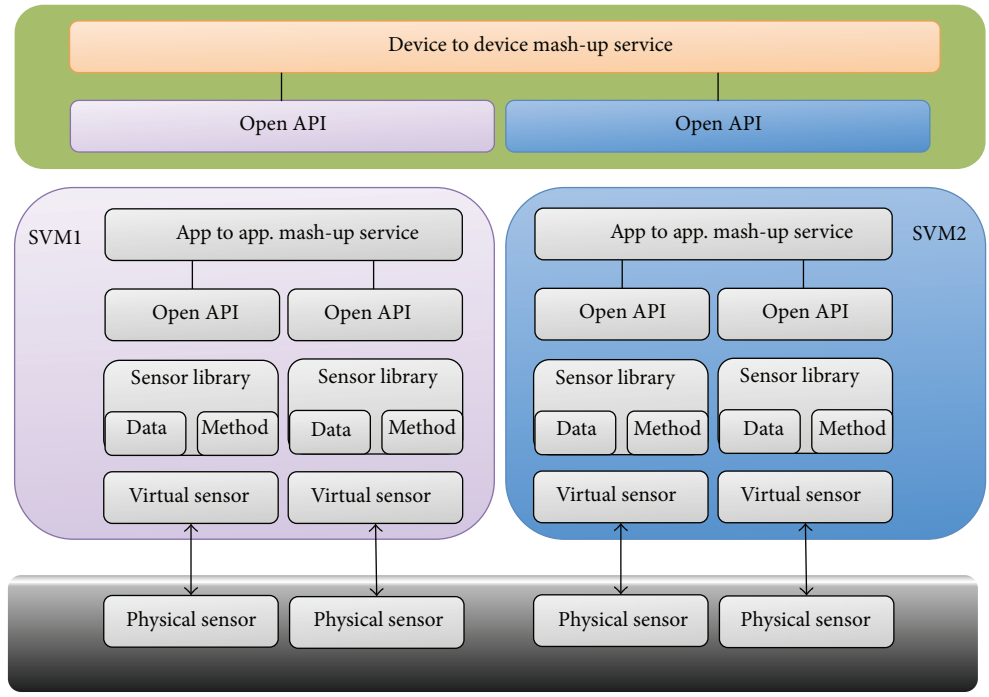


Figure 5: Illustration of sensor data mash-up procedure using *SVM*'s open APIs.

binaries are packaged and sent to the *SVM* (via URL), *SVM* extracts the binaries for the IoT devices and distributes them to the individual devices. At this step, we expect the IoT devices to incorporate some form of over-the-air bootloading and reprogramming method to allow the proper update of software. A well-known example of this is the iOS update process on iPhones. Furthermore for security reasons the mobile device that is reprogramming the IoT devices is authenticated and authorized by an application server before the binaries are distributed and installed.

(ii) Automatic Software Installation on Mobile Computing Platforms. Software update can also move in opposite direction where IoT devices push the required software to the mobile device that it is connected to. When a *SVM*-compliant IoT device with such reprogramming capability discovers and connects to a new mobile device, it simply pushes a predefined URL to the mobile device. Using this URL, the mobile platform retrieves the proper software that the IoT device requested and installs it while making the required configurations to interoperate with the *SVM*. Unless this software is installed on the mobile device, mobile device has limited access to the information and features provided by the IoT device.

3. Application Case Studies

Using the *SVM* environment, we now present two application case studies, implementation of two sample applications that benefit from the use of the *SVM* architecture.

3.1. Sensor Data Management and Mash-Up. The first application we designed with *SVM* is a *sensor data management* application. The goal of this application was to validate the effectiveness of using *SVM* for IoT device interaction and experimentally evaluate the functionality of IoT device resource management and the data mash-up functionality. Using the *SVM*'s open APIs as the development core, we were able to easily interconnect multiple external IoT platforms from the Android OS. As Figure 6 shows, our application interacts with nine different sensing modalities on three physically different IoT devices. We were able to access these devices using both Bluetooth and ZigBee communication modules attached to the smartphone's USB connector.

Furthermore, for testing the data mash-up functionality, we computed the comfort level of the current environment using the humidity and temperature data collected locally and an air clarity measurement of the area, which was accessible through GPS measurements and a web-based query to the meteorological services' server. Using a user defined algorithm to combine these measurements, we were able to create a new customized virtual IoT resource (comfort level) within the *SVM*. Based on the updates of each value, the value of this customized virtual IoT sensor was updated automatically on a periodic basis. Furthermore, this sensor was accessible not only from the smartphone that the physical IoT devices were connected to but also from a cloud-based application server from which other applications can retrieve data.

3.2. Home Appliance Management. Managing and controlling smart home appliances (e.g., air conditioner, smart

(a) Sensor value display (b) Device configuration (c) Mash-up example ("comfort level")

FIGURE 6: Screenshot of sensor data management application.

lighting, and thermostat) are an attractive IoT application. While some appliances may include WiFi radios to achieve global connectivity through preinstalled WiFi APs, such an infrastructure may not be available in all households. However, we noticed that some products had Bluetooth connectivity which allows pairing with a mobile device for appliance management. But using them as they are suggests that a mobile device (or any controller device) needs to be within Bluetooth communication range of the appliance to control it. With *SVM*, smart appliances in a home can be exposed to the cloud as IoT resources and the *SVM* open APIs would allow users to control these devices remotely, either on the web or also from another mobile device.

To exemplify this idea, with the help from our industrial collaborators, we have used a robot cleaner and an air purifier with Bluetooth connectivity and installed our *SVM* on an Internet-connected Bluetooth-enabled smart TV which acted as a gateway to support global connectivity for various smart appliances. The reason for using a smart TV was to showcase a scenario where a device residing at home provides connectivity, and your mobile phone is used to control those devices remotely when you are not at home. The APIs to control the appliances were exposed through our SVM *cloud service* that we implemented, which shows a list of accessible controls that are authorized for each *SVM*-compliant device. Figure 7 shows the screenshot of our cloud service designed to access the *SVM*'s global open APIs through the Internet. Using the cloud-based open APIs, we were able to design a home appliance controlling application that could start and stop home cleaning and air purifying remotely before reaching home to manually control the devices.

4. Related Work

As sensor-equipped smartphones become more prevalent, many new and interesting applications have emerged that make use of the sensors on a smartphone. For example, PEIR [17] is a personal environmental impact report platform for participatory sensing systems research, and Nericell [18] is a monitoring system for road and traffic conditions using mobile smartphones. Eriksson et al. proposed a mobile sensor network for road surface monitoring [19], and SoundSense [20] is a scalable sound sensing system for people-centric applications on mobile phones. Furthermore, Krieger et al. use smartphone sensors for urban tomography in social science research [21]. Abstractions and functionalities provided by our proposed SVM can be used to ease and expedite the development of such applications.

There are several prior works that aim to connect wireless sensors to the Internet by utilizing various Internet standards centered at IP/IPv6. For example, IEEE 802.15.4-based protocols are designed specifically to support interoperability with other already existing IP-based devices (e.g., IETF 6LoWPAN [22] and RPL [23–25]) and communicate with the larger Internet architecture to transport their data to consumers and services in the cloud [13]. Dunkels et al. also evaluated the performance of low-power IPv6 for IoT using the Contiki OS [11].

Another line of related work is programming framework (and APIs) for mobile devices that allow backend users to easily program and task mobile devices on the Internet for collecting sensor data. Medusa [26] proposes a programming system for crown-sensing, which provides a programming language with high-level abstraction for crowd-sensing tasks, and supports specifying various forms of human mediation in

Figure 7: Application diagram and screen capture of our smart appliance management application.

the sensing workflow. It partitions the tasks between the cloud and smartphones and also supports incentives and user specified controls on smartphone resource usage. Another work by Ravindranath et al. [27] also explores tasking smartphones and provides complex data processing primitives and profile-based compile time partitioning. Furthermore, AnonySense [28] is a privacy-aware tasking system for sensor data collection and in-network processing, PRISM [29] proposes a procedural programming language for collecting sensor data from a large number of mobile phones, and [7] is a tasking abstraction for tiered sensor network. However, their focus is on the programming language abstractions on mobile smartphones and does not support virtualization of external sensors or sensor data mash-up or sensor reprogramming capability.

