Journal of ELECTRICAL ENGINEERING, VOL 73(2022), NO5, 355–358

sciendo

COMMUNICATIONS

Novel MAC routing protocol for wireless sensor networks based on IEEE 802.11 ad hoc networks

Woo-Yong Choi[1]

Due to the lack of efficient specified multi-hop routing protocol, IEEE 802.11 ad hoc networks have been in limited use for realizing wireless sensor networks where wireless sensors are dispersed in a region and each sensor can transmit its data to one another. We propose a novel MAC routing protocol for IEEE 802.11 wireless sensor networks, of which the service areas are extended by appropriately appointed pseudo-access points.

K e y w o r d s: wireless sensor networks, Mac, routing, wireless LANs

1 Introduction

As the society experiences the rapid transition to the fourth industrial revolution, more and more machines and devices are interconnected through wireless sensors. In wireless sensor networks, sensors are usually indirectly connected through multiple intermediate sensors because of relatively limited battery power of sensors. For the realization of wireless sensor networks, a sophisticated routing scheme, which considers the transient state of wireless channel between sensors, is required.

Thanks to the advanced development of IEEE 802.11 wireless LAN technologies like IEEE 802.11ac, IEEE 802.11af and IEEE 802.11ah in [1, 2, 3], IEEE 802.11 ad hoc network technology is promising to realize wireless sensor networks. Especially, IEEE 802.11ah wireless LANs can be used for large sensor networks [3]. However, for IEEE 802.11 ad hoc network technology to be successfully applied to realize wireless sensor networks, efficient multi-hop routing protocol for IEEE 802.11 ad hoc networks should be specified.

In the literature, based on IEEE 802.11 wireless LANs, various wireless sensor networks have been designed and developed to support the applications such as environmental control and agricultural and medical monitoring [3-8]. In [3], even though multi-hop communication among stations is possible, ad hoc multi-hop routing protocol for IEEE 802.11ah wireless LANs is not specified. The mesh routing protocol in [4] is too complicated to be applied to sensors with limited processing and power capabilities. Web server directly collects sensory data of temperature, humidity and gas leakage through IEEE 802.11 wireless LAN module in [5]. For agricultural monitoring in [6], sensors use IEEE 802.11 wireless LAN communication module to send agricultural data to router within their wireless communication range. In [7], IEEE 802.11af networks are employed for wireless communication of medical data between APs (access points) and stations. In [8], two-hop transmission scheme that allows sensors with low battery power to transmit their data to APs through pseudo-APs is proposed. To significantly reduce implementation and operational cost of wireless sensor networks based on IEEE 802.11 wireless LANs for various applications, efficient multi-hop routing protocol for IEEE 802.11 ad hoc networks should be specified.

In this paper, we specify the schemes for continuously extending IEEE 802.11 ad hoc networks by appropriately appointed pseudo-APs, and each sensor collecting the connectivity information of IEEE 802.11 ad hoc networks. Wireless sensor networks are created by the result of continuous extensions of IEEE 802.11 ad hoc networks. Based on the schemes for extending IEEE 802.11 ad hoc networks and collecting the connectivity information of wireless sensor networks, efficient multi-hop routing protocol for wireless sensor networks based on IEEE 802.11 ad hoc technology is proposed. To appropriately select new pseudo-APs, through which new sensors can join wireless sensor networks, the connectivity information among sensors is considered.

2 Proposed efficient multi-hop routing protocol

According to [9], an IEEE 802.11 ad hoc network can be initiated by a node of sensor, which periodically broadcasts beacon frames that contain the information elements of the set R of supported data rates and beacon period P. Here R represents the set of data rates with

[1] Department of Industrial and Management Systems Engineering, Dong-A University Nakdong-daero, Saha-gu, Busan, Korea, wychoi77@dau.ac.kr

https://doi.org/10.2478/jee-2022-0048, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X

which each sensor in the network should be able to transmit and receive data, and P the targeted period of beacon frame transmissions. Receiving beacon frames, other sensors can join the network after the authentication process. All sensors that have joined the network participate in the periodic transmission process of beacon frames [9].

We assume that in the IEEE 802.11 ad hoc network all beacon, data and management frames are transmitted using the DCF (Distributed Coordination Function) protocol [9]. At the initiation of the IEEE 802.11 ad hoc network, the first node is appointed as the pseudo-AP.

