Volume 6, Issue 1, January 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Integration of Wireless Sensor Network (WSN) and Internet of Things (IOT), Investigation of Its Security Challenges and Risks

Hamed Sabbagh Gol*

Department of Computer Engineering, Payame Noor University (PNU),
Iran

Abstract— ***Internet of the future known as the "Internet of Things" (IOT) is a global web of things that are uniquely addressable based on standard protocols. In this internet each object is addressed using a unique URL address that is dynamically capable of connecting to network. These things can collaborate efficiently to perform various tasks. RFID tags, wireless sensors (WSN) and…. Can be used to design IOT. Since WSN plays an important role in collecting environmental information and concepts, integration of that with IOT can provide us with new perspectives. This study will provide different ways of integrating WSN and IOT. This integration leads to some challenges such as security, management, quality of service (QOS), protection of information privacy, and protection of privacy. In this paper different problems and challenges that arise from this integration will be discussed and a systematic security structure capable of reducing security risks, enhancing security and preventing penetration into the IOT and WSN integration will be proposed.***

Keywords— Internet of Things (IOT), wireless sensor networks (WSN), security, privacy, QOS.

I. INTRODUCTION

In the future Internet of Things (IOT), everyday objects that surround us become active players in the Internet, as well as information production and consumption. Elements of IOT include not only devices that have already rooted deeply in the technology world (such as cars or refrigerators), but foreign objects of this environment (clothing or perishable food), and even living organisms (farms, forests and livestock). With embedding computational capabilities into all types of objects and organisms, will allow for a qualitative and quantitative leap in the healthcare, services, entertainment and other areas.

Wireless sensor networks (WSN) is In fact one of the important elements in IOT. Connectivity advantages of WSN and other IOT elements, can cooperate and provide joint services as heterogeneous information systems. This integration is not a mere speculation, but is a reality developed by international companies. In addition, the data generated by the elements of a wireless sensor network (sensor nodes) may link to SOAP and REST-based Web services, the messaging mechanisms (e.g., e-mail SMS or social networks (like Twitter) and weblogs (e.g. Word Press) [2]

However, having IP connectivity does not mean that each sensor node should be directly connected to the Internet. There are many challenges, including security ones that must be carefully addressed in this regard.

II. THE MODEL OF REAL CONNECTION BETWEEN WSN AND THE INTERNET

While dealing with some of the most important integration security challenges,(integration of security and service mechanisms, protection of data privacy) in this study, we focus on a specific challenge: the model of real connection between WSN and the internet. Obviously, IOT is a concept that integrates the virtual world of information with the real world of objects. And the real world becomes more accessible through sensors, sensors embedded in devices, computers and small smart devices in business.

Wireless communication technologies and integrated network infrastructures include WSN, RFID systems, Auto mobile network, 3G technology, WiMax, personal area network (PAN), and…. and are rapidly expanding as a IOT network . The communications pivoting around this network have become more complex and security issues have become the more complex than all the systems in this network.

In the next parts of this paper, wireless sensor network will be introduced, and then the integrated approach and the various challenges we will be facing, are discussed.

III. WIRELESS SENSOR NETWORK

Recent developments in the field of smart sensors, wireless communications and digital electronics, have provided the ground for development of small, low power consumption and low cost sensor nodes which can also provide wireless connections. These small sensor nodes consist of three parts: sensor data processing and wireless data transferring. In general, a wireless network includes a large number of such nodes which are collectively used to measure a parameter and the data associated with that. This means that all the data collected for a node of the network, which is usually called the base station, is processed and the actual value of the parameter is estimated fairly accurately.in these networks, The failure of a network node usually has no impact on the estimated value.

In wireless sensor networks, large numbers of sensor nodes placed in the desired location or very close to it are intended to measure the parameters. The Place of these nodes has not been pre-designed. This fact helps to ease the placement of sensors on the network, however, the protocol that is used for these networks should be self-organized. Since these sensors are placed inside the CPU itself, to reduce the volume of the data which is transferred, the sensors only transfer the needed data after processing the original data.

IV. APPLICATIONS OF WIRELESS SENSOR NETWORKS

Sensor networks, include a variety of sensors such as seismic, motion, heat, gas, strain, optical, infrared, pressure, and sound sensors, which are capable of monitoring vast natural conditions such as temperature, humidity, mobility of vehicles, pressure, noise level in the environment, the presence or absence of a particular object in the environment, the mechanical pressure exerted on an object, common features such as speed, direction and size of the objects. Sensor nodes can be used for continuous environment sensing, event detection, local sensing and controlling of the stimuli. Four of the most important applications of these networks include: military applications, environmental applications, medical and health applications and industrial applications.

V. IMPORTANT FACTORS IN DESIGNING WIRELESS SENSOR NETWORKS

The design of a sensor network is influential by several parameters including: the fault tolerance, scalability, costs of production, working environment, sensor network topology, hardware limitations, transferring environment and energy consumption. These factors have been studied by many researchers.