5. Summary and Future Research Directions

The Sensor Virtualization Module proposed in this work provides applications with a common virtualized

environment where external IoT devices can be easily accessed from and via mobile computing platforms. We achieve this by abstracting the networking aspect of IoT devices through user-held mobile devices as a gateway and providing a set of open APIs and device reprogramming functionality, which simplifies the access to various IoT resources. We believe that this work is one of the first attempts to step away from the traditional "stovepipe" software model where only a dedicated software, service, or a limited set of APIs provided by the IoT device vendors are available to third-party application developers. By allowing developers to easily access resources from various IoT devices, we envision that a diverse set of applications can be developed and many users will easily experience the effectiveness of IoT systems in shorter time.

An important next step that we foresee is well defining a protocol for data exchange between the smartphone and external sensors. While various standards can allow the devices to communicate, depending on the physical sensors' initial configurations (e.g., offering push or pull based services or a predefined wireless channel configuration), the quality and stability of data gathering can vary. We argue that an application level standard should address this issue (e.g., defining the format of physical sensor profiles). Furthermore, by providing modular environment for designing new virtual sensors, we believe that applications can maximize the usage of physical wireless sensors for designing various personalized services.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by Project no. 10041725, "Development of Application Service and Software to Support Sensor Terminals for Providing Personalized Service Based on Smart Devices," from the Korean Ministry of Knowledge Economy. For Jeongyeup Paek, this research was supported by the Chung-Ang University Research Grants in 2015.

References

[1] E. Ancillotti, R. Bruno, and M. Conti, "The role of the RPL routing protocol for smart grid communications," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 75–83, 2013.

[2] Cisco, "Smart Grid—Field Area Network," http://www.cisco.com/web/strategy/energy/field_area_network.html.

[3] V. C. Gungor, D. Sahin, T. Kocak et al., "A Survey on smart grid potential applications and communication requirements," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 28–42, 2013.

[4] T. Heo, K. Kim, H. Kim et al., "Escaping from ancient Rome! applications and challenges for designing smart cities," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 1, pp. 109–119, 2014.

[5] A. Brandt, J. Buron, and G. Porcu, "Home automation routing requirements in low-power and lossy networks," RFC 5826, IETF, 2010.

[6] J. Martocci, P. De Mil, N. Riou, and W. Vermeylen, "Building automation routing requirements in low-power and lossy networks," Tech. Rep. RFC 5867, 2010.

[7] J. Paek, B. Greenstein, O. Gnawali et al., "The tenet architecture for tiered sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 4, article 34, 2010.

[8] J. Paek, J. Hicks, S. Coe, and R. Govindan, "Image-based environmental monitoring sensor application using an embedded wireless sensor network," *Sensors (Switzerland)*, vol. 14, no. 9, pp. 15981–16002, 2014.

[9] German Federal Ministry of Education and Research, Project of the Future: Industry 4.0, http://www.bmbf.de/en/19955.php.

[10] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, 2009.

[11] A. Dunkels, J. Eriksson, N. Finne et al., "Low-power IPv6 for the internet of things," in *Proceedings of the 9th International Conference on Networked Sensing Systems (INSS '12)*, pp. 1–6, June 2012.

[12] J. W. Hui and D. E. Culler, "Extending IP to low-power, wireless personal area networks," *IEEE Internet Computing*, vol. 12, no. 4, pp. 37–45, 2008.

[13] J. G. Ko, S. Dawson-Haggerty, D. E. Culler, J. W. Hui, P. Levis, and A. Terzis, "Connecting low-power and lossy networks to the internet," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 96–101, 2011.

[14] H. Kelly, "Helping 'smart' devices talk to each other," *CNN*, 2014.

[15] Y. Park, J. Yu, J.-G. Ko, and H. Kim, "Software radio on smartphones: feasible?" in *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications (HotMobile '14)*, ACM, February 2014.

[16] J. H. Lim, A. Zhan, J. Ko, A. Terzis, S. Szanton, and L. Gitlin, "A closed-loop approach for improving the wellness of low-income elders at home using game consoles," *IEEE Communications Magazine*, vol. 50, no. 1, pp. 44–51, 2012.

[17] M. Mun, S. Reddy, K. Shilton et al., "PEIR, the personal environmental impact report, as a platform for participatory sensing systems research," in *Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '09)*, pp. 55–68, June 2009.

[18] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell—using mobile smartphones for rich monitoring of road and traffic conditions," in *Proceedings of the 6th ACM Conference on Embedded Networked Sensor Systems (SenSys '08)*, pp. 357–358, November 2008.

[19] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, "The Pothole Patrol: Using a mobile sensor network for road surface monitoring," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, pp. 29–39, ACM, June 2008.

[20] H. Lu, W. Pan, N. D. Lane, T. Choudhury, and A. T. Campbell, "Soundsense: scalable sound sensing for people-centric applications on mobile phones," in *Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services (Mobisys '09)*, pp. 165–178, ACM, Wrocław, Poland, June 2009.

[21] M. H. Krieger, M.-R. Ra, J. Paek, R. Govindan, and J. Evans-Cowley, "Urban tomography," *Journal of Urban Technology*, vol. 17, no. 2, pp. 21–36, 2010.

[22] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15.4 networks," RFC 4944, 2007.

[23] T. Winter, P. Thubert, A. Brandt et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC Editor RFC6550, 2012.

[24] J. Ko, J. Jeong, J. Park, J. A. Jun, O. Gnawali, and J. Paek, "DualMOP-RPL: supporting multiple modes of downward routing in a single RPL network," *ACM Transactions on Sensor Networks*, vol. 11, no. 2, article 39, 18 pages, 2015.

[25] H.-S. Kim, J. Paek, and S. Bahk, "QU-RPL: queue utilization based rpl for load balancing in large scale industrial applications," in *Proceedings of the 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON '15)*, Madison, Wis, USA, June 2015.

[26] M.-R. Ra, B. Liu, T. F. La Porta, and R. Govindan, "Medusa: A programming framework for crowd-sensing applications," in *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services (MobiSys '12)*, pp. 337–350, ACM, June 2012.

[27] L. Ravindranath, A. Thiagarajan, H. Balakrishnan, and S. Madden, "Code in the air: simplifying sensing and coordination tasks on smartphones," in *Proceedings of the 13th Workshop on Mobile Computing Systems and Applications (HotMobile '12)*, February 2012.

[28] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "AnonySense: privacy-aware people-centric sensing," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys '08)*, pp. 211–224, June 2008.

[29] T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma, "PRISM: platform for remote sensing using smartphones," in *Proceedings of the 8th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '10)*, pp. 63–76, June 2010.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 196280, 11 pages
http://dx.doi.org/10.1155/2015/196280

Review Article

Convergence Research Directions in Cognitive Sensor Networks for Elderly Housing Design

Shinil Suh,[1] Byung-Seo Kim,[2] and Jae Hee Chung[3]

[1]*Graduate School of Smart City Science Management, Hongik University, Sejong 30016, Republic of Korea*
[2]*Department of Computer and Info. Commun. Eng., Hongik University, Sejong 30016, Republic of Korea*
[3]*Department of Architecture, Hongik University, Sejong 30016, Republic of Korea*

Correspondence should be addressed to Byung-Seo Kim; jsnbs@hongik.ac.kr

Received 19 July 2015; Accepted 6 September 2015

Academic Editor: Jianhua He

As part of resolving the issue related to super-aging society, various information systems for the elderly care have been developed utilizing cognitive sensor networks. However, many sensor network-based systems cognizing radios, resources, environments, and so forth are not practically feasible and useful for the elderly themselves. Therefore, this paper tries to propose novel research directions for designing smart residential environment for the elderly in terms of converging information technologies including cognitive sensor networks and architectural design. In this paper, we clarify the definition of smart home from the literatures and briefly surveys cognitive sensor network-based systems for smart elderly housing. After that, this paper proposes research directions for cognitive wireless sensor networks not only for the elderly smart home services, but also for cooperating with architecture technologies. The proposed directions are to utilize cognitive radio technologies, to classify sensor network technologies according to the types of the elderly, to expand sensor networks services for the elderly housing to the wider area such as blocking unnecessary energy loss, to embed sensor network modules into BIM system, and to research sensor networks fit to modular construction.

