Security Protocols for Internet of Things: A Survey

Mrs. Snehal Deshmukh, Asst. Professor
RMD Sinhgad School of Engg, Warje, Pune.
sa_bhosale@yahoo.com

Dr. S. S. Sonavane, Director,
Dr. D. Y. Patil Technical campus, Lohgaon
sssonavane@gmail.com

Abstract
Internet of Things (IoT) is made up of various technologies, which supports advanced services in various application domains. Security and privacy are a very important aspect for IoT application domains. These applications require data confidentiality, authenticity, integrity and access control within the IoT network. For users and things, security is achieved by enforcing the security and privacy policies. Due to the different standards and communication stacks involved in traditional security solutions, it cannot be directly applied to IoT technologies. In IoT number of interconnected devices is expected to increase tremendously hence scalability is the biggest challenge for IoT development. This survey paper presents the available security protocols at respective IoT layers. A comparison of this information is done with respective to various security aspects and research gaps are identified.

Keywords – Internet of Things; Security;IEEE 802.15.4; 6LoWPAN; DTLS; RPL; CoAP.

1. INTRODUCTION

1.1 Internet of Things

Friedemann Mattern et al. [2010] have discussed about the vision of the Internet of Things (IoT) where everyday objects will be deployed as nodes using internet. These objects will be controlled remotely to achieve expected actions. Those will act as physical access points to internal service. Internet of Things is going to open up huge opportunities in economy field as well as individually. But at other side it also introduces risks along with technical and social challenges.

The **Internet of Things** (**IoT**) is the network of physical objects or devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity which enable these objects to collect and exchange data. Fig. 1 shows the different topics which made the Internet of Things complete. It includes Sensors, Actuators, Storage Devices, Processing, Localization and Tracking, Identification, Communication etc.

In Internet of things Smart object is the central parameter which is developed with embedded communication and information technology. These smart objects consists of sensors which will sense the certain activity and communicate with each other within built networking ability, access the internet services. It also interacts with people and take necessary actions.

To achieve this, conventional objects must upgrade digitally. For digital upgradation, advancement in embedded technology is used to add substantial value to enhance their physical functions. Many devices are being computerized and also equipped with network interfaces like smart car, smart bulb, smart washing machine are available today. With the concept of IoT they are making our life easier.[1]

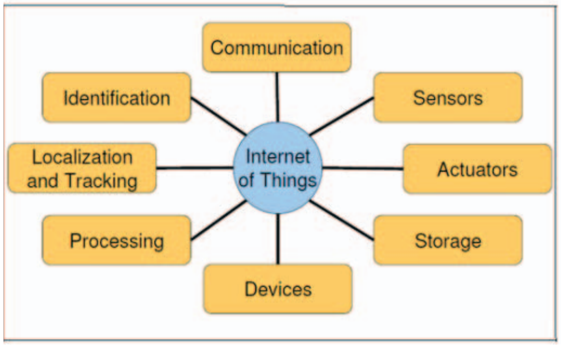

Fig. 1 Topics make up the Internet of Things

Daniele Miorandi et al. [2012] have discussed existing scenarios in Internet of Things (IoT). Today, nearby two billion people around the world use the Internet for a lot of applications like browsing the Web, sending and receiving emails, using social networking applications, accessing multimedia content and services, and many other tasks. As maximum people will access the global information and communication infrastructure, a big challenge is arising related to use of the Internet for communication, compute, dialogue and coordinate between the machines and smart objects. It is expected that, in next decade Internet will be the most essential mechanism of classic networks and networked objects. This new world of internet will support for new ways of interacting; new ways of entertainment; new ways of living new applications, enabling new ways of working. [2]

978-1-5090-5913-3/17/$31.00 ©2017 IEEE

1.2 Need for security in IoT

Kim Thuat et al. [2015] have discussed that the concept of IoT is easy to understand, but still lot of research work is expected in this area. Several aspects of IoT such as IoT applications and architectures are presently being discussed. Currently, major research work is going on in undertaking challenges associated with security, privacy, and trust as majority IoT devices will be deployed. In IoT, every single physical object for example smart car, smart refrigerator or similar devices will be connected to the internet to share the information. This will definitely increase the risk than before as personal data and business secret information will be shared through the internet.[3]

S. Sicari et al. [2015] have discussed that IoT services requires modifications in security and privacy in various applications. In their paper they have surveyed various research directions in IoT security. Security is very important feature in terms of IoT development. IoT consist of heterogeneous environment made up of various technologies and communication standards. Availability, Confidentiality, Privacy for users and things, Authenticity among devices, Integrity to access the remote devices, well defined security and privacy policies these parameters of security in IoT must be addressed properly so that suitable solutions can be designed and deployed.[4]