However, none of these studies have comprehensively investigated all of the above factors in the network design. These factors are very important because they serve as the design policy of sensor network algorithms and protocols and can be used to compare different perspectives.

The following parameters are of great importance in designing efficient protocols for wireless sensor networks:

Fault tolerance, scalability (the ability to cover a large number of sensors) construction costs, hardware limitations, sensor network topology, environmental conditions, transferring environment and energy consumption.

VI. THE INTEGRATED APPROACH

From a network perspective, if we want to know whether a WSN should be fully integrated with the Internet or not, first of all we need to know what kind of integration methods can be used to connect these two infrastructures. The approach which is shown in Figure 1 can be classified in two different ways: stack-based approach [5], topology-based approach [6]. In the stack-based classification, the level of integration between the Internet and wireless network depends on the similarities between the stacks of their network. WSN can be completely independent of the Internet, capable of exchanging information with the Internet host (Gateway), or sharing TCP / IP protocols. On the other hand, in the topology-based classification, the level of integration depends on the actual location of nodes that provides access to the Internet.

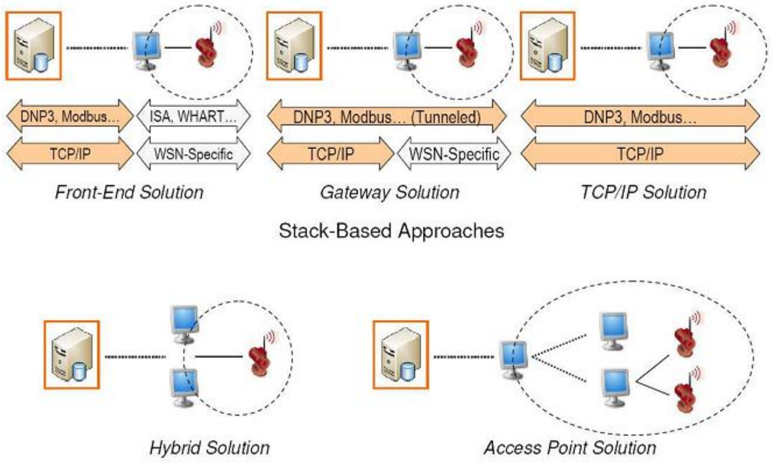

Fig. 1 The integration approach

The nodes can be dual sensor nodes (e.g., base stations) located in the root of WSN (hybrid), or be the backbone of the device that allows the Internet access sensor nodes come together in a hop (Access Point). In order to clarify the point, various methods are described in the following paragraphs.

In The stack-based classification, the first method is the Front-End solution. In this solution, the external Internet hosts and sensor nodes do not directly communicate with each other. In fact, WSN is completely independent from the Internet, thus, it can run its protocol sets (e.g. WirelessHART in the SCADA environments). All interactions between the outside world and sensor networks are managed by a centralized device, such as a base station. The base station can store all the data streams coming from WSN, and also can stream data to external parties via known interfaces (e.g. Web services [7]). In addition, any display of web host will always pass through the base station.

The Second method i.e. the Gateway solution, considers a device (e.g., base station) which acts as a gateway, and is responsible for the translation of the lower layer protocols of both networks (e.g. TCP / IP and proprietary) and routing information from one point to another. Therefore, the internet hosts and sensor nodes can be able to address each other and exchange data without establishing a really direct connection. In this solution, WSN is still independent from the Internet, and all the lines still need a gateway device to travel the path. However, sensor nodes can provide a web service interface to external entities, while maintaining their lower layer protocols.

As the TCP / IP, sensor nodes, stack TCP / IP (or compatible set of protocols such as 6LoWPAN the 802.15.4 network [1]) solutions are used for the third approach, therefore they can regarded as complete elements of the Internet. Each Internet host can open a direct connection with them, and vice versa. In fact, these solutions fully integrate the WSN with IOT. One of the consequences of this approach is that the sensor nodes are no longer able to use specific WSN protocols. According to the topology-based classification, the hybrid solution considers a set of nodes in a wireless sensor network, usually located at the edge of the network, which is able to access the Internet in a direct way. In fact, these nodes can be easily mapped to the base stations, because each sensor in the WSN needs to transfer them in order to connect to the central system, and vice versa. Redundancy and smart networks are Special features of this type of approach. By default, this approach suggests that more than one base station may be provided to access the network capabilities. Moreover, the base stations that can connect to the Internet, indicate that the network's smartness (e.g. running different sub-protocols) is dependent on a subset of WSN.

This integration of capabilities is mostly developed in the access point solution approach. Here, WSNs turns into an unbalanced trees with multiple roots, where leaves are the normal sensor nodes and all other elements of the tree are in form of nodes with access to the Internet. Thus, all the sensor nodes will be able to access the Internet just in one hop. One of the main features of this method is the possibility to increase the ability of nodes that belong to the backbone network. For example, the backbone nodes can have more resources than normal nodes, and can run network standards (e.g. 802.11 to 802.15.4) faster.