1. Introduction

As information technologies (ITs) have rapidly been updated and evolved, things and environments around our societies have also been rapidly changed. In particular, emerging smart phones and sensor technologies have made individual's life style smarter, more convenient, and more efficient. By recognizing environment changes and human's behaviors, wireless sensor networks are able to reduce upcoming hazards and improve efficiencies in daily life. Such changes are also coming to our living environment represented by smart home. Recently, many houses, called "smart home," are equipped with lots of sensors and networks to provide some automatic or prediction services. However, even though it is certain that smart home makes our lives easier, people do not benefit from smart home that much. Particularly, the elderly people has difficulties in using such smart functions because the level of adaptation of the old people to the new environment and era is insufficient.

UN classifies three societies depending on the proportion of the elderly in the population (more than 65 years old) takes in a society: aging, aged, and super aged societies. According to the classification defined by UN, aging society refers to a society of less than 7% to 14% population ratio for the elderly people who aged 65 and more in total population. Society of 14% to 20% elderly people ratio would be referred as an aged society, and society of more than 20% of elderly people ratio would be a super aged society. As shown in Figure 1 [1], many countries rapidly move forward to the aged society. Population of aged people is increasing in nearly all regions. Even more, some of few countries are heading to super aged society passing through the aged society. Figure 2 illustrates the trends of the elderly population growth in Korea. As shown in Figure 2, the ratio of 11% of the elderly of the total population in 2010, 24.3% in 2030, and 40.1% in 2060 would be expected to be grown in total population ratio. Particularly the ratio of more than 85-year-old people will be from 0.7% in 2010 to 10.2% in 2060, and it shows they are increasing 10

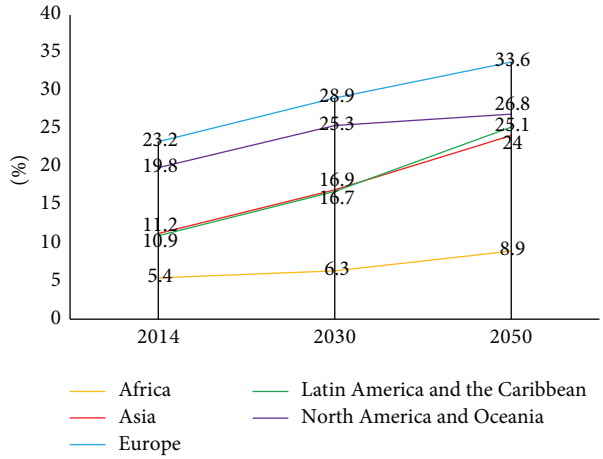


Figure 1: Proportion of population aged 60 or over by region in 2014, 2030, and 2050.

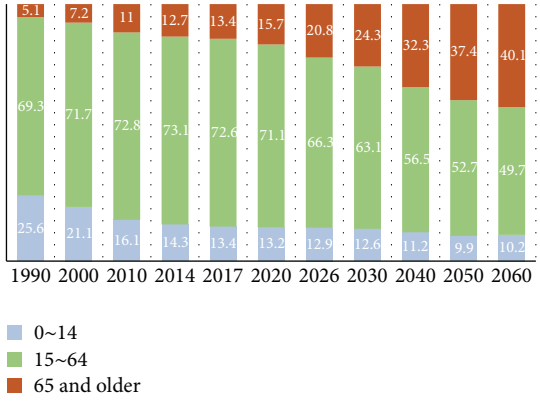


Figure 2: Trends of the elderly population growth in Korea.

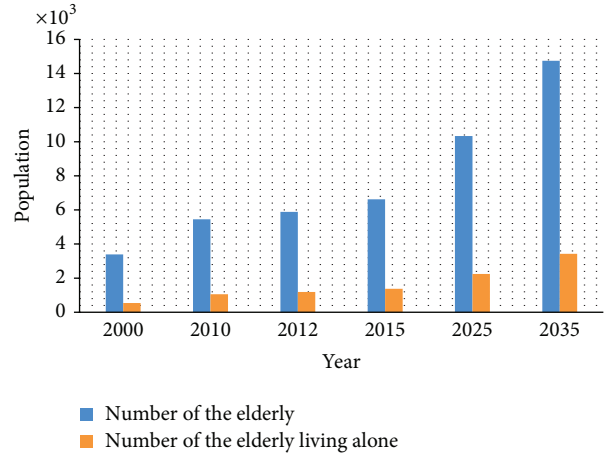


Figure 3: Increasing trends of the number of the elderly and the number of the elderly living alone in Korea.

times [2]. In accordance with the Statistics Korea, the elderly ratio was over 10% of total population ratio in 2010, and the ratio would be 20% in 2026. So then, after 12 years, the elderly will be a person out of 5 people, and that is called the super aged society [3]. Thus, the aged society is on-going so fast in the Republic of Korea. Therefore, many countries have studied issues that can possibly occur for the upcoming society and have been preparing to cope the issues.

One of the issues that the aged society faces might be the elderly's housing. There are a few papers addressing the importance of housing for the elderly's life [4] and the importance is increasing as the number of old people increases. Furthermore, even though the old people is restricted in their activities due to physical degradation, health issues, and so forth and thus, they need more help than younger people does, the number of elderly people living alone is increasing as shown in Figure 3. Therefore, designing the elderly's housing is getting important. With increasing the interest of the elderly housing and tremendous growths of information technologies (ITs), smart home technologies are also paid attention for proving the better life for the elderly [5]. However, even though the elderly and health professionals consider smart home technologies to be beneficial [5] and many services and systems for the elderly's housing have been designed and developed, there are many issues to be resolved such as privacy, cost, and feasibilities. Furthermore, some of the smart homes provide unnecessary services for elderly people because only technical services were formed without carefully considering specific user classification (such as the elderly) that is optimized to particular needs and services for the elderly [6]. To design IT services/systems for smart home, it is important to take into account the fact that learning ability in new environment is not commensurate for real because the elderly and the semielderly are physically and mentally less active than normal adults are, and learning ability for the new skills for them is also low [7].

In this paper, we propose research directions for designing cognitive sensor network-based smart home for the elderly through revisiting the definition of smart home and briefly surveying context-aware or cognitive sensor network-based smart home technologies for the elderly. Unlike sensor network technology-oriented research directions conducted in many preexisting studies, this paper propose sensor network research directions in terms of cognitive radio technology, usability, and cooperating with architectural technologies. In other words, this paper provides some idea to effective architecture design process for the elderly housing by converging cognitive sensor network technologies with architecture engineering.

The paper is organized as follows. Section 2 is divided into three parts. In the first part, we try to clearly define a smart home by revisiting previous studies. The second part describes the current cognitive sensor network-based smart home technologies for the elderly and looked at its problems. We have also investigated the emerging technologies in a smart home. Through these feasibility studies, in Section 3, four directions for designing the elderly's housing in terms of cognitive sensor network technology itself and the convergences of network technologies and the architect technologies are discussed. Finally, the paper is concluded through the conclusion in Section 4.

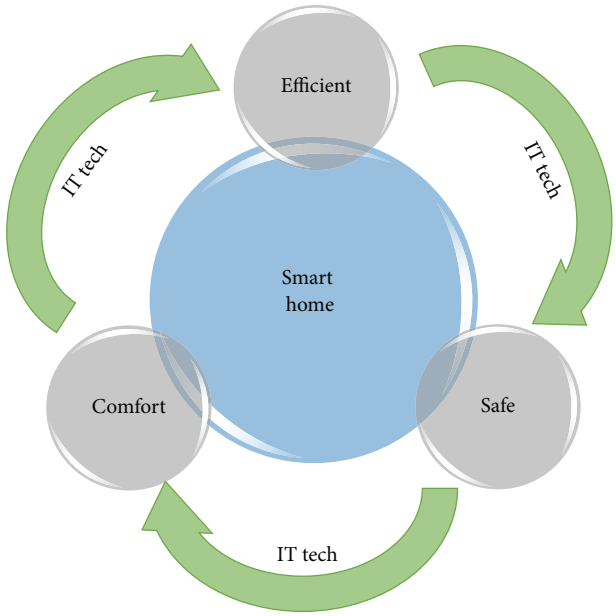


Figure 4: Circulation of the smart home.