Hearing beacon, data or management frames transmitted from sensors in the network with one of supported data rates, each sensor i maintains the set S_i of the MAC (Medium Access Control) addresses of the sensors, of which the transmission signal can be successfully received and decoded by itself. When sensor i can hear the transmission signal of a new sensor not in S_i, the MAC address of the new sensor should be added to S_i.

When sensor i has not heard the transmission signal of sensor j in S_i for more than the amount of time $S_i 3 \times |S_i| P$, the MAC address of sensor j should be removed from S_i.

When the changes of S_i are detected, sensor i reports to the pseudo-AP the changes of S_i by transmitting to the pseudo-AP null or data frames on which the MAC addresses of the sensors that were added to or removed from S_i are piggybacked. The pseudo-AP regularly piggybacks the updated connectivity information of the network, which is the updated set S_i for each sensor, on the next beacon frames broadcast from itself. Detecting the changes of the connectivity information of the network from the beacons frames received from the pseudo-AP, each sensor piggybacks the changes of the connectivity information on the next three beacon frames broadcast from itself.

As stated in [10], considering the connectivity in the network, an appropriate sensor, which has possibly the greatest degree of connectivity with other sensors, should be appointed as the pseudo-AP. The degree D_k of the connectivity of sensor k is defined as the number of the sensors, which can hear the transmission signal of sensor k, and of which the transmission signal can be heard by sensor k. According to the changes of the connectivity of the network, the current pseudo-AP can appoint another sensor to be the new pseudo-AP by transmitting a management frame to the new pseudo-AP [10]. In [10], for an IEEE ad hoc network one-hop or two-hop transmission between nodes is possible through a pseudo-AP, which collects the connectivity information using the PCF (Point Coordination Function) protocol.

Up to this point of this paper, we implicitly assumed that there is only one pseudo-AP in the IEEE 802.11 ad hoc network. However, to realize a wireless sensor network based on the IEEE 802.11 ad hoc network, we should extend the service area of the IEEE ad hoc network by appointing multiple new pseudo-APs in the network. Based on the collected connectivity information of the network, the pseudo-AP can appoint sensors, which are located at the boundary of the service area of the network and have possibly smaller degrees D_{k}'s of the connectivity, as new additional pseudo-AP's.

Receiving beacon frames transmitted from multiple sensors that are or are not pseudo-APs, new sensors can join the IEEE 802.11 ad hoc network after the authentication process with any of those sensors. Each sensor i in the network should report the changes of S_i to all the pseudo-APs with which sensor i is wirelessly connected (that is, sensor i can hear the transmission signal of the pseudo-APs and vice versa) using the DCF transmissions of null or data frames, on which the changes of S_i are piggybacked. Each pseudo-AP should regularly broadcast the updated connectivity information of the network using the next beacon frames, on which the connectivity information is piggybacked. Detecting the changes of the connectivity information of the network from the beacons frames received from pseudo-APs, each sensor that is not a pseudo-AP piggybacks the changes of the connectivity information of the network on the next three beacon frames broadcast from itself.

When a pseudo-AP indirectly detects the changes of the connectivity information as the result of other pseudo-APs broadcasting of the connectivity information and other sensors reporting and broadcasting of the changes of the connectivity information, the pseudo-AP should construct the updated connectivity information of the network, and regularly piggyback it on the next beacon frames. By the process of the reporting and broadcasting of the connectivity information, all sensors can have the full knowledge of the connectivity information of the IEEE 802.11 ad hoc network. Using the connectivity information of the IEEE 802.11 ad hoc network, each sensor can obtain the shortest path to any sensor of the network by the Dijkstra's algorithm.

In the case of multiple pseudo-APs, whether sensor i is a pseudo-AP or not should be included in beacon frames broadcast from sensor i. Hearing beacon frames broadcast from sensors, each sensor i maintains the set T_i of the MAC addresses of pseudo-APs in the network. Similarly to the maintenance of S_is, the changes of Tis should be propagated throughout the network by the reporting and broadcasting of sensors and pseudo-APs so that each sensor can know the MAC addresses of all pseudo-APs in the network.

