Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 1, January 2016, pg.133 – 139

Internet of Things and Security Issues

Suchitra.C[1], Vandana C.P[2]

[1]PG Scholar, Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India

[2]Assistant Professor, Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India

[1] suchitrac30@gmail.com; [2] vandana.hareesh@gmail.com

Abstract— Internet of Things (IoT) is a network of physical objects connected to internet. Physical objects embedded with RFID, sensor and so on which allows object to communicate with each other. The physical objects are provided with unique identifier. Since the IoT is highly heterogeneous, security is a big challenge in IoT. In this paper we analyzed the various security requirements and challenges in IoT and research objectives.

Keywords— Internet of Things IoI, RFID, WSN, DoS, security

I. INTRODUCTION

A. IoT

The Internet of Things (IoT) is a concept that describes a future where every day physical objects can be connected to the Internet and also be able to identify themselves to other devices [1]. IoT is closely identified with RFID, sensor technologies, wireless technologies. It allows objects to be sensed and controlled remotely across existing network infrastructure. Internet is a medium that connect people across the world for emailing, gaming, conferencing, online trading and so on [2]. IoT includes, for example, Cameras connected to internet that allow you to post pictures online with a single click, changing the lane while driving safely, switching off the lights automatically in a room when no one is around [2]. Internet of things can be able to transfer data over the network without human interaction.

B. THE CONCEPT OF IoT AND ITS BASIC CHARACTERSTICS

Internet of things is a collection of physical objects which is has ability to capture information for physical world. IoT is an intelligent system, which has computing and communicating ability. Internet of things has three basic characteristics such as [8]:

1) Comprehensive awareness: Comprehensive awareness is due to the sensors, RFID and M2M terminal. These are used to get information of the object.

2) Reliable transmission: The main aim of reliable transmission is high accuracy and real time.

3) Intelligent processing: The main aim of intelligent processing is to analyze and collect the useful information to meet the user expectation.

C. IoT ARCHITECTURE

The IoT can be capable of interconnecting various heterogeneous objects through the Internet, so there is a need for a flexible layered architecture. The figure 1 illustrates the 3-layer architecture of IoT.