2. Case Studies

2.1. Smart Home. The definition of a smart home can be the living environment providing the convenience and efficiency with comforts and security to the resident using the IT technology as shown in Figure 4. According to Wilson et al. [7], functionally, smart home is a residential environment that implements automated and active control and senses and monitors various situations. Instrumentally, it is an optimal management building itself with real-time information and a price-responsive control of the housing environment. In sociotechnical aspects, smart home is a vision of the future living environment that is automatically and technically connected to everything [7]. In addition, the Korea Association of Smart Home (KASH) [8] defines it as the human-centered smart life environment that enables convenience, welfare promotion, and safe life for the people by converging IT technology to a residential environment. In other words, KASH defines a smart home as a spatial environment including all living-related services and systems rather than home itself. Smart home that is an evolved version of currently existing home has appeared by embedding information and communications technologies into a house. This allows the improvement of the quality of life through new and better features, the reduction of energy consumption, and enhanced system management at home [9]. In addition, this helps the resident to satisfy their needs besides basic needs that they can have at home. Except for the existing residential characteristics provided to residents, the organized main function of the smart home provided to users is as follows.

At first, smart home can give us comfort. Not only the existing house could be comfortable, but also the smart home brings us comfortable convenience because the housing environment could take care of many little things that users should do. Secondly, it is safe. The existing home is bad at protecting from against invasions from outside, accidents for solitary residents in their house, or other emergencies. However, the smart home system could be safe because of the monitoring system from outside invasions, and also it could take follow-up measures of the accident because of immediate notification to other people by sensing and monitoring an accident of residents inside. At last, it is efficient and saves energy. The users, because of human-being, might not be perfect. This means they could waste energies by mistakes or accidents such as turning on lights or water and so forth even if they were not using. There would affect saving energies if the living environment could detect and prevent those wastes. Furthermore, it could be efficient for preventing redundant energy uses such as using heater and air conditioner at the same time. For these reasons, a smart home provides users with more advanced living environments and benefits as compared with the traditional house.

2.2. Sensor Network-Based Systems for Smart Elderly Housing. In this section, we investigate studies focusing on developing sensor network-based IT systems/services for the elderly housing which are published after the year 2010 while Morris et al. [5] survey effectiveness and feasibility of general smart home IT technologies. As many information and communication technologies have been developed and evolved like Internet of Things (IoT), long-term evolution (LTE), smart phones, and so on, a few technologies in a smart home for the elderly have been introduced. Even though sensor network-based IT systems/services for normal people have been proposed a lot, the number of them for elderly housing is relatively small. While the researches on areas such as safety, privacy, reliability, efficiency, and technology correlated with smart home issues are in progress, smart home technology for the elderly is mostly being developed only for health care or safety. Suryadevara et al. [10] have proposed a system of protecting the elderly in the smart home using a wireless sensor network. The authors monitored in real time for their life in weekends and on weekdays by equipping the ZigBee wireless sensor on their appliances and things. With the data, a system was designed for separating normal behavior and abnormal behavior. Charlon et al. [11] propose a more effective location-based monitoring system for the elderly people with dementia. Until now, this real-time patient monitoring system is using infrared-ray sensors. However, monitoring elderly patients and preparing for the safety accidents would be now from attaching the wireless sensors in the form of patches to the elderly's back. Lee et al. [12] proposed a smart environment in bathroom based on the sensor networks. The study addresses that 48.8% of the safety accidents are fall accidents in bathroom based on the statistical analysis of safety accidents for the elderly in 2010. In order to help the elderly's activities in the bathroom, the authors define several living patterns and based on the patterns, the system provides convenient services for the elderly to use bathroom safely. Portet et al. [13] report user evaluation how well the elderly accept voice-command-based home automation systems, which is implemented as a part of SWEET-HOME project, and what sort of benefits can be obtained. SWEET-HOME project is supported by a French and aims to realize

man-machine interaction based on audio processing. In the study, the elderly assesses that speech technologies have potential to ease their life. The noteworthy point is that the technology is more effective in securing their lives than in comfort improvement. Kim et al. [14] propose a monitoring system of U-health smart home for the elderly. Hardware and software of the smart home ontology model (SHOM) and common information model (CIM) were developed and implemented by equipping various sensors. However, this study develops the system for just health monitoring system and energy management system with SHOM. Other systems of health-related as healthcare or behavior pattern prediction are not implemented. Shen et al. [15] propose TV-based videophone system for the elderly in smart home. Because TV does not only come into wide use so that the elderly need to pay more money for the videophone system but also is low cost device with high resolution and large screen which is fit for the elderly, the authors select TV for the videophone system for the elderly. In addition, using Support Vector Machine (SVM) algorithm, the system is able to evaluate "rough" physical and psychological health information of the elderly. This evaluation is performed based on the frequency and the length of using the system of the elderly at home. Lee et al. [16] propose ubiquitous-care system for the elderly in smart home environment. The system provides services to track old people's location inside house, to monitor indoor environment parameters such as temperature and humidity, and to send short message to guidance just in abnormal cases. The proposed system is fit to houses equipped with lots of sensors and well organized networks, which seems infeasible. Yu et al. [17] propose a computer vision-based fall detection system to monitor an elderly person who lives alone at home. The system detects the old people's fall based on posture recognition using a single camera. From the experimental results, the system achieves 97.08% fall detection rate and 0.8% false detection rate on a 15 person dataset. Ransing and Rajput [18] propose a simple home safety system for the elderly by utilizing the wireless sensor network with ZigBee protocol. If the temperature increases abnormally in a particular space, the system will inform the current temperature and send warning messages to the users at the same time. The studies are oriented more to implement wireless sensor networks rather than to resolve issues on elderly housing. Kim et al. [19] propose location tracking system inside smart home for elderly safety. Using RFID technology, this system could monitor locations of the elderly in real time for prevention of abnormal situation if unexpected patterns occurred. In addition, they propose module structures of this healthcare system for elderly people. Those are the tag sensing module, location sensing and tracking module, monitoring module, alarm module, health status information module, and external communication module. These modules are for operating process of this proposed system such as sensing, recording, analysis, and feedback. Table 1 lists not only summaries of contents, but also the targeted functions of all studies mentioned above.

As aforementioned above, smart home technologies for the elderly focus on relatively narrow area comparing to that for common people. For example, as mentioned before, most of smart services for the elderly are health care and safety systems as shown in the "targeted function" column in Table 1 while smart home for general people has various areas including energy reduction/management, invasion detections, home security, and automated environmental change system. Because society is increasingly aging, and elderly housing types for single old person or the elderly's community are expected to be emerging, studying IT services utilizing cognitive sensor networks for elderly housing is necessary to be accomplished in various areas. One of these areas might be energy or electric power-related area specialized for the elderly. For example, since the old people have the lack of memory abilities, they might forget to close windows at their house before turning on air-conditioner, which wastes electric power.

2.3. Energy Saving in Smart Home. As mentioned at the end of the previous section, even though many areas are involved in designing smart home for the elderly, IT services for elderly housing are somewhat limited to health and safety. Therefore, we may extend the study area to the other areas such as efficient energy use just like normal people's houses. As a part of this, energy-related IT systems for elderly housing are survey in this section. However, since as far as we researched, few studies about energy consumption-related issues for elderly housing are reported, we instead survey energy-related IT systems for smart homes in terms of IT technology itself. Han and Lim [20] propose a context prediction-based Smart Home Energy Management System (SHEMS) that is based on the data collected from wireless sensors, whose data transmissions are performed based on Kruskal's algorithm. However, the proposed system is somewhat close to smart service system rather than energy management system. Baig et al. [21] propose Energy Management monitoring System (EMS) and a scheduling method for the system. The method schedules appliances' operation times for each appliance to be operated in particular times when the price of using electric power is low. As a result, while the electric power is used about same amount, the user are able to use it with less price through appropriate scheduling for the low energy costs. Mahmood et al. [22] propose Home Appliances Coordination Scheme for Energy Management (HACS4EM) by communication among smart appliances, Energy Management Unit (EMU), and wireless sensor home area network (WSHAN) using ZigBee wireless sensor networks. With communication of these units, the EMU sets the schedule time of the effectively usable periods for the appliances and then suggests the convenient start time to user because the purpose of this system is to reduce the electricity cost from high to low by controlling the operation time. Usman et al. [23] design a routing protocol in order to transmit information by clustering the wireless sensors. In the clusterization, each of nodes is grouped, each of cluster headers is routed to the other cluster header or base stations, and as a consequence, the data can be transmitted further and faster to the destination. This wireless sensor network could be better efficient in terms of energy consumptions of the nodes. Han and Lim [24] propose multisensing and light control application based on smart energy control system

Table 1: Summary of prior-arts related to smart home systems for the elderly.

