A novel method of IoT wireless sensor nodes management based on OID technology

Junhua Chen, Pengfei Shangguan, Xia Zhang*

Key Laboratory of Industrial Internet of Things & Networked control Ministry of Education, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China

*Corresponding author's email:sgpf1234@163.com

Abstract. With the continuous development of Internet of Things (IoT) technologies, massive wireless sensor nodes are deployed to construct several local wireless sensor networks over the world, which bring a great challenge to enormous wireless sensor nodes management. In this paper, a mechanism of sensor node managed object identifier (OID) is designed to merge classic SNMP MIB managed object identifier with sensor node identifier. Then, the framework of classic SNMP manager and agent is modified and optimised. Finally, a method for sensor nodes remote managing, which adapts to heterogeneous IoT network such as Internet linked with industry wireless network etc., is proposed to achieve hierarchical addressing and unified management of massive sensor nodes. The experimental result demonstrates that the proposed method satisfies the unified managing demand of a tremendous amount of sensor nodes in large-scale IoT network scenario by configuring and controlling sensor nodes.

1. Introduction

The wireless sensor node is an important part of the Internet of Things (IoT) application in the sensing layer, and it is the basic device for IoT applications and deployment. With the rapid development of wireless communication technology and sensor technology, a large number of wireless sensor nodes are deployed in Wireless Sensor Network (WSN). This makes the WSN present the characteristics of a large number of nodes and strong dynamics, which brings difficult management problems to sensor node administrators [1].

IoT identifier technology is a prerequisite for managing large-scale IoT applications and services, and is a key technology in the development of the IoT. At present, all walks of life at home and abroad are carrying out the research work of IoT identifiers and management [2-3]. China's national Standardization Administration has formulated a number of sensor network identifier standards [8]. However, the research on sensor node identifiers and management methods for sensor networks is still in the initial stage.

At the same time, the IETF released IPv6 based low power wireless personal area network standard 6LoWPAN, enabling WSN to connect seamlessly to the Internet [1]. The release of the standard to meet the needs of the IoT sensor nodes to access the IP network, but also the large-scale deployment of IoT sensor nodes possible. Therefore, the study of IPv6 based IoT sensor node management method has become an inevitable trend.

Aiming at this research demand, this paper designs a wireless sensor node management method based on object identifier (OID) technology. This method enables the administrator of the sensor node to input

the OID of the managed object of the sensor node in the client, thereby enabling information interaction with the target sensor node and effective management of the remote sensor node.

2. Architecture of wireless sensor node management base on OID technology

The wireless sensor node management architecture is shown in figure 1. The architecture comprises a manager of the wireless sensor node, node management server, sensor network gateway, and sensor node. The node management server communicates with the gateway using standard SNMP, and the gateway uses the Subagent Protocol to communicate with the sensor nodes.

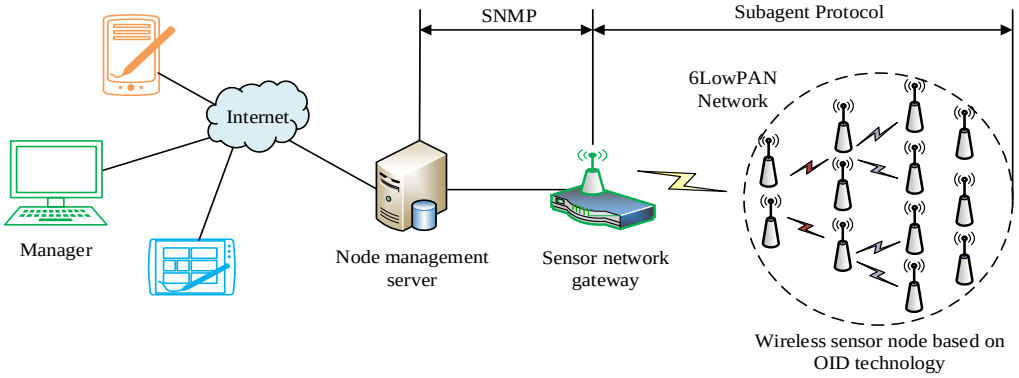

Figure 1. Architecture of wireless sensor node management base on OID technology

In figure 1, the sensor network is a 6Lowpan network. When the sensor node enters the network of the first time, it actively sends the identity identifier of sensor node (ISN) that has been written into the sensor node management information base (MIB) to the sensor network gateway. The sensor network gateway establishes a mapping relationship between the identity identifier of the sensor node and the IP address of the sensor node. At the same time, the sensor network gateway sends the identity identifier of the sensor node to the node management server. After the node management server receives the identity identifier of the sensor node sent by the sensor network gateway, the mapping relationship between the identity identifier of the sensor node and the IP address of the gateway is established. Through this mapping relationship, the manager of WSN only needs to know the identity identifier of sensor node to interact with the target sensor node.

