J Electr Eng Technol.2016; 11(2): 480-489
http://dx.doi.org/10.5370/JEET.2016.11.2.480

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

Interferer Aware Multiple Access Protocol for Power-Line Communication Networks

Sung-Guk Yoon†

Abstract – Hidden station problem can occur in power-line communication (PLC) networks. A simple solution to the problem has been proposed to use request-to-send (RTS)/clear-to-send (CTS) exchange, but this approach cannot solve the hidden station problem perfectly. This paper revisits the problem for PLC networks and designs a protocol to solve it. We first analyze the throughput performance degradation when the hidden station problem occurs in PLC networks. Then, we propose an interferer aware multiple access (IAMA) protocol to enhance throughput and fairness performances, which uses unique characteristics of PLC networks. Using the RTS/CTS exchange adaptively, the IAMA protocol protects receiving stations from being interfered with neighboring networks. Through extensive simulations, we show that our proposed protocol outperforms conventional random access protocols in terms of throughput and fairness.

Keywords: Hidden station problem, Interference mitigation, Power-line communications

1. Introduction

A real-time two-way communication infrastructure is necessary to build a next generation power grid, i.e., *Smart Grid*. Since power-line communication (PLC) uses power cables as its communication medium, it is becoming a prominent communication technology that enables smart grid. PLC in smart grid has multi-hop characteristic or multiple networks to cover a wide area. A measurement based study has been revealed that a communication signal of a PLC network can interfere with some signals from neighboring PLC networks [1]. In a multi-hop network or multiple networks with random access protocols, the hidden station problem [2], which severely degrades throughput and fairness performances, is a classical problem.

To tackle the hidden station problem, many researches have been done mainly in wireless networks [3-6]. They can be classified into: pure contention-based, busy tone-based, power aware, directional antenna-based, and multiple channel-based solutions [3]. In [3] and references therein, diverse solutions for the problem are proposed in wireless networks. The most popular solution to the hidden station problem is to use request-to-send (RTS)/clear-to-send (CTS) exchange before data transmission, which is a part of the IEEE 802.11 standard [4]. However, previous researches have already shown that the RTS/CTS exchange cannot solve the problem perfectly and even degrades the network performance further in some scenarios [5, 6].

Among the solutions from wireless networks, busy tone-based, directional antenna-based, and multiple channel-based solutions cannot be applied to PLC networks because most of PLC standards do not support the functions. To solve the hidden station problem in PLC, the other two solutions have been discussed. First approach is a kind of power aware solution that the hidden station's signal is regarded as a background noise and the signal-to-noise ratio (SNR) with a hidden station is measured [7]. However, this approach degrades PLC performance. The other approach is using the RTS/CTS exchange as IEEE 802.11 standard does, i.e., a pure contention based solution. The state-of-the-art PLC standards, such as ITU-T G.hn [8], IEEE 1901 [9], and HomePlug AV2 [10], have adopted this solution and commercial products of ITU-T G.hn and HomePlug AV2 are currently available at the market [11]. To use the power line medium efficiently, a PLC-customized solution is required.

In PLC, some interference control schemes to improve throughput performance have been proposed for the scheduled access [12]. Recent works have been done for PLC carrier sense multiple access with collision avoidance (CSMA/CA) performance enhancement [13] by knowing PLC channel characteristics [14]. In [15], impulsive noise mitigation algorithm has been proposed. However, to the best of our knowledge, no research for solving the hidden station problem in CSMA/CA rather than the mentioned two approaches has been carried out for PLC networks.

In this paper, we start with a brief performance analysis under the hidden station problem for PLC networks. Then, to solve the hidden station problem, we propose an interferer aware multiple access (IAMA) protocol that uses unique characteristics of PLC networks: static topology and PHY header information. A transmitter which uses IAMA protocol first checks the interference relationship between neighboring networks, and then, according to the

† Corresponding Author: School of Electrical Engineering, Soongsil University, Korea. (sgyoon@ssu.ac.kr)
Received: April 28, 2015; Accepted: September 9, 2015

Copyright ⓒ The Korean Institute of Electrical Engineers
This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

relationship, it decides whether to use the RTS/CTS exchange or not. The fundamental idea in the IAMA protocol is to protect each receiver from being interfered in reception. That is, if a receiver is in an interference relationship, a pair of transmitter and receiver uses the RTS/CTS exchange. Through extensive simulations, we confirm that our proposed IAMA protocol outperforms the other CSMA/CA protocol without RTS/CTS exchange (named the basic access), with RTS/CTS exchange (named the RTS/CTS access), and with power controlled RTS/CTS exchange in terms of throughput and fairness.

The remainder of this paper is organized as follows. In Section 2, we describe our system model for a PLC network. The hidden station problem is briefly described in Section 3. We analyze the performance degradation due to the problem in Section 4, and propose our IAMA protocol in Section 5. After evaluating the proposed protocol in Section 6, we conclude our paper in Section 7.

2. System Model

We consider a PLC system that consists of multiple logical networks. In this work, we use the IEEE 1901 PLC system [9] as a reference one, but any PLC system can be applied without restriction. We consider a homogeneous network where all PLC stations use a same PLC protocol. We refer to a logical network as a basic service set (BSS). A BSS consists of a BSS manager (BM) and several stations. The BM provides services for association, security, and neighboring network coordination. It is assumed that all the PLC stations have no mobility.

We assume that each BSS is separated by a MV/LV transformer. When a PLC signal penetrates a transformer, its strength is attenuated by about 50 dB [7]. Therefore, stations installed near the transformer suffer from interference from neighboring networks. Fig. 1 shows an example topology of our considered system. In this example, there are three BSSs, each of which has one BM; BM1 and BM2 are inside each transformer while BM3 is at the transformer. Each BSS can cover several houses or buildings. Stations *a* and *b* in BSS1 and station *a* in BSS2 interfere with each other. Also, all stations in BSS2 and station *a* in BSS3 interfere with each other.