Related studies	Summary of contents	Targeted function
Suryadevara et al. [10]	(i) Develop a system to detect abnormal behavior by equipping the ZigBee-based wireless sensors on the elderly's appliances. (ii) Abnormal behaviors are detected based on stored daily activity pattern data.	Safety
Charlon et al. [11]	(i) Propose an effective location-based monitoring system for the elderly people with dementia. (ii) Prevent unexpected accidents by attaching wireless sensors in the form of patches to the elderly's back.	Safety
Lee et al. [12]	(i) Propose smart bathroom service system to help the elderly use bathroom safely. (ii) The system operates based on predefined bathroom use patterns. (iii) The proposed system is applicable.	Safety
Portet et al. [13]	(i) Introduce voice-recognition-based smart home system. (ii) Prove voice-recognition technology's potential for the elderly's ease everyday life and security.	Convenience
Kim et al. [14]	(i) Develop and implement hardware and software systems of "U-health smart home" for the elderly. (ii) Develop monitoring system for the elderly focusing on smart home technology only; it cannot be real a U-health home because of the narrow system that is studied for just a monitoring system.	Health
Shen et al. [15]	(i) Propose TV-based videophone system for serving convenience to the elderly at home. (ii) Evaluate physical and psychological health of the elderly based on the frequency and the length of using the system.	Convenience
Lee et al. [16]	(i) Propose system to track indoor locations, to monitor indoor environment, and to provide alarm information through smart phone in the elderly's house. (ii) The proposed system is applicable.	Safety
Yu et al. [17]	(i) Propose fall detection system using posture recognition. (ii) Provide 97.08% of detection rate.	Safety
Ransing and Rajput [18]	(i) Propose a home safety system for the elderly by utilizing ZigBee-based wireless sensor networks. (ii) The proposed system warns abnormal temperature changes to the elderly.	Safety
Kim et al. [19]	(i) Propose indoor location tracking system based on RFID in a smart home for aged people's safety. (ii) Propose module structures of this healthcare system for the elderly.	Safety

for reducing energy costs by using smart energy networks including both ZigBee and IEEE 802.15.4 because one of energy consumptions in home environment is lighting. The reason why Han used both ZigBee and IEEE 802.15.4 is that various manufactured ZigBee devices were used for the interoperability in a system. Through the sensing environment and its data transferred by the wireless networks, the lighting system for reducing electric power would be effectively automatically turned light off or down as befits the environment. Arvind and Ramaswamy [25] develop smart monitoring and controlling system that manages energy usage of home units to be sensed and controlled by using a ZigBee communication module for wireless sensor network. Particularly, it designed to use the minimum energy though temperature monitoring devices with in-built temperature sensor in rooms and communications among the sensors in a building. In addition, software recovery procedures such as exception-handling, autorestart, and alert text mechanism for sensors failure were developed as well. Lampoltshammer et al. [26] propose a method to reduce the energy consumption of the wireless sensor nodes in the health monitoring system for the elderly. The more the data transactions in wireless sensor nodes are increased, the more the energy consumption is increased. In order to reduce the amount of consumed energy in the data transmission processes, primarily the data processes are divided processes in Sensor Layer and ICT Backbone Layer. When a sensor detects an event, the data would be verified preliminarily in the sensor layer. If the event is determined to be an accident, the prevalidated result would be verified again for an obvious situation, and then the accident information will be delivered to the user. In other words, normally the minimum number of sensors is turned on for sensing events, and then other sensors or surveillance systems are implemented when the accident is detected that is to save energy effectively in the monitoring system. Samanta et al. [27] suggest an efficient energy saving method for the elderly in a health monitoring system. Using the prediction algorithm, the sensor nodes are identified and stored as a sensor was often used or not from the data detected at wireless sensor nodes for 10 days because the existing elderly monitoring system consists of too many cognitive sensors including wearable sensors that wastes power usage.

Based on this data, energy consumption would be lower based on this data, energy would be saved because the sensor nodes that are not used in the certain period of time would be deactivated for 2 hours after 10 days. Park et al. [28] propose a power management system, called Smart Energy Management System (SEMS) by using the ZigBee-based communications. SEMS is an energy saving method that a power socket would be turned on by using motion sensors when a user operates equipment in the vicinity the socket. The motion sensor detects user every 10 minutes. If anyone is detected, the socket turns on to use appliances. In addition, if the users are left there after using the unit, the power sockets would be turned on until next detection moment, after that the socket would be turned off. This system could reduce energy consumptions and interrupt standby powers unless the user is near the socket.

As described previously, smart home systems in terms of energy reservation are focused on how to efficiently use energy such as the smart grids, the new wireless sensor network functions, and the use of context-awareness or inference algorithm. However, it was hard to find researches and system developments of the specialized energy-saving system or method for the specific age groups, especially the elderly in smart residential environment.

3. Discussion

From the previous section, a smart home is clearly defined, and prior-arts in the cognitive sensor network-based systems for elderly smart housing are surveyed. Furthermore, energy-saving technologies based on IT in a smart home are studied. Summarizing the studies examined in the previous section are as follows:

(i) Most of IT services for smart elderly housing are based on sensor networks targeting at one specific function such as health monitoring or fall detection or security and they are based on one type of network.

(ii) Sensor network-based systems for residential environment for the elderly mainly focus on relatively narrow area such as risk detections/monitor and health-related area.

(iii) Energy-saving technologies for the elderly-friendly residential environment are rarely found despite the numerous IT systems for energy saving have been proposed.

(iv) Most of sensor network-based system/services for elderly housing are oriented on information technology itself as if the systems can be applicable to all types of old people, even though the elderly themselves are classified.

(v) Most of sensor-network-based services/systems for elderly housing are designed independently without considering spatial and architectural designs.

As taking into account on the summaries above, this section proposes possible cognitive wireless sensor network research directions for elderly housing in terms of converging IT into architectural design and technologies.

3.1. Adaptation and Utilization of Cognitive Radio- (CR-) Based Wireless Sensor Network for Designing Elderly Housing. As mentioned above, most of IT services for elderly housing are depending on sensor networks which exchange small detection data and focused on specific one function such as health monitoring or fall detection or security. Furthermore, the sensor networks are most likely configured in one-type of network such as wireless local area network or ZigBee or Bluetooth or cellular network; that is, the networks are not heterogeneous networks. However, elderly housing needs more sensors comparing normal people's residential area to provide more various and simultaneous services. That is, unlike services focusing only one function, the system/services need to provide various elderly cares such as health, safety, security, and convenience at the same time. Therefore, the elderly housing may be equipped with many different sensor networks which becomes heterogeneous network. In addition, unlike exchanging small data between sensors, the housing requires wireless multimedia sensor networks that deals with bulky video/image data.

In summary, the sensor network for the elderly housing can be characterized as heterogeneous and bulky data-handled condensed sensor networks. In such network environment, wireless networks' performances might be degraded because of the interferences from different types of networks. The interference comes from the fact that most of the networks for smart housing use Industry-Science-Medical (ISM) frequency band due to free of use of the channels. In particular, ZigBee or wireless personal area network or Bluetooth network which is well-used for sensor networks and uses small transmit power is fatal if the networks coexist with bulky data-based WLANs as shown in [29, 30]. Moreover, even though there is only one type of network, in a dese network environment, network performances are significantly degraded [31]. To alleviate such issues, CR-based sensor networks for elderly housing need to be considered. Because CR networks enable operating channels to dynamically change, interference and collisions from other networks can be removed, so that reliable data transmission can be achieved. However, as long as we research, the research on CR-based wireless sensor networks for elderly housing is hardly found in literatures.