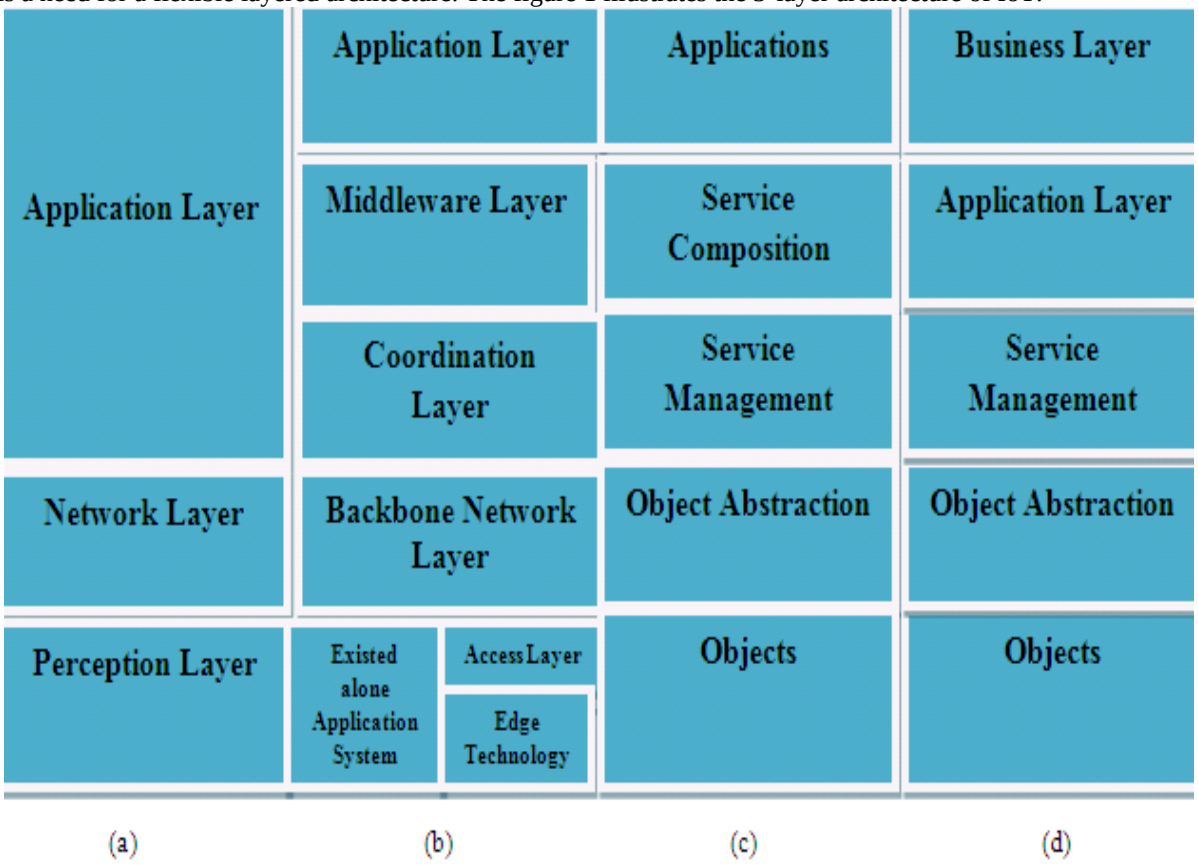

Figure 1: The IoT Architecture (a) Three Layer (b) Middle-ware based Layer (c) SOA based Layer (d) Five-layer

The basic model is a 3-layer architecture consisting of the Application, Network, and Perception Layers. In the recent literature abstraction is added to the IoT architecture [3].

1) Objects Layer

The first layer is objects or perception layer, it represents the sensors used in IoT that collect and process information. The perception layer includes sensors and actuators. The sensors and actuators perform different functionalities such as identifying temperature, motion, location, weight, humidity, vibration, acceleration etc. This layer digitizes and transfers data to the Object Abstraction layer. The perception layer transfers data through secure channels. The perception layer initiates the big data created by IoT. [3]

This layer gives a physical meaning to each object. Object layer consists of data sensors in the form of RFID tags, IR sensors or other sensor networks which can be able to sense the temperature, speed, humidity, location and so on. Object layer gathers the useful information of objects from the sensor devices which is connected to those objects and converts the information into digital signals. Then the digital signal is passed to network layer [4].The Perception layer is nothing but collection of sensor, actuators which forms WSN [6].

2) Object Abstraction Layer

The Object Abstraction layer transfers data to the Service Management layer produced by perception layer through secure channels. Data can be transferred through RFID, 3G, WiFi, GSM, ZigBee, Bluetooth etc. Cloud computing and data management processes are done by Object Abstraction Layer [3].

3) Service Management Layer

The next layer is Service Management or Middleware layer. This layer pairs a service with its requester based on addresses and names. Service Management layer processes the data received, makes decisions and delivers the services required. The Service Management layer also allows the IoT application programmers to work with heterogeneous objects without any consideration to a specific hardware platform [3].

Information received from the sensor devices is processed by Service Management Layer. The information is processed using some Intelligent Processing Equipment. Based on the processed results of the information fully automated action is taken [4].

4) Application Layer

This layer provides the services requested by customers. For example, it provides the temperature and air humidity measurements to customer. Application provides high quality smart services to meet customer needs [3].

Application layer is very helpful in the large scale development of IoT network. Application related to IoT could be smart homes, smart transportation, smart planet and son on [4]. It is a top most layer which consists of business logic, formulas and UI to user end [6].

5) Business Layer

This layer manages the overall IoT system services and activities. Business Layer builds a business model, graphs, flowcharts etc based on data received by Application Layer. The Business Layer also implements, design, monitor, analyze and develop the elements related to IoT. This layer supports decision making processes based on Big Data analysis. Business Layer also monitor and manages the underlying four layers. It also compares the output of each layer with expected output to enhance services [3]. For effective business strategies it generates different business models [4].