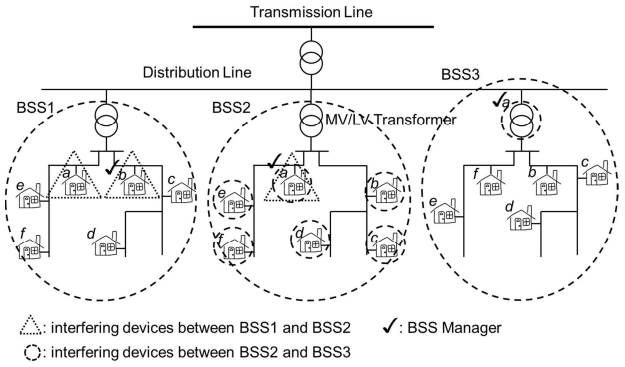

Fig. 1. Example topology

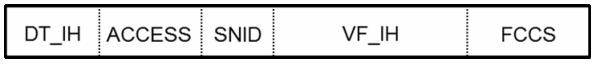

Fig. 2. PHY layer header format of IEEE 1901. DT_IH, SNID, VF_IH, and FCCS denote the type of the packet, the network ID, variant fields according to the packet type, and checksum for the PHY header, respectively [9].

It is assumed that each BSS is synchronized with the AC line cycle and each station can decode the other stations' transmissions within a BSS. Also, if a station is located at near the neighboring BSS, it can decode the physical (PHY) header of a packet from the neighboring BSS. Fig. 2 shows the PHY header format of IEEE 1901, which is 128 bits long [9]. In VF_IH, transmitter and receiver ID are included. Important difference to the IEEE 802.11 standard is that the PHY header has its own checksum. Therefore, any station that receives a packet with valid checksum can obtain information such as network ID, transmitter ID, and receiver ID even if the following data is corrupted.

3. Hidden Station Problem

One of the basic random access protocols for the shared channel is the CSMA/CA protocol. In the CSMA/CA protocol, each station senses the medium before transmission. If the medium is busy, it waits until the medium becomes idle. Otherwise, the station decreases its backoff counter (BC). When its BC reaches zero and the medium is idle, it transmits its packet. After the transmission, it chooses another BC for next transmission.

An important characteristic of channel sensing is that, even if a transmitter senses the medium idle, its receiver may sense it busy because the transmitter and receiver are in different locations. This characteristic possibly causes the hidden station problem. Because of the problem, two important performances, i.e., throughput and fairness degrade severely in some cases.

3.1 Throughput performance degradation

Fig. 3 shows an example of the throughput performance degradation because of the hidden station problem. In this example, *A* and *C* are transmitters, and *B* is their common receiver. Since the distance between *A* and *C* is longer

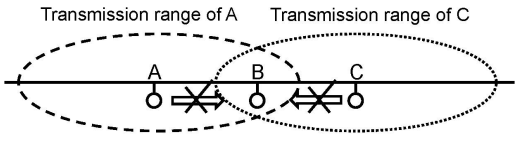

Fig. 3. Example of the throughput performance degradation because of the hidden station problem

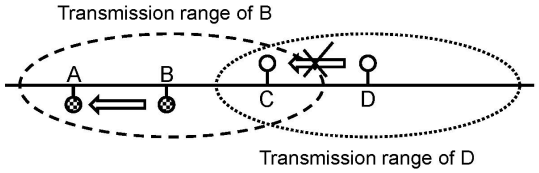

Fig. 4. Example of the fairness performance degradation because of the hidden station problem

than each station's transmission range, *A* and *C* cannot sense each other's transmission. Therefore, *A* starts a transmission regardless of whether *C* is transmitting or not. If *A* starts its transmission while *C* is transmitting, both transmissions will fail.

3.2 Fairness performance degradation

Fig. 4 shows an example of the fairness performance degradation because of the hidden station problem. In this example, *B* and *D* are hidden each other and attempt packet transmissions to *A* and *C*, respectively. When *B* is sending a packet, *C* should wait its reception until *B* completes its transmission for *A*. However, since *D* is out of the transmission range of *B*, it will send its packet to *C*, resulting in transmission failure. This problem leads to an unfair channel access between *B* and *D*.

3.3 Simulation results for the hidden station problem

In this section, we simulate to get an insight on the throughput and fairness performance degradations in a simple network due to the hidden station problem. There are two access modes of CSMA/CA protocol depending on the use of RTS/CTS exchange. The basic access exchanges data and acknowledge (ACK) packets directly (without RTS/CTS exchange), while the RTS/CTS access uses RTS/CTS exchange before data transmission. In the RTS/CTS access, when a station overhears an RTS or CTS packet, it defers its transmission until hearing the ACK. The timing information about the ACK transmission is included in the RTS and CTS packets. We define the throughput performance as channel utilization, i.e., the amount of time spent for delivering data over the total time. It is assumed that one data packet transmission takes 1274.96 usec that carries 24 orthogonal frequency-division multiplexing (OFDM) symbols [9].

Fig. 5 shows the throughput and fairness performance comparison with and without a hidden station. The left four bars represent throughput performance of the basic access and the RTS/CTS access for the simple hidden station scenario shown in Fig. 3. The left most two bars show the throughput performance with no hidden station. The basic access achieves 67.3% while the RTS/CTS access achieves 60.7%. Even in the case of no hidden station, the basic access cannot achieve 100% mainly because of the protocol overhead due to priority resolution slots, idle slots,

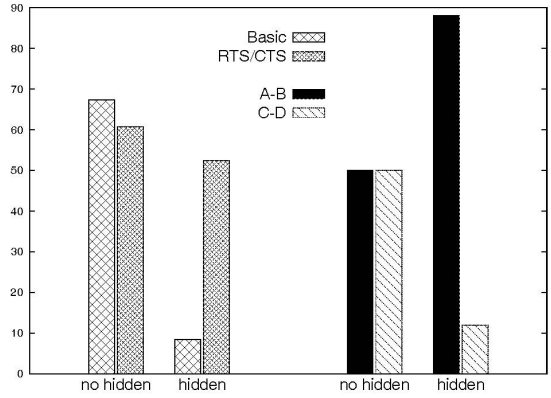

Fig. 5. Throughput performances of the basic access and the RTS/CTS access for the topology of Fig. 3 (left four bars); and fairness performances of A-B and C-D pairs for the topology of Fig. 4 (right four bars). The unit of y-axis is percent.

response interframe space, ACK transmission time, and contention interframe space [16]. In the RTS/CTS access, the protocol overhead increased because of the transmission times of RTS, CTS, the RTS-to-CTS gap, and the CTS-to-data gap, resulting in lowered throughput.