3.2. Classification and Application of the Senor Network Technology from Elderly Types. Currently, residential environment designs for the elderly are changing to residential types as independent or group because of increasing the number of single elderly household in the future and are in progress to be minimized or optimized in accordance with their living types and characteristics of the elderly. On the other hand, information technologies and services used in the smart home are mostly formed to focus on the general convenience by utilizing the newest sensor or network technologies rather than designed them based on the characteristics, capabilities, and needs of the users and as a consequence, the necessity of using them is effectively reduced [6]. For example, some of the smart home technologies that are recently developed are controlled by smart phones, but they are not available

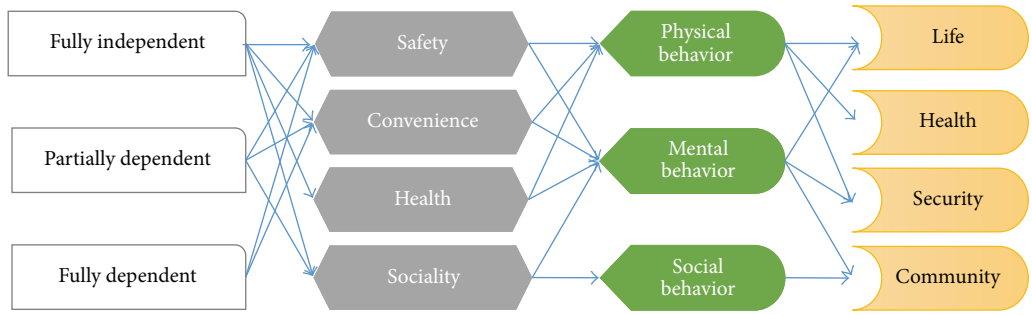


Figure 5: Correlations between types of the elderly and architectural factors.

technologies for the users who are not able to use or do not use a smart phone, who might be the older people. Particularly, in order to perform studies on design of the sensor network-based systems for smart the elderly's housing, the studies on the elderly themselves who have a variety of physical/active limitations need to be performed in advance. That is, prior researches such as comparative analysis of the elderly's behavior with general adults, behavior analysis based on physical types and age groups of the elderly, and requirements analysis on residential life of elderly people are required. Through doing this analyses in terms of the elderly's many aspects, sensor network-based IT services and systems based on such requirements and types of the elderly need to be clarified and classified, and then the results need to be applied and reflected to design smart homes for the elderly. As a result, it is expected that implementation of low-cost IT service and systems optimized for the elderly might be feasible.

To classify the types of the elderly, we may adapt a method used for assessing the elderly's activities of daily living (ADL). In ADL assessment, the old people are asked for their functional status such as eating, toileting, walking, and so on, and they are asked to answer one of three types: fully independent, partially dependent, and fully dependent. That is, functional status of the elderly are classified as such three types. Lim and Chung [32] try to map the three types with architectural factors (Safety, Convenience, Healthiness, and Sociality) and apply this to design the elderly's housing. An example of the mapping process is shown in Figure 5. Such similar process might be applied to build the elderly type-customized IT services/systems. IT service technologies for the elderly's housing are sorted and classified according to four architecture factor types as well as the elderly types used in ADL assessment. Therefore, IT services/systems are also packaged for the architecture factors and the elderly's types. By doing this, IT service packages specialized on the elderly activity types as well as architecture types could be applied to build the elderly's housing. As consequences, this package would easily apply IT service designs itself to residential area designs for certain elderly types, and it would be possible to design residential environments with optimizer smart home services and design cost reduction unlike conventional smart home design in which IT services are for general old people. It also reduces time-consumption and cost to design IT service/system for the elderly's housing.

3.3. System Development for Preventing from Unnecessary Energy-Losses due to Physical/Mental Particularities of the Elderly. As many existing studies, reducing energy consumptions as efficiently as possible by utilizing sensors and smart devices in smart homes would be one good way for energy-savings. However, the smart home for the elderly may require more energies comparing to normal people's house because the old people need more systems and services due to their physical limitations. On the other hand, the research needs to focus on reducing unnecessary energy loss due to the elderly's physical/mental limits, which have not been well-studied so far. Therefore, the smart home for the elderly considers not only how to efficiently use the energy, but also how to reduce unnecessary wasted-energy due to the nature of limited physical and mental abilities. For example, the elderly might let home appliances continuously operate even though they are not using the appliances because the elderly easily forget to turn off them. For another example, they might operate an air conditioner or heater while windows are open. Thus, in order to reduce such energy-wasting cases, behavior patterns of the elderly with different characteristics need to be carefully scrutinized and the cases wasting energy in the elderly's house are defined. By doing this, we may develop smart IT system for saving energy specialized for the elderly. As a part of this, some IT systems might be considered as follows. The first example of the system may be a system to block abnormal energy usages comparing to the life pattern of individual old people. By collecting data of an old person's living pattern and analyzing the data, when unexpected energy is spent besides the behaviors of any particular pattern of the elderly people by times and situations, the system automatically blocks the loss of energy. For the second example, a system integrating multiple appliances which are affected each other in energy perspective is needed to block any unnecessary energy loss. This is applied to the aforementioned case like turning air conditioner with opening windows. That is, air conditioner and windows are correlated because when turning on air conditioner, windows need to be closed. Like this case, if there is correlated operation between multiple appliances, a system is needed to let those appliances cooperatively operated,

so that energy loss can be automatically blocked without a physical interruptions, which are constraints in the elderly.

3.4. Convergence with the Architectural Technology

3.4.1. Architectural Design Cooperating with Sensor Network-Based Services/Systems Design. As defined above, a smart home is specialized as a designed living space for improving the performance and efficiency in various aspects with user-centered environment comparing to the traditional residential environment. Convergence of the IT technology and architecture design of the existing residential area needs to be considered for the accomplishment of smart home's purpose for the elderly. In designing a smart home for the elderly, designing sensor network-based services and systems is exclusively and separately proceeded with the area/space design and architectural design. On the other words, during the process of architecture design, design of sensor network-based IT services and systems for the elderly housing are somewhat abstractly utilized or carelessly considered. Thus, mismatching of initial designs of architect and ITs and frequent change-requirements in architectural design or IT system design during the subsequent construction process occur. As a consequence, the increase of budgets, processing-time, and inefficiency of IT systems occurs. In particular, inefficient sensor network design generates cases in which the users would not use the services.

For example, because of the exclusive operation between architectural design and IT service design, the efficient visual range of surveillance camera would not be ensured, and the design of IT systems and sensors would not be effective. In the first case, despite the problem of invasion of privacy, the use of the monitoring camera has been recognized as necessary for risk detections, and so forth in the elderly residential environment. However, to increase the number of surveillance cameras or to limit its monitoring function would be a problem by designing space and user's movement to ignore the visual range and resolution of installed camera. In the second case, even though the use of the various communication sensor modules and various wireless communication devices is increasing for the behavior judgment and context awareness of the elderly, their substantial function would not be performed by expansion of the shadowing areas due to not only communication interferences between each other [29, 30] but also inappropriate materials used for constructions of spaces.

Thus, space design as an architectural process and sensor network design as IT service/system design process need to be cooperatively progressed from residential area design from the beginning. Through this, it will be able to minimize the unnecessary waste of budget and time and to increase user's satisfaction. Even though we propose the method mentioned in this subsection for the elderly housing, this proposed idea can be applied to any other house/building design process to obtain similar benefits. However, because sensor network-based services/systems for the elderly housing need to be more optimized for the elderly comparing to universal house design [33], the proposed method is required more in the elderly's housing.