D. SECURITY ISSUES IN IoT

Internet is key infrastructure of IoT hence there is a possibility for some prominent security issues [5]. IoT is a collection of physical objects connected to internet; hence many security issues may occur. Some of the security issues are:

1) Security issues in perception layer:

It is a lowest level of IoT construction. Perception layer is the source of access to information throughout the IoT. The security issues in Perception layer include physical security of sensing devices and security of information collection. IoT cannot provide a security protection system and it is vulnerable to the attack due to diversity, energy limited, simple and weak protective capability of sensing node which affects the security of WSN, RFID and M2M terminal. The RFID includes security problems such as information leakage, replay attacks, information tracking, tampering, cloning attacks and man-in-the-middle attacks. The security problems faced in perception layer includes capture gateway node, physical capture, unfair attacks, congestion attack, DoS attacks, node replication attack and forward attack [8].

1.1) Security issues in the wireless sensor networks (WSNs):

WSN is a network of nodes that sense and control the environment. It also enables the interaction between persons or computers and the surrounding environment. WSN includes sensor nodes, actuator nodes and so on. WSN is a collection node hence there is a possibility of security issues.

The operations performed in a wireless sensor network can be categorized under three categories [5]:

i. Attacks on secrecy and authentication
ii. Silent attacks on service integrity
iii. Attacks on network availability

1.2) Security issues in RFID technology

In IoT, RFID technology is mainly used as RFID tags for automated exchange of information without any manual involvement. The RFID tags are vulnerable to various attacks from outside due to the incorrect security status of the RFID technology [5]. The four most common types of attacks and security issues of RFID tags are as follows:

i. Unauthorized tag disabling: In this DoS attacks the RFID tags will become incapable temporarily or permanently. Such attacks make RFID tag available to malfunction and misbehave under the scan of a tag

reader. These attacks can be done remotely, allowing the attacker to manipulate the tag behavior from a distance.

ii. Unauthorized tag cloning: Capturing the identification information through the manipulation of the tags by dishonest readers falls under this category. Once the identification information of a tag is compromised, replication of the tag is made possible which can be used to bypass fake security measures as well as introducing new vulnerabilities using RFID tags automatic verification steps [5].

iii. Unauthorized tag tracking: The dishonest readers can trace the tag, which results in giving the sensitive information, for example person's address. Thus from the viewpoint of customer, buying a product which is having an RFID tag guarantees them no confidentiality regarding the purchase of their chase and in fact endangers their privacy.

iv. Replay attacks: In Replay attacks the attacker uses a tag's response to a dishonest reader's challenge to impersonate the tag. In this attacks, the communicating signal between the reader and the tag is intercepted, recorded and replayed upon the receipt of any query from the reader at a later time, thus faking the availability of the tag

2) Security issues in physical layer:

The physical layer performs different functionalities such as selection and generation of carrier frequency, modulation and demodulation, encryption and decryption, transmission and reception of data [5]. This layer is attacked mainly through

i. Jamming: This DoS attack occupies the communication channel between the nodes and prevents them from communicating with each other. It exploit the transmission of radio signal to interfere with radio frequencies that used by sensor network. It can be performed either continuously or in an isolated way [7]. In both the cases network will suffer from damage.

ii. Node tampering: Extracting sensitive information is known as node tampering

3) Security issues in network layer:

Internet of things faces some risk in the network like illegal access, confidentiality, data eavesdropping, integrity, DoS attacks, destruction, virus attack, man-in-the-middle attack and so on. IoT sensing a large number of devices hence a variety of formats of the data collected, and the data information has a massive, multi-source and heterogeneous characteristics. It will also causes network security issues like data transfer needs of large number of nodes leading to network congestion, resulting in DoS attacks [8].
The function of the network layer is routing [5]. The DoS attacks taking place in the network layer:

i. Hello flood attack: Hello flood attack causes high traffic in channels by congesting the channel with an high number of useless messages unusually. Here a single malicious node sends a useless message then that message is replayed by the attacker to create a high traffic.

ii. Homing: In this attack, a search is made in the traffic for cluster heads and key managers which having the capability to shut down the entire network.

iii. Selective forwarding: In this, a compromised node sends few selective nodes instead of all the nodes. The selection of the nodes is based on the requirement of the attacker to achieve his malicious objective and thus such node does not forward packets of data.

iv. Sybil: In this attack, the attacker replicates a single node and then presents it with multiple identities to the other nodes.

v. Wormhole: Wormhole attack causes relocation of bits of data from its original position. The relocation of data packet is carried out while passing bits of data over a link of low latency

vi. Acknowledgement flooding: When routing algorithms are used then the acknowledgements are required at times in sensor networks. In Acknowledgements flooding attack, a malicious node spoofs the acknowledgements providing false information to the destined neighboring nodes.