Under the hidden stations, i.e., next left two bars with titled "hidden," the throughput of the RTS/CTS access is slightly reduced to 52.4%, while that of the basic access is significantly reduced down to 8.5%. In the RTS/CTS access, although data and ACK transmissions are protected, RTS and CTS packets can still collide with other packet transmissions, resulting in slight performance degradation.

The fairness performance under the hidden station scenario in Fig. 4 is also shown in Fig. 5, i.e., right four bars. With no hidden station, the pairs of *A-B* and *C-D* share the medium equally, i.e., 50% each. However, with hidden stations, the pair of *A-B* occupies 88.1% while the pair of *C-D* takes a share of 11.9% of the total packet transmissions. This is due to particular positionings of receivers. That is, *A* is safe to receive a packet but *C* is not. Note that both the basic and RTS/CTS accesses shows similar result. That is, the RTS/CTS access is not the solution of the fairness performance degradation.

4. Throughput Analysis under the Hidden Station Problem in a PLC Network

In this section, the throughput performance of a PLC network under the hidden station problem is studied. We consider a simple hidden station scenario in Fig. 3, where two transmitters attempt to send packets to one common receiver and they are hidden from each other. In [17], PLC throughput performance has been analyzed under an assumption of no hidden station through a 3-dimensional discrete-time Markov chain. Some researches for throughput analysis under the hidden station problem have been

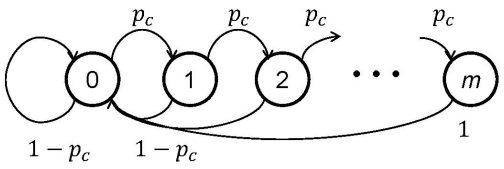

Fig. 6. Markov chain model

carried out in wireless networks [18]. However, to the best of our knowledge, there is no PLC throughput performance analysis under the presence of hidden stations. For PLC throughput analysis under hidden stations, we apply a method similar to that in [18].

4.1 Throughput Analysis

Steady-state probability: For simplicity, we assume that any overlapped receptions at a receiver result in collision and transmission failure. That is, the capture effect[1] is not considered. Fig. 6 shows the Markov chain model for a station under the considered scenario. The state represents the backoff procedure counter (BPC) of the station where m is the maximum BPC and p_c denotes the collision probability which is independent of the BPC.

When a station attempts to send a packet, it uses its initial BPC, i.e., 0. If it fails in transmission, it increases its BPC by one. Otherwise, it resets its BPC to 0. When it fails $m+1$ times consecutively, it discards the packet. With these state transition probabilities, we can obtain the steady-state probability p_i as

$$p_0 = (1-p_c)p_0 + (1-p_c)p_1 + \cdots + (1-p_c)p_{m-1} + p_m, \quad (1)$$

$$p_i = p_c^i p_0, \quad i \in [1, \cdots, m]. \quad (2)$$

The summation of all the steady-state probabilities equals one, that is, $\sum_{i=0}^{m} p_i = 1$. Therefore, we have

$$p_0 = \frac{1-p_c}{1-p_c^{m+1}}. \quad (3)$$

This represents that all the steady-state probabilities can be expressed with p_c.

Vulnerable period: We now define the vulnerable period T_v during which any transmission from an interferer results in a collision. This period differs depending on the RTS/CTS use of the CSMA/CA protocol. If the interferer starts its transmission during a data transmission of a victim, both transmissions fail. In the basic access, if the interferer starts its transmission when a receiver is preparing the ACK transmission, the receiver should reply with ACK packet. Therefore, the ACK transmission time is not included in T_v in the basic access. That is, $T_v = 2T_{data}$ where T_{data} is the data transmission time.

In the RTS/CTS access, however, if the interferer sends a packet while the receiver is preparing for CTS transmission, the receiver cannot reply with CTS packet. Therefore, the vulnerable period becomes twice an RTS transmission time plus the RTS to CTS gap (RCG), i.e., $T_v = 2(T_{RTS} + T_{RCG})$ where T_{RTS} and T_{RCG} denote the durations of RTS and RCG, respectively.

The unit of T_v is second, and we transform this unit into the number of idle slots. Let σ denote an idle slot time in IEEE 1901. Then, we can express the vulnerable period in unit of idle slots as $T_{v,slot} = T_v / \sigma$.

Collision probability: We now derive the collision probability p_c. It is assumed that any overlapped transmissions during T_v result in a collision. Then, we obtain the collision probability as

$$p_c = \sum_{i=0}^{m} p_i \cdot P[BC_i \le T_{v,slot}], \quad (4)$$

where BC_i is a chosen BC at BPC i. If a station succeeds in transmission, it resets its BPC to 0. If not, it increases its BPC by one. When transmission failure occurs m times consecutively, it drops the packet. The contention window (CW) size for a station in the IEEE 1901 CSMA/CA protocol is listed in Table 1. A station chooses a random number in [0, CW_i] as its BC_i at BPC i. Inserting the steady-state probabilities of (2) and (3) into (4) and using a numerical method, we can obtain p_c.

