ISBN:978-93-5254-640-4

Internet of Things, Technology and Challenges

Prof. Aparna Phatak

Pratibha College of Commerce and Computer Studies,

Chinchwad, Pune 411019.

gateaparna@gmail.com

Abstract: **Current world has become a global village. Advanced options and technological advancement in connectivity technology and connectivity devices are leading the world for communications on one click. Today, "Internet of Things" (IoT) is used as a catchphrase by many sources. This expression encompasses a galaxy of solutions somehow related to the world of intercommunicating and smart objects. The Internet of Things is, thus, the evolution of the Internet to cover the real-world, enabling many new services that will improve people's everyday lives, spawn new businesses and make buildings, cities and transport smarter. Smart things allow indeed for ubiquitous data collection or tracking, but these useful features are also examples of privacy threats that are already now limiting the success of the Internet of Things vision when not implemented correctly. These threats involve new challenges such as the pervasive privacy-aware management of personal data or methods to control or avoid ubiquitous tracking and profiling. This paper takes a complete review of Internet of things. Developments, Applications and Threats in Internet of things. It takes review of the security architectures for the threats and protocol suite for internet of things.**

Keywords- **network, internet of things, security, threats, challenges.**

I. INTRODUCTION

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure

Figure 1 explains the framework of Internet of Things service support system.

Meanwhile, a number of challenges are in the way of the IoT. In terms of scalability, IoT applications that require large numbers of devices are often difficult to implement because of the restrictions on memory, time, processing, and energy constraints. For example, calculation of daily temperature variations around all of the country may require millions of devices and result in unmanageable amount of data. And the deployed hardware in IoT often have different operating characteristics, such as sampling rates and error distributions, meanwhile sensors and actuators components of IoT are always very complex. All of these factors contribute to the formation of the heterogeneous network of IoT in which the data of IoT will be deep heterogeneous. Moreover, it is expensive to transmit huge volume of raw data in the complex and heterogeneous network, so IoT need data compression and data fusion to reduce the data volume. Consequently, standardization of data processing awareness for future IoT is highly desired. In addition, virus, malicious software and hackers in the communication process might disturb data and information integrity. With the development of IoT technology, information insecurity will directly threat the entire IoT system.

Applications of IoT can bring convenience to people, but if it cannot ensure the security of personal privacy, private information may be leaked at any time. So the security of IoT cannot be ignored. Once the signal of IoT is stolen or interrupted, it will directly affect the security of the entire information of IoT. With the widely spreading of IoT, it will provide more extensive wealthy of information, the risk of exposure of such information will increase. If IoT cannot have a good solution for security issues, it will largely restrict its development. Thus, above all the problems of IoT, security problem is particularly important.

Security threats for IOT can be summarised as follows:

1. Cloning of smart things by untrusted manufacturers;

2.Malicious substitution of smart things during installation;

3. Firmware Replacement Attack;

4. Extraction of security parameters since smart things may be physically unprotected;

5. Eavesdropping attack if the communication channel is not adequately protected;

6. Man-in-the-middle attack during key exchange;

7. Routing Attacks;

8. Denial-Of-Service Attacks;
9. Privacy Threats.

The paper discusses some architecture for security of internet of things. It discusses IP based IOT security and layer based security of IOT .

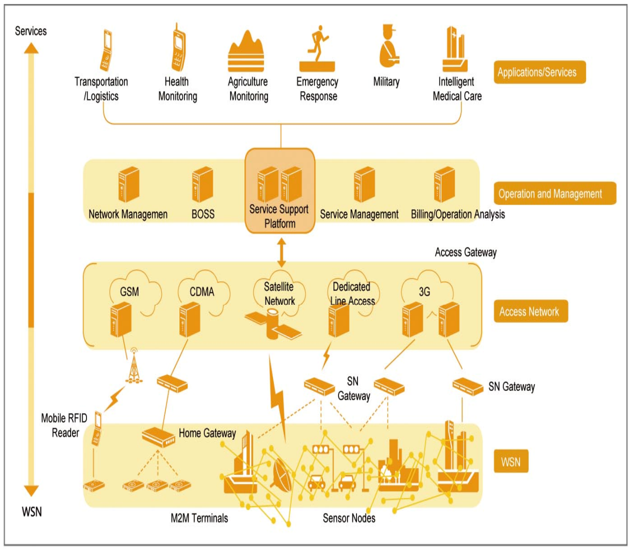

Figure 1. Framework of the Internet of Things service support system.

