# Short Paper: Wireless Sensor Network Management for Sustainable Internet of Things

Jaewoo Kim, Seok Yu, and Jaiyong Lee
Department of Electrical and Electronics Engineering
Yonsei University
Seoul, Korea
kimjw064@yonsei.ac.kr, PowerfulRS@gmail.com, jyl@yonsei.ac.kr

***Abstract*— Conventional network management was based on wired network, which is unsuitable for resource constrained devices. WSNs consist Internet of Things (IoT) can be large scale networks, and it is impossible to manage each node individually. In this paper, we propose a network management protocol for WSNs to reduce management traffic.**

***Keywords—Internet of Things (IoT); Wireless sensor networks (WSNs); Management architecture; Management Information Base (MIB); Management protocol***

## I. INTRODUCTION

Recent advances of wireless communication and ubiquitous computing technology, the world's people could connect to the Internet at anytime and from anywhere. Moreover, by embedding mobile transceiver into the everyday things and devices, the world's things could be connected each other. IoT devices and things monitor certain events with sensors and the captured events are relayed through wired or wireless networks to servers or users, which extract and process the information gathered and automatically control and instruct other machines.

Fig. 1 represents the IoT service architecture. There are various issues at each domain for IoT services [2]. We concentrate on the network management and sustainability issues of IoT. Since WSNs can be deployed in or at harsh environment and resources are scarce, unexpected problems such as fault node or energy depletion can cause malfunction of network. Therefore, through network management, it is necessary to monitor the state and operation of WSNs. Also, in the face of unexpected events, WSN applications and network parameters will need to reconfigure and adapt themselves based on the information of the network [4].

In this paper, we propose a WSN management protocol for IoT to exchange the MIB while reduce the management traffic. We adapted the cluster-based management architecture and MIB of [3]. Sink node acts as a gateway between WSN and Internet. It interworks with IoT platform and also sends management policies to all cluster head (CH) nodes. There are some cluster head (CH) with more powerful capability than sensor nodes. Sink node (manager) and CHs communicates with existing SNMP. We define management protocol for communication among the CH and sensor nodes.

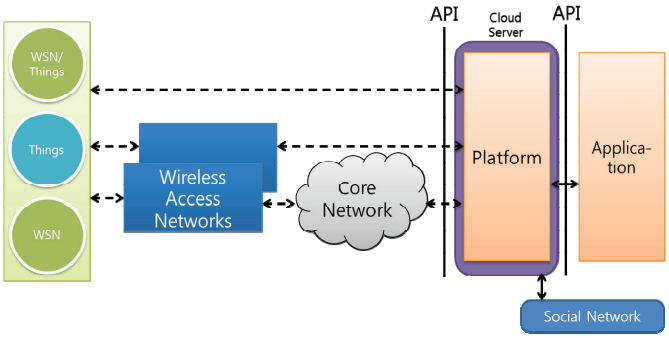


Fig. 1. IoT Service Architecture

## II. IOT-M

In WSNs, since the network status such as battery depletions or faults changes dynamically, it is necessary to get the information periodically. In SNMP, the manager has to send request to get some information from agents. However, in WSNs, resources are scarce and such polling mechanism causes huge traffic because of the large number of nodes and multi hop communication. To solve this problem, we define management protocol for WSNs with the purpose of reducing the management overhead.

*1) Message Types:* We define 4 message types as in Fig. 2: GET, SET, REP, TRAP which is similar to SNMP. But the usage is different. CH uses GET/SET messages when the cluster requests or set some management information. Sensor nodes use the REP message for the response of GET or SET message. Sensor nodes also generates periodical/eventual TRAP message to send its dynamic MIB by defining the data generation conditions. Polling requires two times of data transmission. However, TRAP requires only one-way data transmission to get MIB. Therefore, in order to monitor the status of the network, we use periodic or event-driven TRAP given by sensor nodes.


Fig. 2. 4 message types between CHs and nodes

978-1-4799-3459-1/14/$31.00 ©2014 IEEE

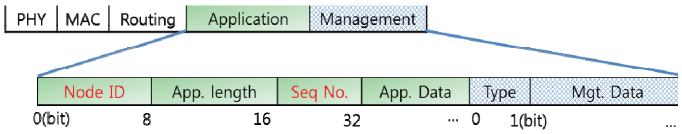


Fig. 3. Message format

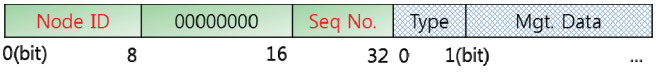


Fig. 4. Message format of non-piggyback case

*2) Message Format:* In order to reduce overhead of management message, we designed by combing the management protocol with application message. The messages are sent and received as the payload of existing PHY, MAC, and Routing protocols. Fig. 3 represents the message format of the proposed protocol. "Node ID" and "Seq. No." field are shared by application and management to reduce the message length. Each field of the message format is described below:

- Node ID: Node ID indicates the receiving node ID of this message.
- App. length: App. length indicates the length of the application data field. This field indicates the receiving node where application data is end and management message is start from in this packet.
- Seq No.: Using the sequence number field, the manager and nodes can distinguish different messages.
- App. data: This field contains sensor application data.
- Type: Type field indicates that this is which kind of messages by using only 1 bit. In case of the CH sends a message, "0" means that this is a GET message, and "1" means that this is a SET message. In case of a node sends a message, "0" means that this is a REP message, and "1" means that this is a TRAP message.
- Mgt. Data: Management data contains some of management data of MIB.

There are two cases sending the message: piggyback case and non-piggyback case. In piggyback case, nodes send their sensing application and management data together when sending REP or periodic TRAP messages. In non-piggyback case, nodes or CH sends the management data without application data when GET and SET sent from the CH or event-driven TRAP from the nodes. In this case, App. length field is set the value to 0 as in Fig. 4.

## III. Operation Sceanario

Fig. 5 shows the flow of an operation scenario example. SNMP is used between the sink and CHs, and IoT-M is used between CHs and member nodes. At the network initialization phase, static information is collected to the sink node using GET/REP messages, and configurable information such as report period is configured using SET/REP messages. Afterwards, most of the information needed to manage WSN is dynamic information. In case of time-driven information and event-driven information, instead of using periodic GET/

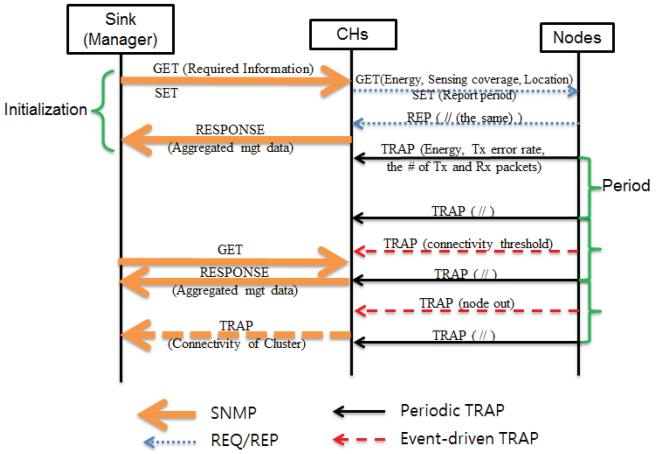


Fig. 5. An example of operation scenario of proposed framework

REP messages, TRAP messages are generated from a node periodically or when an event occurs and sent to the CHs. For critical information, if the value is lower than the predefined threshold, node generates TRAP message and sends it to the CHs. Collected MIBs in CHs are aggregated and sent to the sink node. For all kinds of MIB, GET and REP message can be used. However, due to its inefficiency, it is used only in special cases such as the manager wants.

Due to the only one-way data transmission to get dynamic MIB, the management traffic can be reduced by approximately half compared with existing polling approaches.

## IV. Conclusion

We proposed a network management protocol for WSNs. Using the simple message format and TRAP message the management overhead can be reduced. In the future work, we consider the management of the mobile sink application which one or more mobile node collect the information of the network. Also, it is needed to articulate the MIBs according to the various applications.

## Acknowledgment

This research was funded by the MSIP(Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013

## References

[1] ETSI TS 102 689, "Machine-to-Machine communications (M2M); M2M service requirements", Aug. 2010.

[2] J. Kim, J. Lee, J. Kim, J. Yun, M2M Service Platforms: Survey, Issues, and Enabling Technologies, *IEEE Communications Surveys and Tutorials*, in press.

[3] J. Kim, H. Jeon and J. Lee, "Network management framework and lifetime evaluation method for wireless sensor networks," *Integrated Computer-Aided Engineering*, vol. 19 no.2, pp. 165-178, April 2012

[4] L. B. Ruiz, J. M. Nogueira, and A. A. F. Loureiro, "MANNA: A Management Architecture for Wireless Sensor Networks," *IEEE communications Magazine*, vol. 41, no. 2, pp. 116-125, 2003.

[5] A. Jacquot, J. Chanet, Kun Mean Hou; G. De Sousa, A. Monier, "A new management method for wireless sensor networks," *Ad Hoc Networking Workshop (Med-Hoc-Net), 2010 The 9th IFIP Annual Mediterranean*, vol., no., pp.1,8, 23-25 June 2010