Throughput performance[2]: Using p_c and the analysis method in [17], we can obtain the throughput for the considered PLC network. In our considered case of two transmitters, the probability that a station transmits a packet becomes p_c. For n stations, at least one station

Table 1. IEEE 1901 system parameters

Simulation parameter	Value
CW at BPC = 0	7
CW at BPC = 1	15
CW at BPC = 2	31
CW at BPC > 2	63
Maximum BPC	6
T_{PHY}	110.48 usec
T_{RTS}, T_{CTS}, T_{ACK}	110.48 usec
T_{CIFS}	100 usec
T_{RIFS}	120 usec
T_{RCG}, T_{CMG}	120 usec
σ	35.84 usec
T_{sym}	48.52 usec
Response timeout	230.48 usec
Transmission power	24 dBm
Carrier sensing threshold	-35 dBm

[1] A receiver can successfully decode a stronger signal even if multiple signals are received simultaneously.

[2] Here, we define the throughput performance as channel utilization.

transmits with the probability of $p_{tr} = 1-(1-\tau)^n$, where τ is the probability that a station attempts a transmission in a randomly chosen time slot. Then, we have the probability that a station successfully transmits a packet as $p_s = \frac{n\tau(1-\tau)^{n-1}}{p_{tr}}$. Finally, we obtain the throughput as

$$S = \frac{p_{tr} p_s T_{data}}{(1-p_{tr})\sigma + p_{tr}(p_s T_s + (1-p_s)E[T_c])}, \quad (5)$$

where T_s and T_c are the total time required for a successful data packet transmission and the amount of wasted time due to a collision, respectively.

For the transmission time of a data packet, we have

$$T_{data} = T_{PHY} + k \cdot T_{sym}, \quad (6)$$

where k is the number of OFDM data symbols in a packet, and T_{PHY} and T_{sym} are the PHY header transmission time and one OFDM symbol duration, respectively. For the basic access, we have T_s as

$$T_{s,basic} = T_{data} + T_{RIFS} + T_{ACK} + T_{CIFS}, \quad (7)$$

where T_{RIFS}, T_{ACK}, and T_{CIFS} denote the durations of the response-distributed spacing (RIFS), ACK, and the contention distributed spacing (CIFS), respectively. For the RTS/CTS access, we have T_s as

$$T_{s,RTS/CTS} = T_{RTS} + T_{RCG} + T_{CTS} + T_{CMG} + T_{s,basic}, \quad (8)$$

where T_{CTS} and T_{CMG} denote the durations of CTS and the CTS to data gap, respectively.

For the wasted time due to a collision, we have the T_c as $T_{c,basic} = T_{data} + T_{RIFS} + T_{ACK} + T_{CIFS}$ for the basic access, which is the same as the successful transmission time for a data packet, and as $T_{c,RTS/CTS} = T_{RTS} + T_{RCG} + T_{CIFS}$ for the RTS/CTS access. Table 1 summarizes the IEEE 1901 system parameters used in numerical analysis and simulations [9].

4.2 Numerical results

Fig. 7 shows the throughput performance for the simple hidden topology in Fig. 3 according to the number of OFDM symbols in a data packet. The data packet transmission time linearly increases with the number of OFDM symbols in a data packet as expressed as in (6). For example, considering 12 and 24 symbols in a data packet, we have the packet transmission times of 692.72 usec and 1274.96 usec, respectively.

The numerical and simulation results for the RTS/CTS access shows that the analysis is very accurate with the error rate of less than 1.5%. For the basic access, however, the gap between two results rises from 5% to 17% when the number of symbols in a data packet is greater than 17. The large gap for large sized packets comes from the synchronous assumption that the two transmitters synchronously starts to transmit at each backoff stage. This assumption is no longer valid when the packet transmission time becomes large.

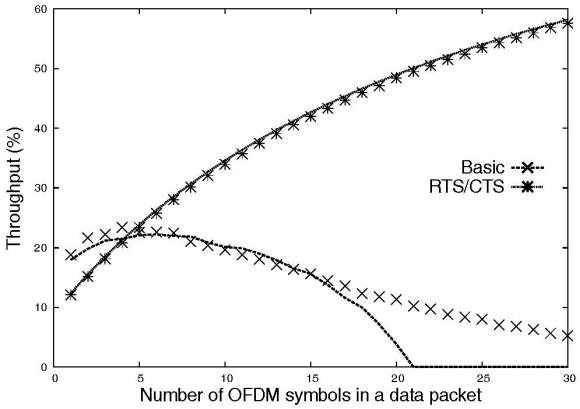

Fig. 7. Throughput performance for a simple hidden topology according to the number of OFDM symbols in a data packet

It is confirmed that the throughput performance for the basic access is severely degraded under the presence of hidden stations. For a packet containing 12 data symbols, the throughput degradation due to hidden stations is greater than 50%. For 24 data symbols, the degradation reaches 80%[3].

5. Interferer Aware Multiple Access in a PLC Network

To overcome the performance degradation caused by hidden stations in PLC networks, using the RTS/CTS access is a good approach. However, it increases the protocol overhead, resulting in throughput degradation when there is no hidden station. Also, the RTS/CTS access cannot solve the fairness performance degradation problem. To overcome these drawbacks of the RTS/CTS access, we propose to use the interferer aware multiple access (IAMA) protocol for PLC networks. Our proposed IAMA protocol consists of two phases: initialization and runtime operation. In the initialization, each BSS collects the information on

[3] We can easily convert the obtained normalized throughput into bits/sec. For instance, if the throughput is 0.5, it indicates that 50% of the time is spent for data packet transmission. Since one OFDM symbol time is 48.52 usec, there are 20610 OFDM symbols in one second and 10305 symbols out of them are used in data transfer. If the transmitter uses the 64QAM 16/21 modulation and coding scheme, each symbol carries $6 \times 16/21 = 4.57$ bits. Therefore, the throughput in bits/s for a carrier is $10305 \times 4.57/1 \approx 47.1$ kb/s. Since IEEE 1901 has 917 subcarriers, the throughput of 0.5 corresponds to 47.1 kb/s $\times 917 = 43.2$ Mb/s.

nearby interfering networks through decoding the PHY header. With this information, our proposed IAMA smartly decides whether to use the RTS/CTS exchange or not, and the transmission power during runtime operation.