II. IP BASED SECURITY CHALLENGES

IP based security challenges mainly concerned with the devices i.e. the things' life cycle.

A. Thing life cycle

We consider the installation of a Building Automation Control (BAC) system to illustrate the lifecycle of a thing. A BAC system consists of a network of interconnected nodes that perform various functions in the domains of HVAC (Heating, Ventilating, and Air Conditioning), lighting, safety etc. The nodes vary in functionality and a majority of them represent resource constrained devices such as sensors and luminaries. Some devices may also be battery operated or battery-less nodes, demanding for a focus on low energy consumption and on sleeping devices. In our example, the life of a thing starts when it is manufactured. Due to the different application areas (i.e., HVAC, lighting, safety) nodes are tailored to a specific task. It is therefore unlikely that a single manufacturer creates all nodes in a building. Hence, interoperability as well as trust bootstrapping between nodes of deferent vendors is important. The thing is later installed and commissioned within a network by an installer during the bootstrapping phase. Specifically, the device identity and the secret keys used during normal operation are provided to the device during this phase. Deferent subcontractors may install different IoT devices for different purposes. Furthermore, the installation and bootstrapping procedures may not be a denned event but may stretch over an extended period of time. After being bootstrapped, the device and the system of things are in operational mode and run the functions of the BAC system. During this operational phase, the device is under the control of the system owner. For devices with lifetimes that span several years, occasional maintenance cycles may be required. During each maintenance phase, the software on the device can be upgraded or applications running on the device can be reconfigured. The maintenance tasks can thereby be performed either locally or from a backend system. Depending on the operational changes of the device, it may be required to re-bootstrap at the end of a maintenance cycle. The device continues to loop through the operational phase and the eventual maintenance phase until the device is decommissioned at the end of its lifecycle. However, the end-of-life of a device does not necessarily mean that it is defective but rather denotes a need to replace and upgrade the network to next-generation devices in order to provide additional functionality. Therefore the device can be removed and re-commissioned to be used in a di_erent network under a different owner by starting the lifecycle over again. Figure 1 shows the generic lifecycle of a thing. This generic lifecycle is also applicable for IoT scenarios other than BAC systems.

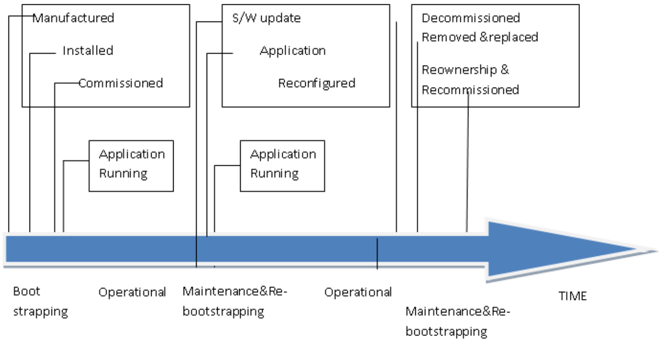

Figure 2: A Life Cycle Of A Device In The Internet Of Things

At present, BAC systems use legacy building control standards such as BAC- Net or DALI with independent networks for each subsystem (HVAC, light- ing, etc.). However, this separation of functionality adds further complexity and costs to the configuration and maintenance of the different networks within the same building. As a result, more recent building control networks employ IP- based standards allowing seamless control over the various nodes with a single management system. While allowing for easier integration, this shift towards IP-based standards results in new requirements regarding the implementation of IP security protocols on constrained devices and the bootstrapping of security keys for devices across multiple manufacturers.