The method can effectively solve the problem that the sensor node cannot be effectively managed when the IP address of the sensor node is unknown in the dynamically changing WSN [4-7]. At the same time, this approach enables a network architecture that integrates form the Internet to WSN and manages remote sensor nodes.

3. Function entity of wireless sensor node management based on OID technology

The function entity design of wireless sensor node management based on OID technology is shown in figure 2.

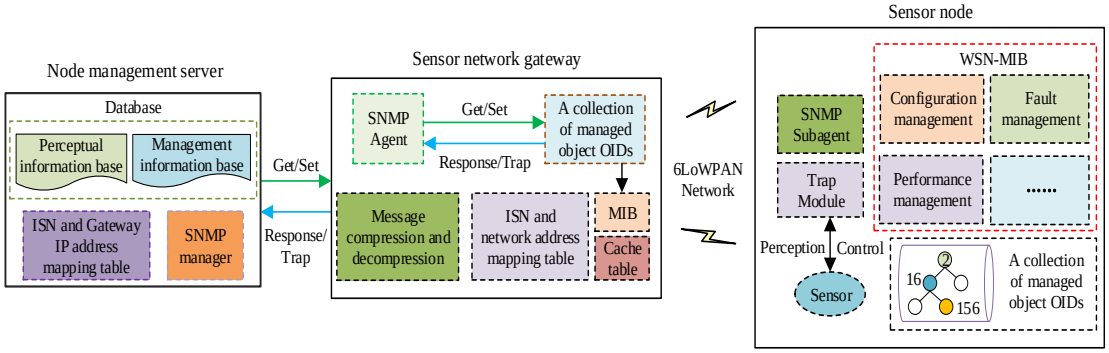

Figure 2. Function entity of wireless sensor node management based on OID technology

In this design, the node management server is responsible for responding to the user's management request for the sensor node, maintaining the perceptual information base and the management information base, establishing the identity identifier of sensor node and gateway IP address mapping table, and hosting the SNMP manager entity.

The sensor network gateway is responsible for hosting the SNMP agent entity, establishing and maintaining a mapping table of the identity identifier of the sensor node and its IP address, and completing the compression and decompression of the SNMP protocol message. In addition, a cache table is designed in the gateway, which is responsible for temporarily storing the perceptual information and management information of the node, so that the administrator can directly access the information that has not expired. This design can effectively reduce the traffic in the network.

The Subagents of SNMP and the managed objects of the sensor nodes reside in the sensor nodes. In addition, the Trap mechanism in the sensor node periodically sends the sensing data and the management information to the gateway, and the auxiliary gateway establishes a cache table. At the same time, the MIB in the sensor node is designed to meet the requirements of the management of the IoT sensor node and the resource nodes with limited resources.

3.1. OID design of managed object for sensor node

In the standard SNMP, the MIB is a collection of managed objects, and each managed object is uniquely identified by an OID. These OIDs are related to each other and form a tree-like hierarchical structure, the encoding rules for OID follow standards promulgated by the International Organization for Standardization. However, the managed object in the SNMP is designed for the management requirements of Internet devices. Therefore, the OID needs to be redesigned for the management requirements of the IoT to identify the managed objects.

The China National Standardization Administration has developed a sensor node identifier coding rule. Therefore, the encoding rule can be merged with the OID encoding rules of the managed object in the standard SNMP. The encoding rules for the OID of the managed object applied to the IoT sensor node are shown in figure 3.