5.1 Initialization

The goal of the initialization phase is to obtain information on which stations are suffering from interference towards other neighboring BSSs. To this end, each station freely transmits packets during the initialization phase. Any transmission within the same BSS is not considered as interference.

When a station receives a packet with valid PHY header checksum, it can get BSS ID from the PHY header of the packet. If BSS ID is different, i.e., neighboring BSS, it reports the existence of interfering station to its BM. After receiving all the reports from stations, the BM creates a table for interfering neighbor BSSs (TINB). TINB keeps the interference related information such as its own BSS ID (BID), station IDs (SIDs), neighboring BSS IDs (N-BIDs), and station IDs in neighboring BSSs (N-SIDs). The created TINB is shared all the station in the BSS through the broadcasting beacon. Note that TINB can be changed when stations join or leave a network so TINB is continuously updated and broadcasted in every minute.

Fig. 8 and Table 2 show an example topology and a TINB created and managed by the BM of BSS2. Three stations in BSS2 can hear transmissions from neighboring BSSs. Station *b* in BSS2 can hear transmission from station *y* in BSS4. Stations *c* and *d* in BSS2 can hear transmissions from station *k* in BSS1. Here, "hear" implies "interfere with."

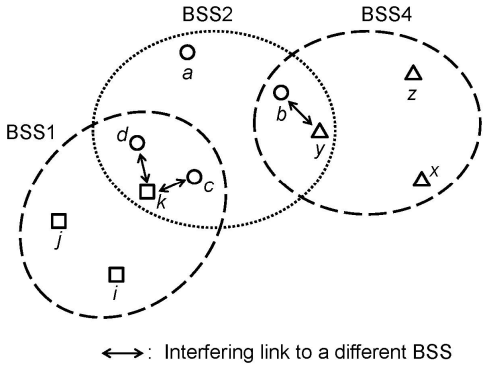

Fig. 8. Example logical topology for a PLC network. Squares, circles, and triangles represent stations in BSS1, BSS2, and BSS4, respectively.

Table 2. Example of TINB for BSS2 in Fig. 8

BID	SID	N-BID	N-SID
2	*b*	4	*y*
2	*c*	1	*k*
2	*d*	1	*k*

5.2 Runtime operation

With the interference information, the IAMA protocol aims to protect receivers from interference. For doing so, the RTS/CTS exchange is used only when the receiver is at the risk of being interfered with neighboring BSSs. Otherwise, the basic access will be applied. According to the TINB, the IAMA protocol classifies transmission pairs into four cases, and applies a different channel access strategy for each case.

To improve spatial reuse, the IAMA protocol does not use virtual carrier sensing for transmissions of neighboring BSSs. When a sender has a data packet to transmit, it checks whether the sender itself and its receiver are in TINB or not. Then, it decides whether to transmit the data packet directly (the basic access) or to use the RTS/CTS exchange before data transmission (the RTS/CTS access).

1) **Both of transmitter and receiver are not in TINB:** Since there is no interference from neighboring BSSs, the transmitter and receiver run the basic access with maximum transmission power.
2) **Transmitter is not in TINB but receiver is:** Fig. 9 with transmitter *A* and receiver *B* shows an example of this case. Station *B* is interfering with station *C* which belongs to another BSS. Because the transmitter needs to protect its data transmission from interference of neighboring BSS, the RTS/CTS access is applied. By exchanging RTS/CTS packets, the hidden station of *B* (*C* in this example) is aware of a transmission of *A*. The transmitter does not interfere with any station in the neighboring BSS, so it uses its maximum power for RTS and data transmissions. However, the receiver adjusts the power for CTS and ACK transmissions to avoid generating severe interference toward neighboring BSSs.

   Transmitters in this case operate the RTS/CTS access with no modification. That is, after the transmitter waits until its BC reaches zero, it sends an RTS packet and our proposed IAMA protocol works at the receiver, as shown in Fig. 10. If the receiver does not sense a transmission from a neighboring BSS[4], it uses its maximum power for CTS and ACK packets. If it senses

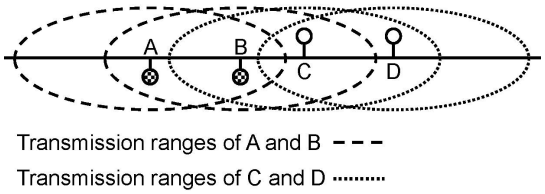

Fig. 9. Example topologies for cases 2 and 3. Nodes with dotted and empty circles indicate that they belong to different BSSs, respectively.

[4] Even if a neighboring BSS occupies the medium, it is always sensed idle at the transmitter side in this case.

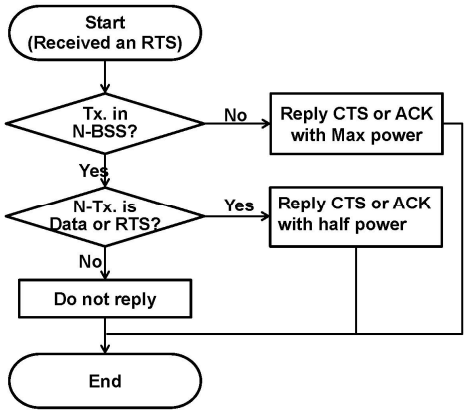

Fig. 10. Flow charts for the receiver in case 2.

a packet transmission from the neighboring BSS, it checks the packet type. If the type is data or RTS, the receiver reduces its transmission power by half to avoid generating severe interference toward the neighboring BSS. If the type is CTS, the receiver does not reply to the transmitter.