4) Security issues in application layer:

Application of IoT is the result of closely integration between communication technology, computer technology and industry professional which can be able to find applications in many aspects. The security issues in application layer include eavesdropping and tampering [8]. This layer carries out the responsibility of traffic management. It also provides software for different applications which carries out the translation of data into a comprehensible form or helps in collection of information by sending queries [5]. A path-based DoS attack is initiated in application layer by stimulating the sensor nodes to create a huge traffic in the route towards the base station.

II. COMMUNICATIONS AND SECURITY ON THE IOT

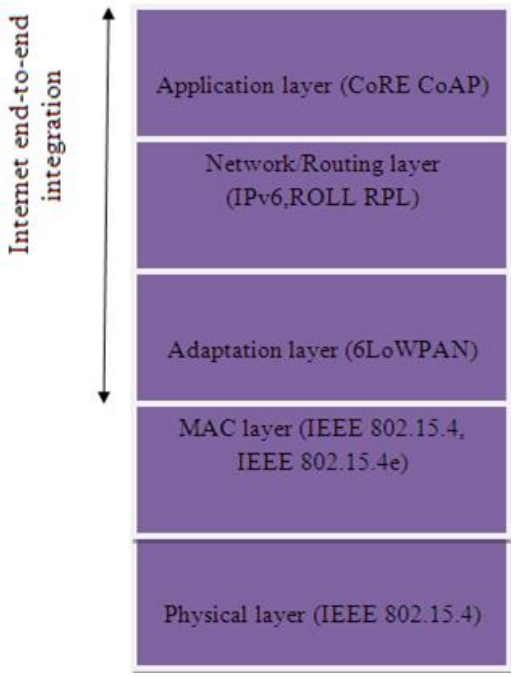

Figure 2: Communication protocols in the IoT

The figure 2 illustrates the communication protocols in the IoT. The protocols that support internet communication with sensing devices in IoT [9].

A. Protocol Stack for the IoT

The constraints of scale factors and sensing platforms of the IoT make most of the communications and security solutions. The Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE) are designing new security protocols and communications which plays a fundamental role in enabling future IoT applications. Those solutions are being designed in line with the constraints and characteristics of low—rate wireless communications and low-energy sensing devices. The new standardized solutions are being designed to guarantee interoperability with existing Internet standards and guarantee that sensing devices should be able to communicate with other Internet entities in the context of future IoT distributed applications.

The communication protocols designed by IEEE and IETF currently enable a standardized protocol stack illustrated in Figure 2. The mechanism that forms the stack must enable Internet communications involving sensing devices, while copying with the requirements of low-energy communications environments and the goals and the lifetime of IoT applications.

In bottom up approach, the main characteristics of the various protocols in the stack are:

1) Low-energy communications at the physical and Medium Access Control layers are supported by IEEE 802.15.4. IEEE 802.15.4. Hence lays the ground for IoT communication protocols at higher layers and also sets the rules for communications at the lower layers of the stack.

2) Low-energy communication environments using IEEE 802.15.4 at most 102 bytes for the transmission of data at higher layers of the stack. A value that is much less than the maximum transmission unit (MTU) of 1280 bytes is required for IPv6. This aspect is addressed by adaptation layer (6LoWPAN) by enabling the

transmission of IPv6 packets over IEEE 802.15.4. 6loWPAN and also implement mechanisms for packet fragmentation and reassembly, among other functionalities.

3) Routing Protocol for Lossy Networks (RPL) and Low-power supports Routing over 6LoWPAN environments. Rather than being a routing protocol, RPL provides a framework which is adaptable to the requirements of particular IoT application domains. Routing requirements and optimization goals are identified by defining Application-specific profiles.

4) Communications at the application layer are supported by Constrained Application Protocol (CoAP). IETF has designed this protocol to provide interoperability in conformance with the representational state transfer architecture of the web.