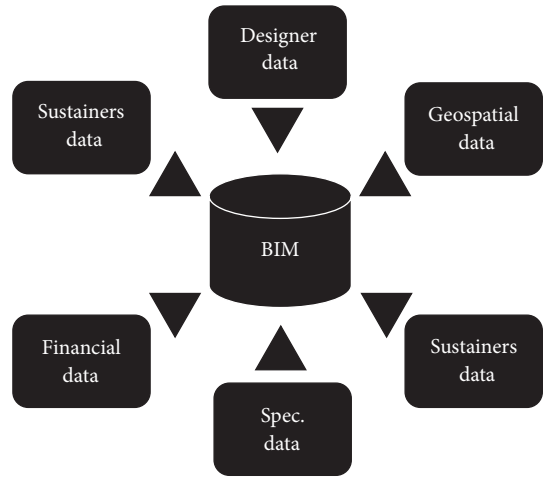
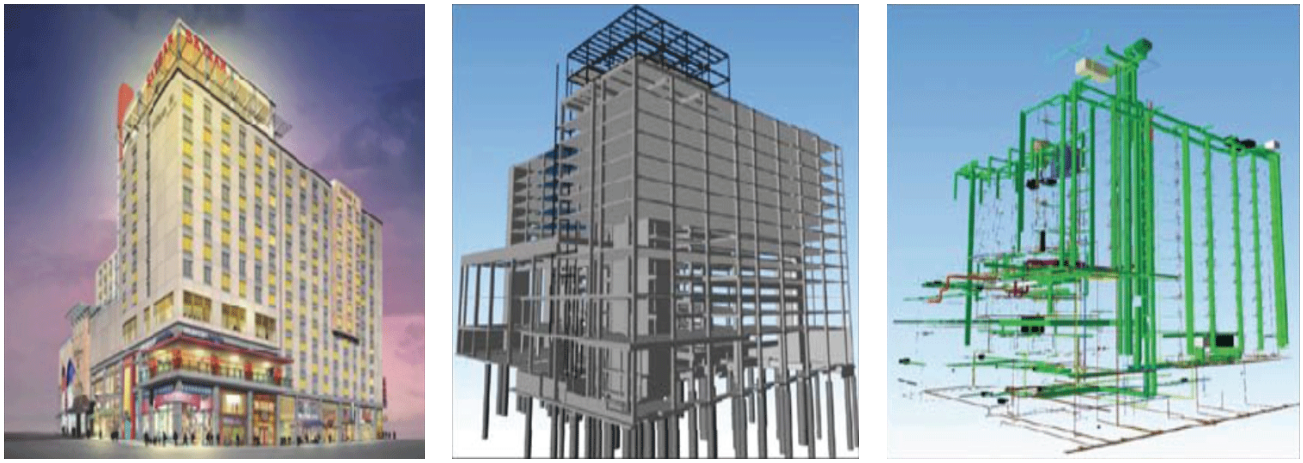


Figure 6: Building information modeling.

3.4.2. Convergence of Sensor Network-Based Home Services/Systems with Building Information Modeling (BIM). As part of aforementioned cooperation between sensor network and architect designs, a method for modularizing sensor network technology and systems for elderly housing need to be studied in accordance with design modules of Building Information Modeling (BIM) that is used for architectural design. As shown in Figure 6, BIM is a simulator using data models of every object in a building as applying building's characteristics, information, and change factors that cognize each other. Moreover, it can create and manage various data applied to a variety of fields from the concept design phase to maintenance phase. Furthermore, it can store all data in computer database from the construction design and express the data to various types as occasion demands. In other words, it is a designing and processing tool that predicts and prepares constructions in advance and minimizes wastes and builds better quality of the building by creating a digital model in a virtual space with 3D model having attribute information of the object. An example of models designed by BIM is shown in Figure 7.

BIM which recently gives many advantages to building designs is focused on the architecture, construction, electrical equipment design, and so forth; on the other hand the information about the sensor/network modules for IT system design is very limited. Accordingly, based on the classification of sensor network technologies previously proposed for the elderly, some libraries for sensor networks' components might be built in BIM, so that the housing designers will be able to easily apply such components to their elderly housing design from the beginning stage of the design process. Unlike current design process in which space design and IT system design are separated, since a space designers design housing with considering IT systems, the better and more efficient housing design for the elderly can be realized.

3.4.3. Convergence of Wireless Sensor Network Technology according to a Modular Construction Technology. Recently modular-based architecture and construction technology



(a) (b) (c)

Figure 7: Architectural (a), structural (b), and plumbing (c) models of BIM for Hilton Aquarium at Atlanta, Georgia, USA [35].

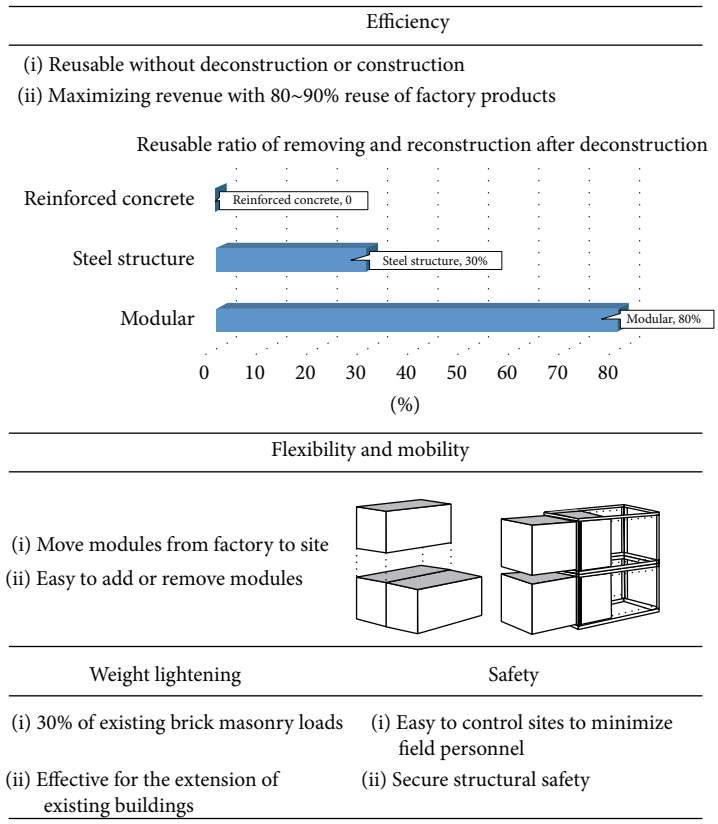


Figure 8: Advantages of the modular construction technology.

[33, 34] are actively being researched as an alternative residential area for the elderly. Modular architecture technology is an industrialized building construction system where modular units produced in the factory are moved to the construction site and the building is finalized by assembling them. It increases efficiency through the modularization of building materials, minimizes construction processes at site, and provides more secured works in the construction processes. Moreover, it could be moved and reusable technology even after installation. The advantages of modular construction are described as Figure 8. This modular design technology would be expected to apply residential designs for the elderly a lot. The reason is that number of the elderly who live alone will increase in the future as illustrated in

Figure 3, and residential area for them will be smaller. The smaller house is needed for the elderly because it has small house works [32]. In addition, as aforementioned above, types of the elderly are changed as time goes by, and according to this, area for them will be also possible to change. Atkinson et al. [33] also insist that the modular construction-based house is appropriate for the elderly's housing because it is low cost and is reusable. In conclusion, it is certain that the modular construction technology is used for the elderly's housing.

Therefore, the sensor network technology according to this modular architecture should be developed to install and operate effectively within the modular residential environment. Even if the environment is formed to different shapes by another resident, the sensor network technologies enabling to provide always efficient and reliable services are necessary to be studied. As an example of this, instead of using wired sensor networks, the wireless-based sensor networks are suitable for a modular transformative residential areas. In other words, the use of the wireless sensor networks could solve the trouble caused by wires for changing areas freely, and the considerations of the line arrangement might be lower in the modular area implementation. For another example, there might be the detection and link technology of dynamic and automatic connection device in the central management panel. Eventually, the wireless sensors as mentioned above would collect data and deliver control command through the central management system (central control panel with a type of GUI). In this case, the type and location of the communication device would be changed by changing areas in various ways, and this will be automatically detected, and then the technology is necessary to be integrated and removed for sensors and devices in the central management system without user's additional behavior.

4. Conclusion

Even though many countries are heading to an aged society or even an aging society, studies on residential environment for the elderly have not actively been conducted so far. Particularly, IT services/systems represented by sensor networks for smart home are mainly focused on universal purpose, not specialized for the elderly. In this paper, we propose the directions of researches for sensor networks-based elderly housing in three perspectives. One is adopting CR-based sensor network technologies to cope with dense sensors environment and heterogeneous network environment, customizing sensors/networks classification correlated with the elderly types, and converging sensor network technologies with architectural technologies. We hope that these researches might be an initiative that the elderly-specialized smart home with IT is developed to satisfy user characteristics in the future, so that the elderly has the better life.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Ministry of Education (MOE) and National Research Foundation of Korea (NRF) through the Human Resource Training Project for Regional Innovation (no. 2014H1C1A1066943).