Note that our protocol allows the receiver to reply CTS and ACK to the transmitter even under on-going transmission of a neighboring BSS. This approach solves the unfairness problem which comes from the hidden station problem.

3) Transmitter is in TINB but receiver is not: This case is shown in Fig. 9 with transmitter *B* and receiver *A*. Since the receiver is not suffering from transmissions of neighboring BSSs, the basic access is applied. The use of the basic access improves throughput performance. Receivers in the case operate the basic access without modification. However, since the transmitter is in the interference range of the neighboring BSS, it operates our proposed IAMA shown in Fig. 11.

When the BC at the transmitter reaches zero, the algorithm starts. If the transmitter does not sense a transmission from a neighboring BSS, it sends a data packet with maximum power. Otherwise, the transmitter checks the type of a neighboring BSS's transmission. If the transmission of the neighboring BSS is performed without RTS/CTS exchange, the transmitter sends a data packet with maximum power since the receiver is

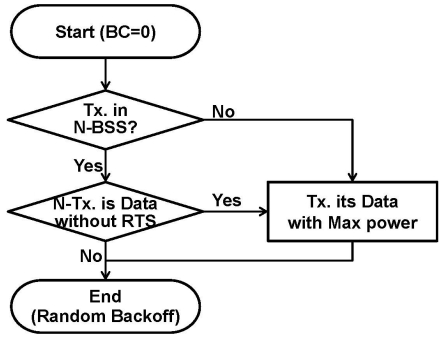

Fig. 11. Flow charts for the transmitter in case 3.

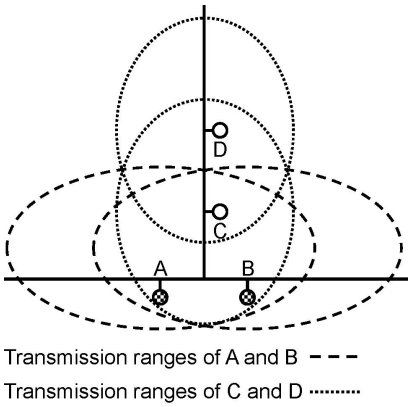

Fig. 12. Example topologies for 4. Nodes with dotted and empty circles indicate that they belong to different BSSs, respectively.

not in the TINB. However, if the transmission of the neighboring BSS uses the RTS/CTS exchange, the transmitter defers its transmission until the transmission of the neighboring BSS is complete.

4) Both transmitter and receiver are in TINB: Fig. 12 shows an example of this case. Since both the transmitter and receiver (*A* and *B*) are in the transmission range of neighboring BSSs (*C*), the RTS/CTS access is applied. In order to avoid being interfered too much by neighboring BSSs, both the transmitter and receiver adjust their transmission powers by half according to the medium state. The flow charts for the transmitter and receiver are shown in Figs. 10 and 11, respectively. The only difference is that they use a reduced power by half again when they sense a transmission from a neighboring BSS.

Table 3 summarizes the proposed algorithm. Only if receiver is in interference range of neighboring BSS, the RTS/CTS access is used. The power control is performed at the stations which are in TINB.

Table 3. Summary of IAMA Runtime Operation

Case	Tx in TINB	Rx in TINB	Access type	Power control
1	X	X	Basic	None
2	X	O	RTS/CTS	Receiver
3	O	X	Basic	Transmitter
4	O	O	RTS/CTS	Both

6. Performance Evaluation

In this section, we compare the performance of our proposed IAMA protocol with those of the basic access, RTS/CTS access, and RTS/CTS access with power control [5] in terms of throughput and fairness. In the RTS/CTS access with power control scheme, the RTS/CTS exchange are performed with maximum power, and the following data and ACK transmissions' power are adjusted to solve the hidden station problem.

Fairness performance is measured through Jain's fairness index I_F [19], which is given as

$$I_F = \frac{(\sum_{j=1}^{N} X_j)^2}{N\sum_{j=1}^{N} X_j^2}, \quad (9)$$

where X_j and N denote the number of packet transmissions of station j and the total number of stations, respectively. The fairness index has a value in $[1/N, 1]$. As I_F is close to one, each station transmits a similar number of packets. Perfect fairness (i.e., $I_F = 1$) is achieved when each station transmits a same number of packets.

6.1 Simulation settings

We consider two scenarios; one is a simple hidden station scenario of two transmission-reception pairs and the other is more general scenarios of several BSSs. In our simulations, we use the IEEE 1901 CSMA/CA protocol with parameter values given in Table 1 [9]. We use an event-driven simulator written in C++ language for simulation.

To emulate the PLC channel, we use a PHY abstraction model [20]. In the model, a statistical channel model is used to generate a power line channel and the channel is modeled as a sum of weighted Dirac-impulses [21]. The PHY abstraction method offers four power line channel models (excellent, good, medium, and bad) with a log-linear approximation of the packet error rate (PER). We adopt the "good" channel model, which consists of 10 different paths, and three modulation and coding schemes, including QPSK 1/2, 16QAM 1/2, and 64QAM 16/21. In this model, if the received SNR is higher than some threshold value given in the PHY abstraction model, the packet reception is successful. The given SNR threshold values for 64QAM 16/21 are 12 dB, 15 dB, 15.5 dB, and 16 dB for PER values of 1, 0.1, 0.01, and 0.001, respectively.

By using the PHY abstraction model, the capture effect is also counted, where a station can decode a received packet with sufficiently strong signal strength against some interference. When the received SNR including interference, i.e., SINR, is higher than the threshold value, the packet is successfully received. Otherwise, it is corrupted.

