사물 인터넷망에서의 보안 위협 기술 동향 분석

신윤구, 정승화, 도태훈, 김정태

목원대학교

Analyses of Trend of Threat of Security in Internet of Things

Yoon-gu Shin, Sungha Jung, Tahoon Do, Jung Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

Abstract

With the development of sensor, wireless mobile communication, embedded system and cloud computing, the technologies of Internet of Things have been widely used in logistics, Smart devices security, intelligent building and o on. Bridging between wireless sensor networks with traditional communication networks or Internet, IoT gateway plays n important role in IoT applications, which facilitates the integration of wireless sensor networks and mobile communication networks or Internet, and the management and control with wireless sensor networks. The IoT Gateway is a key component in IoT application systems but It has lot of security issues. We analyzed the trends of security and privacy matters.

Keyword

Security, IoT, Gateway, Privacy

Ⅰ. Introduction

Many implementations of Internet of Things (IoT) exist. Many works focuses on an architecture having a central unit (cloud server) running web applications for dual-way communications with both remote sensors and actuators. The sensor networks will be remote, running on mobile Internet connections that may have irregular drops in the Internet connection. A lot of researchers deal with low cost devices may be connected to and accessible from the Internet. The function can be sensor readings, sending control commands or receiving alarm messages. A Wireless Sensor Network (WSN) can be utilized for local applications so it may operate without a gateway. But for IoT usage there is a need of gateways [1]. As the Internet of Things is composed by RFID, WSN, Internet and other network, transmission of information security issues become more complicated .Using traditional security of a single network environment can't guarantee secure data transmission of IoT.

Ⅱ. Design considerations for IoT technologies

Information security, privacy and data protection should systematically be addressed at the design stage. Unfortunately, in many cases, they are added on later once the intended functionality is in place. This not only limits the effectiveness of the added-on information security and privacy measures, but also is less efficient in terms of the cost to implement them. Moreover, the IoT objects do not always have enough computing power to implement all the relevant security layers/functionalities; the heterogeneity of objects becomes very challenging in this context. Similarly, the heterogeneity of privacy policies needs to be taken into account.

Ⅲ. IoT Architecture

Many architectures for IoT look like that in Figure 1, where WSN is deployed in a different locations, running different applications. A gateway relays information from WSN into a cloud server where the user accesses the data from sensors or sends control commands to actuators [1].

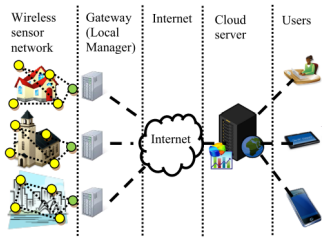

Fig 1. IoT Architecture

we consider the following features for the vision in IoT:

1. Four key technology areas provide the basis for IoT: pervasive identification and addressing, processing, networking and sensing
2. Communication will take place at an object to object and object to person basis
3. The amount of individuals' data collected and processed will increase substantially and will come from various different sources (object identifiers, sensor data etc.)
4. Most communications will occur automatically – objects will decide to exchange data with their environment, potentially without the user being aware of it
5. Objects are heterogeneous, providing different functionalities depending on the context of their applications. Based on the features identified above, we have identified some major challenges and issues with regard to privacy & data protection and information security. Regarding IoT-powered systems some gaps have still to be addressed, namely (i) device provision and activation and (ii) security. Device provision and activation is an important aspect of the device life cycle. While some devices might require a technician to be installed, many elements can be installed directly by the user. We are currently working on a method, depicted in figure 2, that involves a provision of chain, and it is simpler enough to be implemented in current commercial supply chains. Security will also play a major role in future IoT systems, and in particular in home and building automation networks. The security of actual systems is based more on a physical approach (i.e., protect the physical medium). Conversely, attacking an IEEE 802.15.4-based system is quite trivial. In order to build a secure system (to protect both users' privacy and security) an integrated approach is needed [2].

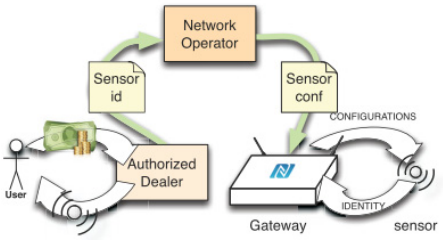

Fig 2. IoT Devices with Chain Connections

Ⅳ. Conclusion

The advances in the smart objects systems and, specifically, in the Internet of Things approach are remarkable. As a matter of fact, devices are nearly usable for commercial systems. However, to enhance the feasibility and overall sustainability of those remark systems, a standard gateway architecture is essential to apply IoT applications.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2010-0024133)

Reference

[1] Patrik Huss, Niklas Wigertz, Jingcheng Zhang, Allan Huynh, Qinzhong Ye and Shaofang Gong, "Flexible Architecture for Internet of Things Utilizing an Local Manager", International Journal of Future Generation Communication and Networking, Vol.7, No.1 ,2014, pp.235-248

[2] Romano Fantacci, Tommaso Pecorella, Roberto Viti and Camillo Carlini, "Short Paper: Overcoming IoT Fragmentation Through Standard Gateway Architecture", 2014 IEEE World Forum on Internet of Things (WF-IoT), pp.181-182