Each pseudo-AP can appoint new additional pseudo-APs, and sensor j that is currently a pseudo-AP can be released from the job of pseudo-AP when it finds the set S_j to be covered by the union of the sets S_is of other pseudo-APs. In relation to the changes of pseudo-APs, we can apply the following rules:

Replacement:

When a pseudo-AP finds another sensor i, which is not a pseudo-AP and is wirelessly connected with the pseudo-AP, to have the set S_i that includes more than all the MAC addresses of the sensors with which the pseudo-AP is wirelessly connected, sensor i can be appointed as the

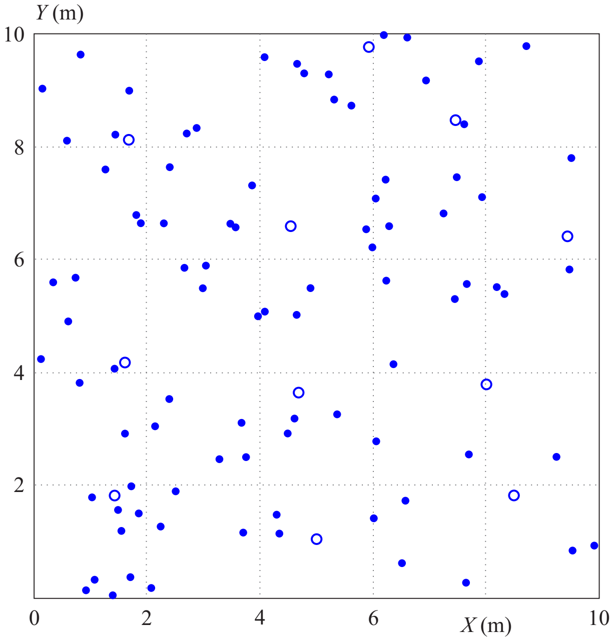

Fig. 1. Example of sensor deployment in square service area

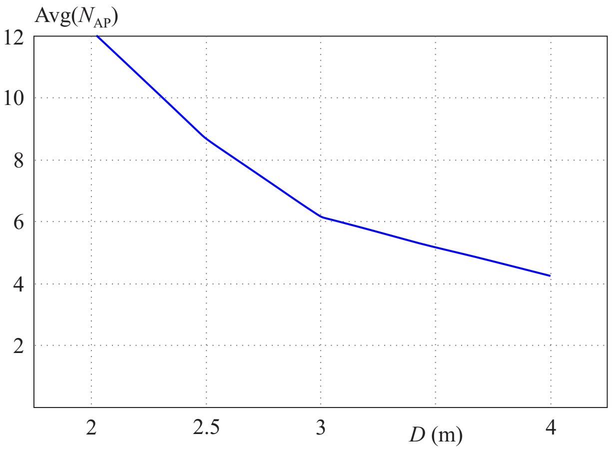

Fig. 2. Numerical results of average number of pseudo-APs versus transmission range

new pseudo-AP, and the old pseudo-AP can be released from the job of pseudo-AP. This replacement can be done by the old pseudo-APs transmitting a management frame to the new pseudo-AP using the DCF protocol.

New Appointment:

When a pseudo-AP finds the set S_j of sensor j, which is not a pseudo-AP and is wirelessly connected with the pseudo-AP, not to be covered by the union of the sets S_i's of the existing pseudo-APs, sensor j can be appointed as the new additional pseudo-AP, and the old pseudo-AP remains a pseudo-AP. This new appointment can be also done by the old pseudo-AP's transmitting a management frame to the new pseudo-AP using the DCF protocol.

Deletion:

When sensor j that is currently a pseudo-AP finds the set S_j to be covered by the union of the sets S_is of the existing pseudo-APs, sensor j can be released from the job of pseudo-AP. This deletion can be done by sensor j's transmitting a management frame to each pseudo-AP with which sensor j is wirelessly connected using the DCF protocol.

3 Simulation results

To propagate the connectivity information throughout wireless sensor networks, most of the overhead traffic caused by the MAC routing protocol proposed in the previous section is transmitted by pseudo-APs, which broadcast beacon frames, on which the connectivity information is piggybacked. The less the number of pseudo-APs is, the less the overhead traffic becomes. In this section, by simulation results we study the average number of pseudo-APs that are generated by the proposed MAC routing protocol to examine the efficiency of the protocol with respect of the overhead traffic. Let us assume that over the service area of a square with side of 10 meters one hundred sensors are sequentially deployed at random locations. Each sensor is assumed to have the same transmission range D. An example of such a deployment of sensors is shown in Fig. 1.

As one hundred sensors are sequentially deployed, the protocol in the previous section is applied to construct a wireless sensor network so that pseudo-APs are appropriately appointed to cover all sensors and the connectivity information can be propagated throughout the network. Except the first sensor deployed all sensors are assumed to continuously attempt to hear beacon frames from the wireless sensor network in construction to join the network. When new deployed sensors can hear beacon frames from existing sensors of the network in construction, new sensors join the network and the connectivity information between existing sensors of the network in construction and new sensors are propagated through pseudo-APs to all sensors in the network according to the protocol in the previous section. In Fig. 1, when the transmission rage D is 2 meters, eleven pseudo-APs were obtained by the protocol in the previous section and are represented by large circles.