6.2 Simple scenario

This scenario considers only two transmission-reception pairs. According to the position of each station, we have the following five cases:

- **Case I**: *B* **and** *C* are transmitters, and *A* and *D* are receivers as shown in Fig. 9.
- **Case II**: *B* and *D* are transmitters, and *A* and *C* are receivers as shown in Fig. 9.
- **Case III**: *A* and *D* are transmitters, and *B* and *C* are receivers as **shown** in Fig. 9.
- **Case IV**: *A* **and** *C* are transmitters, and *B* and *D* are receivers as shown in Fig. 12.
- **Case V**: *A* **and** *D* are transmitters, and *B* and *C* are receivers as shown in Fig. 12.

Figs. 13 and 14 show the throughput and fairness performance results for the five cases, respectively. The basic and RTS/CTS accesses show very much different performance depending on each case. Our proposed IAMA protocol shows good and steady performance in terms of both throughput and fairness. In Case I, the RTS/CTS access shows the worst performance in throughput because of the additional protocol overhead. Our proposal shows the best throughput performance owing to its efficient channel access mechanism.

In Case II, the basic access achieves the best throughput but poor fairness performance. Also, the RTS/CTS access shows poor fairness performance. Since the two transmitters are hidden from each other, they transmit packets regardless of the existence of other ongoing transmission. Then, due to the location of each station, the transmission for the pair of *A* and *B* succeeds while that for

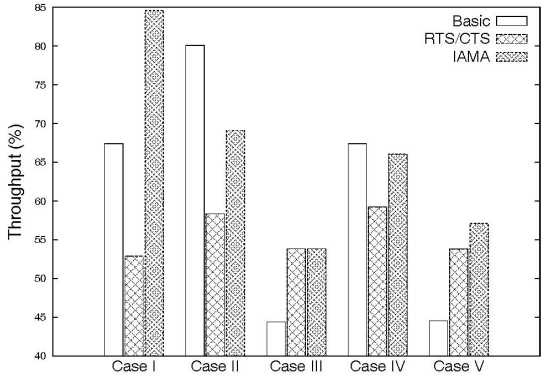

Fig. 13. Throughput performance of the simple scenario

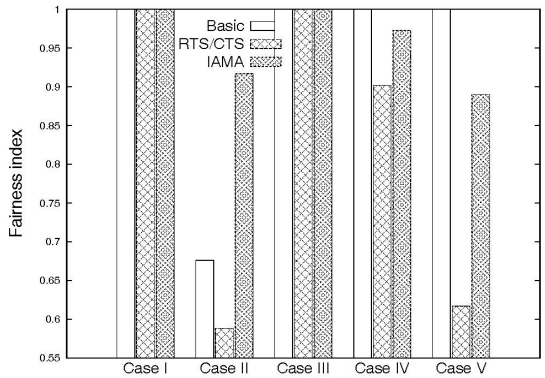

Fig. 14. Fairness performance of the simple scenario

the other pair fails, resulting in poor fairness performance. In our proposal, however, *C* (receiver) replies with CTS even under the transmission of *B* as explained in Fig. 11. Therefore, our proposal improves the fairness performance by 56% compared to the RTS/CTS access.

In Case III of the hidden station problem, the basic access shows the worst throughput performance, and the other two accesses show the same performance. In this case, the IAMA protocol operates in the same way as the RTS/CTS access, so they achieve the same performance. In Case IV, the RTS/CTS access shows the worst throughput and fairness performance, and the basic access and our proposal show similar performance.

In Case V, the basic and RTS/CTS accesses show the worst throughput and fairness performance, respectively. The basic access achieves the lowest throughput due to the hidden station problem. In the RTS/CTS access, owing to the location of each station, the pair of *A* and *B* is able to occupy the channel most of the time. Our proposal shows good throughput and fairness performance in this case too.

Note that the RTS/CTS access with power control access shows the same performance with the RTS/CTS access since power control has no meaning with only four stations.

6.3 General scenarios

In this scenario, we change the number of BSSs from two to six. Each BSS has three transmission-reception pairs, i.e., six stations. That is, we vary the number of stations from 12 to 36. The case of three BSSs is shown in Fig. 1.

The throughput and fairness simulation results are shown in Figs. 15 and 16, respectively. The basic access and IAMA show good throughput performance regardless of the number of BSSs. The fairness performance of the basic access shows the worst while that of the IAMA show the best. The RTS/CTS access achieves the worst throughput performance and small fairness performance improvement compared to the basic access. The RTS/CTS access with power control shows almost the same performance with the RTS/CTS access since PLC networks have relatively low density compared to wireless networks.

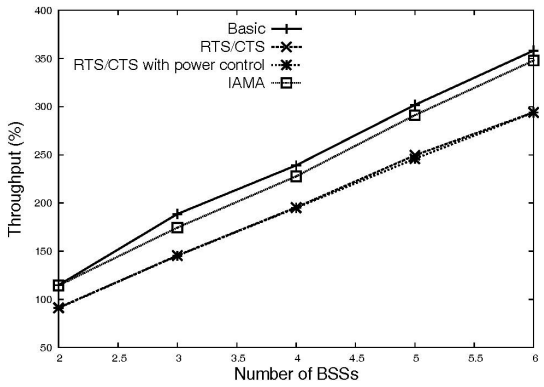

Fig. 15. Throughput performance according to the number of BSSs

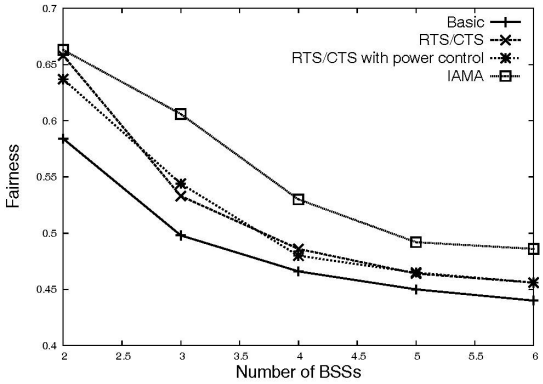

Fig. 16. Fairness performance according to the number of BSSs

Note that 200% throughput performance means that two concurrent transmissions exist on average in the network.