It is important to note that the network, based on the previously shown network topology, is generally combined with stack-based classification methods. For example, in a backbone network, nodes with access to the Internet can act as:

A) As a front-end, which effectively isolates the WSN sensor from the internet, or b) as Gateway, that allows for exchange of information between sensors and the central system. However, there is an exception here: the combination of TCP / IP solutions with hybrid and backbone solutions is basically irrelevant, and each node will be able to connect to the Internet. In fact, the nodes connected to the internet through local networks can only serve as a translator (e.g. between 6LoWPAN and IPv6).

VII. INTEGRATION CHALLENGES

In order to allow WSN to become a staple of IOT with a secure method, many security challenges must be considered. As mentioned earlier, we focus on network-level connectivity in this article. However, there are additional security challenges that even if they are not studied in this paper, should be addressed in the future.

These challenges are largely related to WSN, but can also be applicable to other technologies related to IOT. Security mechanisms and user acceptance are among the most important challenges of integration [3]. It is necessary to Considering IOT security from a global perspective, not as an isolated set of issues related to specific technologies. Otherwise, we may get to a point where technology (for example WSN) satisfies a minimum set of security requirements. But its integration with other technologies (such as RFID) generates new needs that have not been previously considered. From the user perspective, IOT should be able to meet their expectations without betraying their trust. Not only IOT should be useful, but users should understand that they control any information that are relevant to them. If users feel that they are controlled by the system, or they have a false sense of security because they have betrayed their own rights, they will directly reject any advantage that IOT can provide.

Protection of Data privacy should also be seriously taken into considerations. The Information related to a particular user not only includes his personal information, but also any data generated by objects around the individual (e.g. sensor nodes).

In this situation, it is necessary to clarify who owns the data, and how the user can be confident that the data is secure and cannot be used without his consent. In addition, there will be some cases in which part of the data should be shared in order to provide services. For example, in case of emergency, a person should clearly share their health information (i.e. personal information and allergy) with ambulances and medical staff. Beyond individual users, data privacy is also a concern for business scenarios. Any individual who uses the mechanisms provided by IOT, develops a large flow of data (such as the interaction of human resources, manufacturing processes). Such data should remain confidential only when needed, and be controlled and make available by the company.

VIII. SECURITY

Finally, protection of the IOT components using adequate security mechanisms is another important aspect that should be taken into considerations. This applies not only to the use of security protocols and mechanisms at the network level but also to the interaction between objects and services. IOT is a dynamic, heterogeneous and distributed infrastructure that should integrate several technologies, protocols and models to provide services through a convenient method. From a security perspective, objects and basic infrastructure must be able to withstand several identification and security mechanisms in a transparent and scalable way. However, some isolated cases (e.g. a digital home, the headquarters of a company) in which the interaction between objects is kept under control, may provide various services (such as logistics) where several elements are geographically distributed around the world. According to the above descriptions, reaching a point of balance in safe interactions between objects and services is one of the most interesting challenges in IOT [4]

IX. CONCLUSION

In this paper we proposed different ways of integrating WSN and IOT. This integration lead to some challenges such as security, management, quality of service (QOS), protection of information privacy, and protection of privacy. In this paper different problems and challenges that arise from this integration discussed and the results of this new security structure can reduce the newly developed security risks, enhance security and prevent penetrations into the IOT and WSN integrations.

ACKNOWLEDGEMENT

This research was supported by [PNU South Khorasan]. We thank our colleagues who provided insight and expertise that greatly assisted the research, although they may not agree with all of the conclusions of this paper.

REFERENCES

[1] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. 2007.

[2] Libelium: Interfacing the Sensor Networks with the Web 2.0, http://www.libelium.com/, Accessed on October 2010.

[3] C.P. Mayer. Security and Privacy Challenges in the Internet of Things. KiVS Workshop on Global Sensor Network, 2009.

[4] J. Claessens. Trust, Security, Privacy, and Identity perspective. Panel on Future Internet Service Offer, 2008.

[5] R. Roman, J. Lopez. Integrating Wireless Sensor Networks and the Internet: a Security Analysis. Internet Research, Vol. 19, no. 2, pp. 246-259, 2009.

[6] D. Christin, A. Reinhardt, P.S. Mogre, R. Steinmetz. Wireless Sensor Networks and the Internet of Things: Selected Challenges. 8th GI/ITG KuVS Fachgesprch “Drahtlose Sensornetze”, 2009.

[7] A. Kansal, S. Nath, J. Liu, F. Zhao. enseWeb: An Infrastructure for Shared Sensing. IEEE Multimedia, Vol. 14, no. 4, pp. 8-13, 2007.