B. Security Aspects

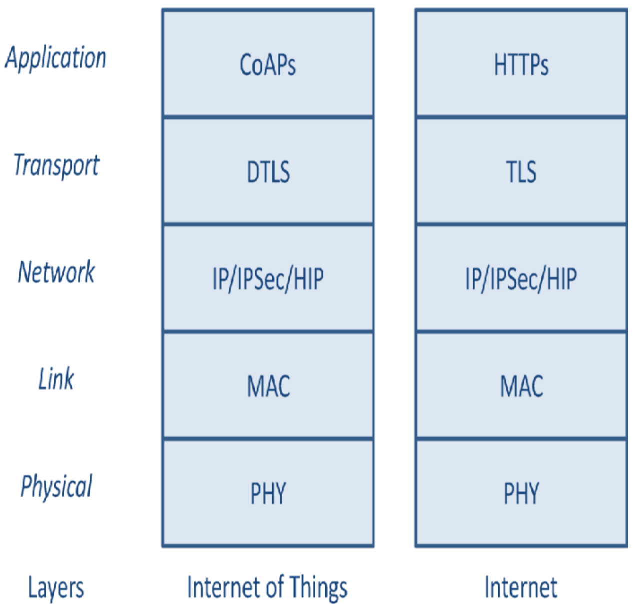

Figure 3: IP based security layers

Referring to the IoT protocol stack of Figure 3, at the application layer there is the CoAP application protocol that can be used to interact in a request/response manner between smart objects or between a smart object and a non-constrained (standard) Internet node (possibly by using some intermediate relay/proxy node). CoAP itself does not provide primitives for authentication and data protection, so these functions should be implemented directly at the application/service layer (by directly protecting the data encapsulated and exchanged by CoAP) or at one of the underlying layers. Although data authentication, integrity, and confidentiality can be provided at lower layers, such as PHY or MAC (e.g., in IEEE 802.15.4 systems), no end-to-end security can be guaranteed without a high level of trust on intermediate nodes. However, due to the highly dynamic nature of wireless multi-hop communications expected to be used to form the routing path between remote end nodes, this kind of security (hop-by-hop) is not, in general, sufficient. For such reason, security mechanisms at network, transport, or application level should be considered instead of (or in addition to) PHY and MAC level mechanisms.

It uses lightweight cryptography for smart objects. Together with security protocols, another important aspect related to security is the definition and implementation of cryptographic algorithms, tailored for constrained devices. Lightweight cryptographic algorithms have been overviewed and compared in order to highlight the main features of each and to isolate those that are more suitable for use in constrained environments. Key agreement protocols and group key distribution mechanisms for secure group communication have been discussed, since it may be particularly relevant in scenarios where several smart objects need to communicate and cooperate in order to perform some common task. Related to this aspect, secure data aggregation schemes through homomorphic encryption algorithms have been also discussed, as a possible solution to minimize the processing of smart objects and optimize data transmission.

III. CONCLUSION

Internet of things ,applications bring convenience to people for communications between things to people, things to thing. At the same time it is required to keep this communication secure, keeping private data of people safe. The same can be obtained by applying IP based security layers, a protocol suite for internet of things along with the cryptographic solutions.

REFERENCES

[1]. Tobias Heer, Oscar Garcia-Morchony,, Ren_e Hummen, Sye Loong Keohy, Sandeep S. Kumary, and Klaus Wehrle,, Springer Journal on Wireless Personal Communications

[2]. Simone Cirani , Gianluigi Ferrari and Luca Veltri, Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview,Algorithms,2013

[3]. John A. Stankovic, Research Directions for the Internet of Things, IEEE,2014.

[4]. Mike Turner, How to secure internet of things, ComputerWeekly.com