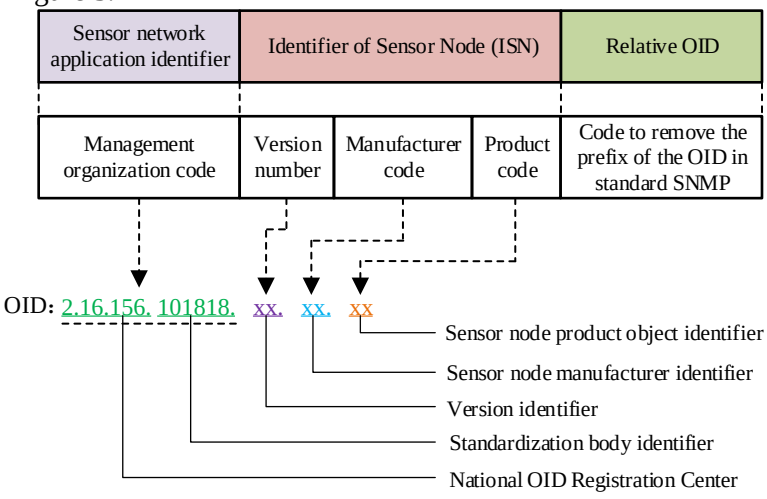

Figure 3. OID composition structure of the sensor node

The OID of the managed object of the sensor node is composed of three identifiers: Sensor Network Application Identifier + Identifier of Sensor Node+ Relative OID.

The sensor network application identifier is composed of the management organization code, which is used for the assignment and management of the sensor node identifier [8]. According to the Chinese National Standardization Standard, the code for this segment identifier is 2.15.156.101818.

The identifier of the sensor node is used to uniquely identify the sensor node in the global scope, and the encoding method is stipulated by the standardization organization of each country. The coding rules of the identifier of the sensor node can be queried for the sensor node identifier coding standard

formulated by the National Standardization Committee of China. According to this standard, the manufacturer of the sensor node assigns an identity identifier for the sensor node before the sensor node leaves the factory.

The relative OID is the code of an instance of a managed object in the sensor node, and its encoding rules can be combined with the encoding rules of the OID in the standard SNMP. The OID prefix of the managed object in standard SNMP is: iso(1).org(3).dod(6).internet(1), and the part after the prefix can be used as the encoding rules for the relative OID.

3.2. WSN-MIB design

In the SNMP protocol, the MIB is a collection of managed objects that defines a series of attributes of the managed object: the object name, the object access rights, and the data type of the object [4]. By reading or setting the value of the managed object instance in the MIB, you can get information about the IoT sensor node or control the running status of the sensor node.

The MIB in standard SNMP is applied to the collection and management of Internet device information, and cannot be applied to the management of information on the IoT sensor node devices. Therefore, it is necessary to redesign a lightweight MIB suitable for WSN sensor nodes in combination with the characteristics and requirements of the IoT sensor node device [4].

In this paper, the MIB of the sensor nodes of the WSN is classified into four categories: configuration information base, power information base, trap information base, and topology information base, as shown in figure 4.

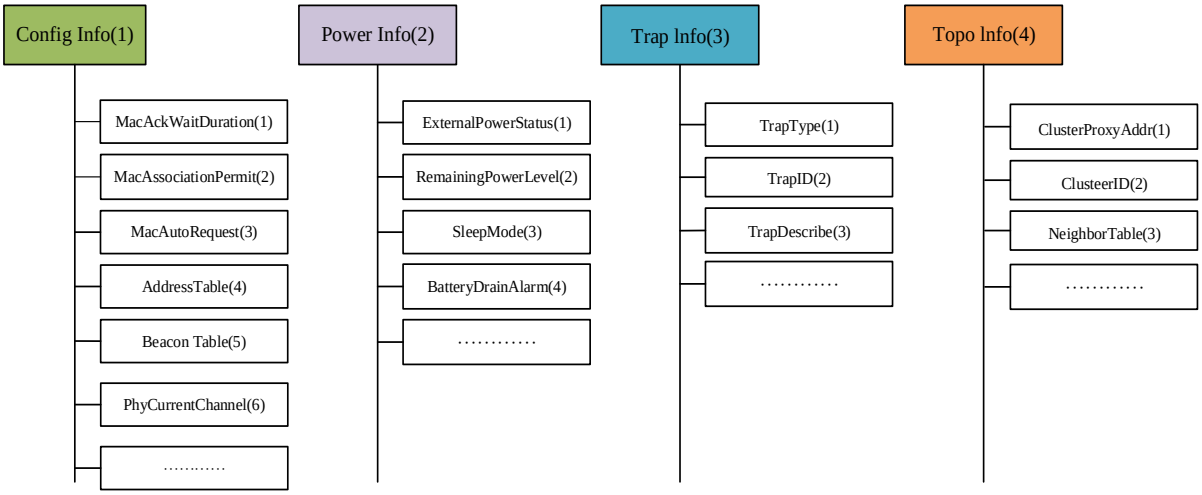

Figure 4. WSN-MIB

In the standard SNMP, the MIB uses a complex doubly linked list to store the OID of the managed object, dynamic memory allocation is required in the storage process. This method is not feasible in resource-constrained sensor nodes [5].