From the numerical simulation experiments of ten networks for each case of the transmission range D of 2 meters, 2.5 meters, 3 meters, 3.5 meter and 4 meters, we obtained the average number $Avg(N_{\mathrm{AP}})$ of pseudo-APs generated by the proposed protocol for each case of the transmission range D as shown in Fig. 2. From Fig. 2, we can see that as the transmission range D becomes larger, the number of pseudo-APs becomes smaller. This is because with the larger transmission range D, each pseudo-AP can cover more sensors in wireless sensor networks.

For the transmission range D, the lower bound of the minimal number of pseudo-APs necessary to cover the service area of a square with side of 10 meters can be obtained as

$$\left\lceil \frac{100}{\pi D^2} \right\rceil$$

where $\lceil x \rceil$ is the smallest integer that is greater than x or equal to x. Using this formula, we can obtain the lower bounds of the minimal number of pseudo-APs as 8, 6, 4, 3 and 2 for the transmission range D of 2 meters, 2.5 meters, 3 meters, 3.5 meter and 4 meters, respectively. The gaps between the lower bounds of the minimal number of pseudo-APs and the average number $Avg(N_{\mathrm{AP}})$ of pseudo-APs generated by the proposed protocol are 4.2, 2.7, 2.2, 2.2 and 2.3 for the transmission range D of 2 meters, 2.5 meters, 3 meters, 3.5 meter and 4 meters, respectively.

4 Conclusions

We proposed a novel MAC routing protocol to realize wireless sensor networks based on IEEE 802.11 ad hoc networks. For MAC routing protocol, the connectivity information of wireless sensor networks should be propagated to all sensors through pseudo-APs. To reduce the number of necessary pseudo-APs, the rules for replacing existing pseudo-APs, appointing new pseudo-APs and deleting existing pseudo-APs were explained. By numerical examples, we studied the efficiency of the proposed MAC routing protocol with respect of the average number of pseudo-APs necessary for the proposed MAC routing protocol, which is closely related with the amount of the overhead traffic. Future research can be focused on the development of a distributed algorithm for optimal number of pseudo-APs that cover the service area of wireless sensor networks.

Acknowledgements

This work was supported by the Dong-A University research fund.

References

[1] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz", *IEEE Std 802.11ac*, IEEE Press, 2013.

[2] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Television White Spaces (TVWS) Operation", *IEEE Std 802.11af*, IEEE Press, 2014.

[3] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation", *IEEE Std 802.11ah*, IEEE Press, 2017.

[4] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 10: Mesh Networking", *IEEE Std 802.11s*, IEEE Press, 2011.

[5] T. Thaker, "ESP8266 based Implementation of Wireless Sensor Network with Linux based Web-Server", *Proc. of Symposium on Colossal Data Analysis and Networking*, 2016.

[6] G. R. Mendez, M. A. M. Yunus, and S. C. Mukhopadhyay, "A WiFi based Smart Wireless Sensor Network for an Agricultural Environment", *Proc. International Conference on Sensing Technology*, 2011.

[7] M. E. Bayrakdar, "Priority based Health Data Monitoring with IEEE 802.11af Technology in Wireless Medical Sensor Networks", *Medical & Biological Engineering & Computing,*, vol. 57, pp. 2757–2769, 2019.

[8] W.-Y. Choi, "Energy-Efficient MAC Protocol for Wireless LANs with WiFi Sensors", *Journal of Electrical Engineering,*, vol. 72, pp. 352–355, 2021.

[9] *IEEE Wireless LAN Edition*, IEEE Press, 2003.

[10] W.-Y. Choi, "Extending Service Area of IEEE 802.11 Ad Hoc Networks", *Frequenz*, vol. 66, pp. 215-220, 2012.

Woo-Yong Choi was born in Busan, Korea 1970. He received the BS, MS and PhD degrees in industrial engineering from POSTECH in 1992, 1994 and 1997, respectively. From 1997 to 2001 he was a senior member of technical staff at Hyundai Electronics Industries Co., Ltd. From 2001 to 2005 he was a senior member of technical staff at ETRI. Since 2005 he has been with Department of Industrial & Management Systems Engineering at Dong-A University, where he is currently a full tenured professor.

Received 30 September 2022