III. RELATED WORK

Table 1: Security issues and their current proposed solutions in IoT

	ISSUES	TECHNOLOGY	SOLUTION	LIMITATIONS
WSN	Limitation of power, computing ability and storage capacity Attacks towards routing protocol	Secure routing protocol in WSN	Secure routing protocols designed specifically for WSN	If an alternate path is not available then the network is influenced to pratitioning under attack [12].
RFID tags	Multiple tags in one reader's working scope	Conflict collision prevention in RFID	Anti-collision algorithm	It reqiures additional central control area to calculate working scope which increases complexity and cost [10].
Network layer	DDos/Dos attack	Access control and network encryption technologies	Access control	Access control refers that only authorized users can access the WiFi network [10].
Adaptation layer	DDOS attack	Supervision capability: enhance management	Information disclosure protection, disaster control and recovery, supervision	Not distributed [7].
Application layer	DDOS attack	Intrusion detection system	GuardDog, other vendors	Heavy processing overhead [11].

The table 1 illustrates the security issues and solution of IoT. The security issues in WSN are limited of power, computing ability and storage capacity. Since WSN is collection of nodes hence there possibility of attack towards routing protocol. The solution for these issues is secure routing protocol. Multiple tags in reader's working scope is one security issues in RFID tags. The solution for this attack is anti-collision algorithm. DoS attack is a main issue in Network layer, hence access control is a solution for this attack. There are some security issues in Adaptation layer. One of the issues is DoS attack; the solution for this is information disclosure, disaster control and recovery. The DoS attack is one of the issues in application layer and solution for this is GuardDog.

IV. SECURITY REQUIREMENTS

Security in IoT is a need of the time. Security must provide integrity, confidentiality, non-repudiation and authentication of the information flows. Security of IoT communications can be addressed in the context of the communication protocol, or on the other end by external mechanisms. Other security requirements should be considered for the IoT and in particular regarding communications with sensing devices. Some mechanisms are also required to implement protection against threats to the normal functioning of IoT communication protocols. For example, fragmentation attacks at the 6LoWPAN adaptation layer. Some other relevant security requirements are anonymity, privacy, trust and liability which will be fundamental for the social acceptance of most of the future IoT applications employing Internet integrated sensing devices.

V. CONCLUSION AND FUTURE WORK

In this paper we have discussed the current state of internet of things and analyzed the various security issues in IoT. We briefed the communication protocol stack employed in IoT and various layered in IoT architecture. In future, a framework to detect Denial of Service (DoS) attack in IoT will be proposed and its effectiveness will be measured.

REFERENCES

[1] Jun Wei Chuah "The Internet of Things: An Overview and New Perspectives in Systems Design" 2014 International Symposium on Integrated Circuits 978-1-4799-4833-8/14.
[2] Sarita Agrawal, Manik Lal Das "Internet of Things – A Paradigm Shift of Future Internet Applications" Institute of technology, nirma university, ahmedabad – 382 481, 08-10 december, 2011.
[3] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications" ieee communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.
[4] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal "A Review on Internet of Things (IoT)" International Journal of Computer Applications (0975 8887)
Volume 113 - No. 1, March 2015.
[5] Tuhin Borgohain, Uday Kumar and Sugata Sanyal "Survey of Security and Privacy Issues of Internet of Things"
[6] Krushang Sonar, Hardik Upadhyay "A Survey: DDOS Attack on Internet of Things" International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X Volume 10, Issue 11 (November 2014), PP.58-63.
[7] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito and Mark Vinkovits "Denial-of-Service detection in 6LoWPAN based Internet of Things" 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).
[8] QuandengGOU, Lianshan YAN, Yihe LIU and Yao LI "Construction and Strategies in IoT Security System" 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing.
[9] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues" ieee communication surveys & tutorials, vol. 17, no. 3, third quarter 2015.
[10] Qi Jing • Athanasios V. Vasilakos • Jiafu Wan • Jingwei Lu • Dechao Qiu "Security of the Internet of Things: perspectives and challenges" Wireless Netw DOI 10.1007/s11276-014-0761-7.
[11]http//www.slideshare.net.
[12] "A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks" [Deng+].