The MIB applied to the IoT can store it in an array when storing the OID. In addition, because the prefix content of the OID is the same, it needs to be stored only once.

This method makes it easy to find instances of managed objects and less memory usage [9-10].

At the same time, the method for storing the OID causes the SNMP packet received by the gateway to be in a non-standard format [11-12]. Therefore, when the gateway receives an SNMP packet or sends an SNMP packet, it needs to perform the corresponding conversion. If the gateway receives the SNMP packet sent by the node management server, the gateway deletes the OID prefix and sends the unprefixed SNMP packet to the corresponding sensor node. If the gateway receives the response or TRAP message sent by the sensor node, the gateway adds the prefix to the OID to form a standard SNMP message, and then sends the message to the node management server.

3.3. Mapping of identity identifiers of sensor nodes

In the management of IoT sensor nodes based on OID technology, the node management server needs to manage the identifier mapping relationship in all sensor networks within its region to ensure unique traceability to the sensor nodes [13-14]. The process of establishing a mapping relationship will be described in detail below.

When the sensor node first enters the network, the identity identifier that has been written into the sensor node MIB is actively reported to the sensor network gateway, and the gateway queries whether there is a corresponding mapping match. If there is no corresponding mapping match, the gateway establishes a mapping relationship between the ISN of the sensor node and its IP address. At the same time, the gateway sends the sensor node identity identifier to the node management server. If there is a corresponding mapping relationship, the gateway determines whether the mapping relationship between the stored identity identifier of the sensor node and its IP address is consistent with the network status of the current sensor node. If they are consistent, there is no need to change the mapping relationship stored in the gateway. If they are inconsistent, the mapping relationship corresponding to the identity identifier of the sensor node stored in the gateway needs to be updated.

After the node management server receives the identity identifier of the node uploaded by the gateway, it needs to query in the database of its own storage mapping relationship whether the mapping relationship corresponding to the node identity identifier already exists. If the mapping relationship does not exist, the mapping between the identity identifier of the node and the gateway IP address is established. If the mapping relationship exists, check whether the mapping relationship between the stored identifier of the node and the gateway IP address is consistent with the current network state. If the mapping relationship is inconsistent, the node management server needs to update the mapping relationship between the node's identity identifier and the gateway IP.

This mode is a layered addressing method. When the OID of the managed object is input on the client, the node management server finds the IP address of the gateway through the OID, and the gateway finds the IP address of the sensor node through the OID.

In addition, an interface can be invoked in the node management server to index the OID stored in the gateway. In this way, the node management service does not need to record each OID, thereby reducing the burden on the node management server.

The mapping process of the identity identifier of the node is as shown in Figure 5.