References

[1] HelpAge International, "Global AgeWatch Index 2014 Insight report, summary and methodology," 2014, http://www.helpage.org/download/542b0adfb65fb/.

[2] Statistics Korea, *Future Population Projection: Year 2010~2060*, Press Releases, 2011.

[3] Statistics Korea, *2014 Statistics of the Elderly*, Statistics Korea, 2014.

[4] L. A. Pastalan, *Aging in Place: The Role of Housing and Social Supports*, Routledge, 1st edition, 2013.

[5] M. E. Morris, B. Adair, K. Miller et al., "Smart-home technologies to assist older people to live well at home," *Journal of Aging Science*, vol. 1, no. 1, pp. 1–9, 2013.

[6] H. C. Kim, S. M. Ko, H. J. Oh, J. M. Shin, and Y. G. Ji, "A study on the service characteristics in a smart home environment and the actual service usage for the elderly," in *Proceedings of the Fall Conference of Korean Institute of Industrial Engineers*, Suwon, Republic of Korea, 2013.

[7] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Smart homes and their users: a systematic analysis and key challenges," *Personal and Ubiquitous Computing*, vol. 19, no. 2, pp. 463–476, 2014.

[8] Korea Association of Smart Home, http://www.kashi.or.kr/html/smarthome_001.html.

[9] S. Y. Cheong, J. Y. Cheon, and Y. H. Yoon, "An analysis on characteristics of space design and U-service of smart home for the elderly," in *Proceedings of the AIK General Meeting and Spring Conference*, vol. 31, pp. 91–92, Architectural Institute of Korea, April 2011.

[10] N. K. Suryadevara, A. Gaddam, R. K. Rayudu, and S. C. Mukhopadhyay, "Wireless sensor network based safe home to care elderly people: behavior detection," in *Proceedings of the EuroSensors XXV*, Athens, Greece, September 2011.

[11] Y. Charlon, W. Bourennane, F. Bettahar, and E. Campo, "Activity monitoring system for elderly in a context of smart home," *IRBM*, vol. 34, no. 1, pp. 60–63, 2013.

[12] H. Lee, J. Y. Jung, and S. J. Park, "Smart services of the bathroom reflecting the behavior patterns of the elderly," *Korean Institute of Interior Design Journal*, vol. 22, no. 1, pp. 256–264, 2013.

[13] F. Portet, M. Vacher, C. Golanski, C. Roux, and B. Meillon, "Design and evaluation of a smart home voice interface for the elderly: acceptability and objection aspects," *Personal and Ubiquitous Computing*, vol. 17, no. 1, pp. 127–144, 2013.

[14] J. Kim, H.-S. Choi, H. Wang, N. Agoulmine, M. J. Deen, and J. W.-K. Hong, "POSTECH's U-Health Smart Home for elderly monitoring and support," in *Proceedings of the IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM '10)*, pp. 1–6, Montreal, Canada, June 2010.

[15] J. Shen, C. Zhang, and C. Jiang, "TV-based caring videophone system for the elderly in the smart home environment," *Journal of Electrical and Computer Engineering*, vol. 2013, Article ID 651471, 7 pages, 2013.

[16] H.-J. Lee, S.-J. Kang, H.-G. Jang, C.-W. Jeong, and S.-C. Joo, "Implementation of u-care system based on multi-sensor in u-home environment," *Journal of Internet Computing and Services*, vol. 12, no. 2, pp. 135–147, 2011.

[17] M. Yu, A. Rhuma, S. M. Naqvi, L. Wang, and J. Chambers, "A posture recognition-based fall detection system for monitoring an elderly person in a smart home environment," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1274–1286, 2012.

[18] R. S. Ransing and M. Rajput, "Smart home for elderly care, based on wireless sensor network," in *Proceedings of the IEEE International Conference on Nascent Technologies in the Engineering Field (ICNTE '15)*, pp. 1–5, IEEE, Navi Mumbai, India, January 2015.

[19] S.-C. Kim, Y.-S. Jeong, and S.-O. Park, "RFID-based indoor location tracking to ensure the safety of the elderly in smart home environments," *Personal and Ubiquitous Computing*, vol. 17, no. 8, pp. 1699–1707, 2013.

[20] D.-M. Han and J.-H. Lim, "Design and implementation of smart home energy management systems based on ZigBee," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1417–1425, 2010.

[21] F. Baig, A. Mahmood, N. Javaid, S. Razzaq, N. Khan, and Z. Saleem, "Smart home energy management system for monitoring and scheduling of home appliances using zigbee," *Journal of Basic and Applied Scientific Research*, vol. 3, no. 5, pp. 880–891, 2013.

[22] A. Mahmood, I. Khan, S. Razzaq et al., "Home appliances coordination scheme for energy management (HACS4EM) using wireless sensor networks in smart grids," *Procedia Computer Science*, vol. 32, pp. 469–476, 2014, Proceedings of the 5th International Conference on Ambient Systems, Networks and Technologies (ANT '14), the 4th International Conference on Sustainable Energy Information Technology (SEIT '14).

[23] M. J. Usman, Z. Xing, H. Chiroma et al., "Recent advances on energy efficient cluster based routing protocols of wireless sensor networks for healthcare systems," *International Journal of Computer Science Issues*, vol. 11, no. 3, p. 41, 2014.

[24] D.-M. Han and J.-H. Lim, "Design and implementation of smart home energy management systems based on zigBee," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1417–1425, 2010.

[25] R. Arvind and M. Ramaswamy, "Power management in intelligent buildings using WSN," *International Journal of Modern Trends in Engineering and Science*, vol. 2, no. 1, 2015.

[26] T. J. Lampoltshammer, E. P. de Freitas, T. Nowotny et al., "Use of local intelligence to reduce energy consumption of wireless sensor nodes in elderly health monitoring systems," *Sensors*, vol. 14, no. 3, pp. 4932–4947, 2014.

[27] N. Samanta, A. K. Chanda, and C. RoyChaudhuri, "An energy efficient, mmnimally intrusive multi-sensor intelligent system for health monitoring of elderly people," *International Journal on Smart Sensing and Intelligent Systems*, vol. 7, no. 2, 2014.

[28] S. Park, M.-I. Choi, B. Kang, and S. Park, "Design and implementation of smart energy management system for reducing power consumption using ZigBee wireless communication module," *Procedia Computer Science*, vol. 19, pp. 662–668, 2013.

[29] S. Y. Shin, H. S. Park, and W. H. Kwon, "Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b," *Computer Networks*, vol. 51, no. 12, pp. 3338–3353, 2007.

[30] J.-H. Park and B.-S. Kim, "Reliable beacon transmission based MAC protocol for LR-WPANs over WLAN interferences," *Journal of Zhejiang University: Science C*, vol. 15, no. 6, pp. 470–481, 2014.

[31] W. Sun, O. Lee, Y. Shin et al., "Wi-Fi could be much more," *IEEE Communications Magazine*, vol. 52, no. 11, pp. 22–29, 2014.

[32] S. Lim and J. H. Chung, "A study on the elderly-friendly smart home planning based on healthcare: focused on user preference and activity of the elderly," in *Proceedings of the Architectural Institute of Korea Fall Conference*, September 2014.

[33] A. Atkinson, J. Payling, B. Lucas, and K. Gray, "Affordable housing adaptations using modular construction—a case study in applied project management," in *Proceedings of the CIB World Building Congress on Performance in Product and Practice*, pp. 535–545, Wellington, New Zealand, April 2001.

[34] M. Lawson, R. Ogden, and C. Goodier, *Design in Modular Construction*, CRC Press, New York, NY, USA, 2014.

[35] S. Azhar, A. Nadeem, J. Y. Mok, and B. H. Leung, "Building Information Modeling (BIM): a new paradigm for visual interactive modeling and simulation for construction projects," in *Proceedings of the 1st International Conference on Construction in Developing Countries*, pp. 435–446, Karachi, Pakistan, August 2008.