In conclusion, our proposed IAMA protocol always shows the best or close to the best throughput and fairness performance, regardless of given topologies. It is because the IAMA protocol uses the RTS/CTS exchange adaptively according to the topology information which is obtained by decoding the PHY header.

7. Conclusion

Power-line communication (PLC) networks are not free from hidden station problem when multiple logical networks coexist. In this paper, we have first analyzed the throughput performance degradation under the hidden station problem scenario. To solve the hidden station problem, we then have proposed a new multiple-access protocol, named the interferer aware multiple access (IAMA) protocol, which uses unique characteristics of PLC networks. According to the relative positions of the transmitter and receiver, our proposed IAMA protocol adaptively decides whether to use the RTS/CTS exchange or not. Basically, the RTS/CTS exchange is used to protect the receiver from being interfered with neighboring networks. The simulation results have showed that our proposal steadily achieves overall good performance in terms of throughput and fairness, regardless of given topologies.

Acknowledgements

This work was supported by the Soongsil University Research Fund of 2014.

References

[1] Z. Liu, A. El Fawal and J. -Y. Le Boudec,

"Coexistence of Multiple HomePlug AV Logical Networks: A Measurement Based Study," in *Proc. IEEE GLOBECOM*, Houston, USA, Dec. 2011.
[2] F. Tobagi and L. Kleinrock, "Packet Switching in Radio Channels: Part II-The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," *IEEE Trans. Commun.*, vol. 23, no. 12, pp. 1417-1433, Dec. 1975.
[3] K. Kosek-Szott, "A Survey of MAC Layer Solutions to the Hidden Node Problem in Ad-Hoc Networks," *Ad Hoc Networks*, vol. 10, no. 3, pp. 635-660, May 2012.
[4] IEEE 802.11-2012, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE Std., Mar. 2012.
[5] Y. Zhou and S. Nettles, "Balancing the Hidden and Exposed Node Problems with Power Control in CSMA/CA-Based Wireless Networks," in *Proc. IEEE WCNC*, Mar. 2005.
[6] B. Alawieh, Y. Zhang, C. Assi, and H. Mouftah, "Improving Spatial Reuse in Multihop Wireless Networks-A Survey," *IEEE Commun. Surveys Tutorials*, vol. 11, no. 3, pp. 71-91, Third Quater 2009.
[7] ETSI, "PowerLine Telecommunications (PLT) Hidden Node Review and Statistical Analysis," Technical Report ETSI TR 102 269 V1.1.1 (2003-12), ETSI, Dec. 2003.
[8] International Telecommunications Union (ITU), "ITU-T recommendation G.9961, Data Link Layer (DLL) for unified high-speed wire-line based home networking transceivers," Geneva, Switzerland, Jun. 2010.
[9] IEEE Std P1901-2010 "Standard for Broadband over Power Line Net- works: Medium Access Control and Physical Layer Specifications," 2010.
[10] HomePlug Powerline Alliance, "HomePlug AV Specification Version 2.0," Beaverton, OR, USA, Jan. 2012.
[11] D. Ngo, "Top five power line adapters: When Wi-Fi fails you," CNET Report, Jun. 2015, available: http://www.cnet.com/news/top-five-power-line-adapters-when-wi-fi-fails-you/
[12] D. Ayyagari and W.-C. Chan, "A Coordination and Bandwidth Sharing Method For Multiple Interfering Neighbor Networks," in *Proc. IEEE CCNC*, Las Vegas, USA, Jan. 2005.
[13] S.-G. Yoon, D. Kang, and S. Bahk, "Multichannel CSMA/CA Protocol for OFDMA-Based Broadband Power-Line Communications," *IEEE Trans. Power Delivery*, vol. 28, no. 4, pp. 2491-2499, Oct. 2013.
[14] K. Ouahada, "Nonbinary Convolutional Codes and Modified M-FSK Detectors for Power-Line Communications Channel," *J. Commun. Netw.*, vol. 16, no. 3, pp. 270-279, Jun. 2014.
[15] J. Lin, M. Nassar, and B. Evans, "Impulsive Noise Mitigation in Powerline Communications Using Sparse Bayesian Learning," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1172-1183, Jul. 2013.
[16] S.-G. Yoon and S. Bahk, "Adaptive rate control and contention window size adjustment for power line communication," *IEEE Trans. Power Del.*, vol. 26, no. 2, pp. 809.816, Apr. 2011.
[17] M. Chung, M.-H. Jung, T.-J. Lee, and Y. Lee, "Performance Analysis of HomePlug 1.0 MAC With CSMA/CA," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 7, pp. 1411-1420, Jul. 2006.
[18] A. Tsertou and D.I. Laurenson, "Revisiting the Hidden Terminal Problem in a CSMA/CA Wireless Network," *IEEE Trans. Mobile Comput.*, vol. 7, no. 7, pp. 817-831, Jul. 2008.
[19] R. Jain, D. Chiu, W. Hawe, A quantitative measure of fairness and dis-crimination for resource allocation in shared systems, Technical Report, DEC TR-301, Littleton, MA, 1984.
[20] K.-H. Kim, H.-B. Lee, Y.-H. Lee, and S.-C. Kim, "PHY Abstraction Methodology for the Performance Evaluation of PLC Channels," in *Proc. IEEE ISPLC*, Rio de Janeiro, Brazil, Mar. 2010.
[21] Pathloss as a Function of Frequency, Distance and Network Topology for Various LV and MV European Powerline Networks, The OPERA Consortium, Project Deliverable, EC/IST FP6 Project No. 507667 D5v0.9, Apr. 2005.

Sung-Guk Yoon He received the B.S. and Ph.D. degrees from Seoul National University, Seoul Korea, in 2006 and 2012, respectively. From 2012 to 2014, he was a Postdoctoral Researcher at the same university. He is currently with Sonngsil University as an Assistant Professor since March 2014. His research interests include smart grid and power line communications.