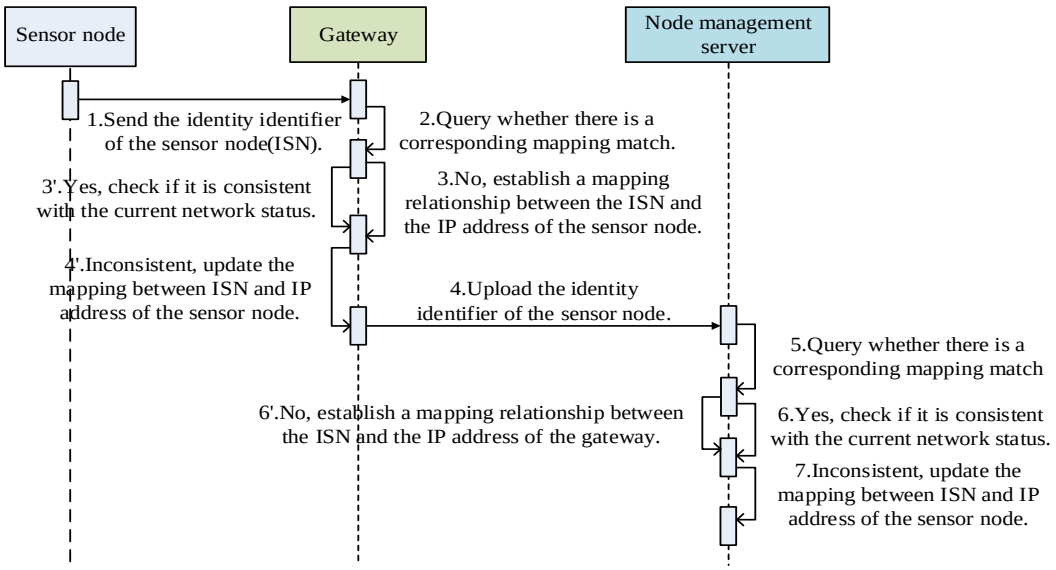

Figure 5. Mapping relationship established

4. Experimental

Through the establishment of the actual test environment, the wireless sensor node management of IoT based on OID technology method proposed in this paper is verified.

The sensor node in the WSN uses the STM32F103RB processor and the communication chip is the AT86RF212. The Contiki operating system is ported on the sensor node, and the Contiki operating system implements the complete 6LoWPAN protocol stack, the application layer of the protocol stack runs the SNMP. The sensor network gateway uses ARM9 chip S3C2440, equipped with Linux operating system, IPv4 and IPv6 protocol stack. The deployment of the test environment is shown in figure 6.

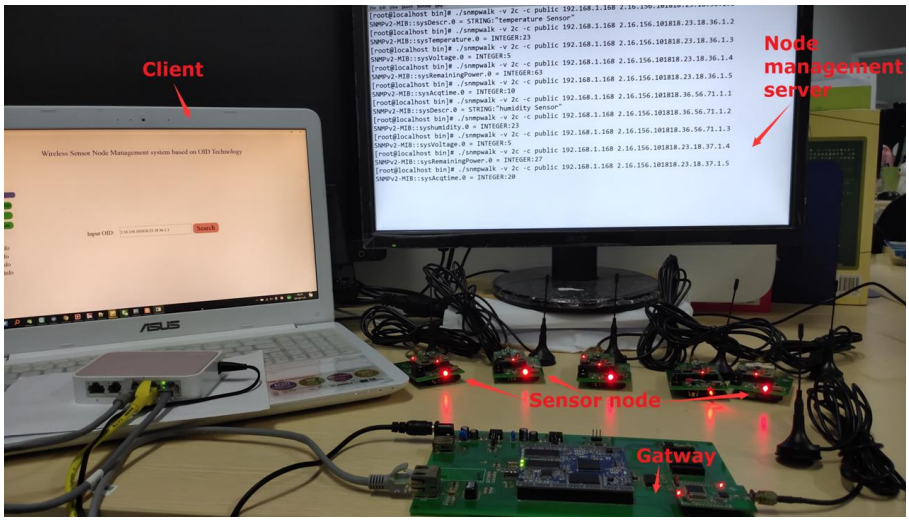

Figure 6. Snapshot of test environment deployment

The node management server uses the RedHat Linux platform, when the command is entered on the node management server to get the information of the sensor node, the printed information is shown in figure 7.

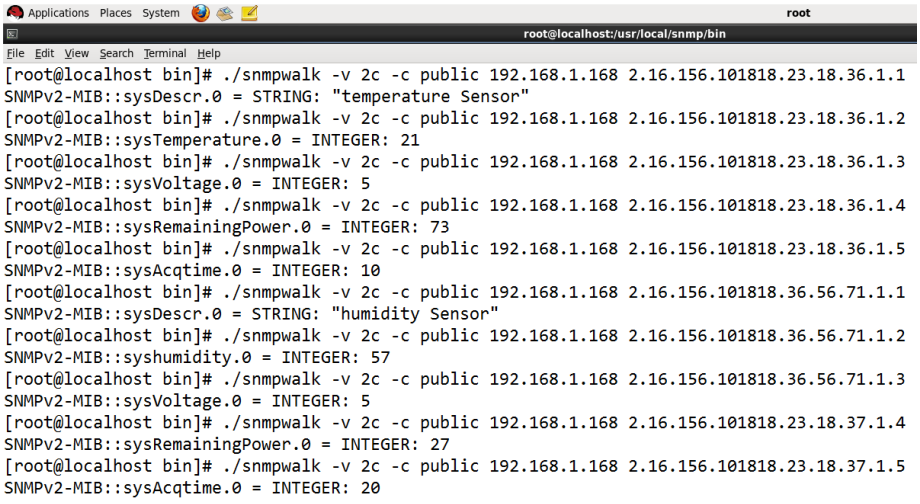

Figure 7. Snapshot of Node management server obtains sensor node information

In the picture, 192.168.1.68 is the IP address of the gateway, 2.16.156.101818 is the management organization code of the sensor node, 23.18.36 is the identity identifier of the node, and 1.1 is the relative OID.

5. Conclusion

The proposed wireless sensor node management base on OID technology method in this paper is feasible. The method is compatible with the existing Internet management protocol SNMP, and realize unified device management from the Internet to the wireless sensor network. More importantly, the method enables the sensor nodes to be efficiently managed in the dynamically changing sensor network by assigning identity identifiers to the sensor nodes and establishing mapping relationships. Finally, the method can provide advanced guiding significance for sensor node manufacturers and sensor node administrators, which can promote large-scale application of sensor networks and accelerate the construction of sensor network sensor node identification and management.

Acknowledgments

This work was supported by the National Key R&D Program of China (2017YFE0123000), Special key research and development projects for key technology innovations in key industries of China (No. cstc2018jszx-cyzdX0122), CERNET Innovation Project (NGII20170302).

References

[1] Lamaazi, H., Benamar, N., Jara, A.J. (2014) Challenges of the Internet of Things: IPv6 and Network Management. In: Eighth International Conference on Innovative Mobile & Internet Services in Ubiquitous Computing. Birmingham. pp. 328-333.

[2] Rodrigues, Joel J. P.C., Neves, Paulo A.C.S. (2010) A survey on IP-based wireless sensor network solutions. International Journal of Communication Systems, 23(8): 963-981.

[3] Jung, E., Choi, Y., Lee, J. S., & Kim, H.J. (2012) An OID-based identifier framework supporting the interoperability of heterogeneous identifiers. In: International Conference on Advanced Communication Technology. South Korea. pp.304-308.

[4] Chen, W., Zhou, Y., Wu, Y., Liao, X.F., &Ding, X.R. (2013) Wireless sensor network management based on SNMP protocol. Applied Mechanics and Materials, 303-306: 292-296.

[5] Ma, Y. W., Chen, J.L., Huang, Y.M., & Lee, M.Y. (2010) An Efficient Management System for Wireless Sensor Networks. Sensors, 10(12):11400-11413.

[6] Garcia, F. P., Andrade, R. M., Oliveira, C. T., & de Souza, J.N. (2014) An energy-efficient passive monitoring system for wireless sensor networks. Sensors, 14(6):10804-10828.

[7] Chaudhry, S.A., Boyle, G., Song W, et al. (2010) A Network Management Protocol for IP-based Wireless Sensor Networks. In: Communication in Wireless Environments and Ubiquitous Systems: New Challenges (ICWUS). Tunisia. pp.256-262.

[8] Xu, D.M., Xu, Q.P., & Dong, T. (2012) Sensor networks identification technology and standardization. information technology and standardization, 4:20-22;

[9] Zhang, W.B., Zhang, X.X., Tan, X.B., & Li-Dong, F.U. (2012) Network management method for WSN based on virtual OID computation. Computer Engineering, 38(6):83-85.

[10] Tadros, C.N., Mokhtar, B., Rizk, M.R.M. (2018) Software defined Network based management framework for wireless sensor networks. In: Electronics and Mobile Communication Conference. Canada. pp.1200-1205.

[11] Kim J., Jeon H., Lee J. (2012) Network management framework and lifetime evaluation method for wireless sensor networks. Integrated Computer-Aided Engineering, 19(2) :165-178.

[12] Paventhan A., Krishna S., Krishna H., Kesavan R., Ram N.M. (2013) WSN monitoring for agriculture: Comparing SNMP and emerging CoAP approaches. In: Texas Instruments India Educators' Conference. India. pp. 353-358.

[13] Tian, H. Q., Qin, Y. J., Tao, Z., & Gao, D. Y. (2010). Implementation of intelligent infrared control node in wireless sensor networks. Journal of Computer Applications, 30(9):2549-2552.

[14] Jacquot, A., Chanet, J. P., Hou, K. M., Diao, X., & Li, J. J. (2009). A new wireless management tool. Journal of the American Academy of Dermatology, 47(5):766-769.