Ala Al-Fuqaha et al [2015] have provided an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols and application issues. The current revolution in Internet, mobile and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge various technologies to enable new applications by connecting physical objects together in support of intelligent decision making. Security plays an important role in designing of abovementioned concept.[5]

2. THREATS IN IOT AND THEIR COUNTERMEASURES

2.1 Research challenges in Internet of Things

Daniele Miorandi et al. [2012] have given an overview of the critical issues of services and technologies related to IoT. Authors have identified many research challenges in their survey which are expected to become major research trends in future. This survey has provided many guidelines to researchers and developers to work on major issues related to security, communication and similar challenges in field of IoT. Many use cases are identified in this survey which will be helpful as guidelines for researchers so that the innovative technical solutions can make IoT from research vision into reality.[2]

Jorge Granjal et al [2015] have analyzed current technologies and various protocols which are used to add security in IoT. They have also analyzed research trends in this direction. Authors have also done a thorough analysis and concluded about existing security approaches towards IoT and to protect communication in the IoT along with suggestions on future challenges and strategies in the mentioned area. [6]

Rolf H. Weber [2015] has discussed the main challenge in the context of IoT is a challenge of privacy and security. In future IoT will face the challenge of collection of huge amount of data and maintain its security. For this strong technologies must be developed which will take care of security in communication and storage of the data. A lot of work is expected to be done to solve the security and privacy issues in IoT. But these issues regarding IoT data have remained unaddressed. A lot of work is also expected to create industry standards which will maintain minimum level of privacy. In case of transmission or storage the data of sensitive matter for example, health related data, Financial information or some critical data of defense or similar sensitive data, must be maintained properly therefore working on security and privacy issues in IoT is now mandatory. [7]

2.2 Security in IoT

Chen Qiang1 et al. [2013] have discussed the existing researches of network security technology. There are many problems in the security of Internet of Things (IoT) such as RFID tag security, wireless security, network transmission security, privacy protection, information processing security etc. All these issues must be addressed for better future of IoT.[8]

Somia Sahraoui et al [2015] proposed a 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) compression for the header of HIP (Host Identity Protocol) packets. [9]

Reem Abdul Rahman et al. [2016] discussed about Internet of things (IoT) which is a wireless communication network between smart objects connected to the internet.

Table 1: Comparative Chart Security Parameters

Name of Layer\ Security Parameters	**Confidentiality**	**Integrity**	**Authentication**	**Non-Repudiation**	**Fragmentation Attack Protection**	**End to End Security**	**Replay Protection**	**Internal Attack Protection**
Physical/ MAC Layer	**Y**	**Y**	**Y**	**Y**	**NA**	**Y**	**N**	**N**
6LoWPAN Adaptation Layer	**Y**	**Y**	**Y**	**Y**	**N**	**N**	**N**	**N**
Network Layer	**Y**	**Y**	**Y**	**Y**	**N**	**N**	**N**	**N**
Transport Layer	**Y**	**Y**	**Y**	**Y**	**N**	**Y**	**Y**	**Y**
Application Layer	**Y**	**Y**	**Y**	**Y**	**NA**	**Y**	**Y**	**NA**

Y-Addressed N-Not Addressed NA- Not Applicable

It is a latest and fast developing market which connects objects and people and also billions of gadgets and smart devices. With the growth of IoT, there is also increase in security threats of the linked objects. There are several new published protocols of IoT, which focus on protecting critical data. [10].

Table 1 summarizes the various security parameters with respect to communication layers. This table gives the research gaps in the security of IoT.

3. COMMUNICATION LAYERS AND PROTOCOL STACK IN IOT

Reem Abdul Rahman et al. [2016] have given the idea Protocols at respective layers. The widely used protocols such as IEEE 802.15.4 at PHY/MAC layer, 6LoWPANAdoption layer, at, and RPL at Network layer are available in IoT. Constrained Application Protocol (CoAP) is the application layer protocol designed as a equivalent of the HTTP. Various versions of CoAP has been developed which shows it's significant role in various applications in the future of IoT.[10]

Table 2 gives the IoT stack and respective security protocols for IoT.

3.1 Adding security at the Link Layer

Roman et al. [2011] have proposed security system for link layer. They have proposed key management system for sensor network which has added security at link layer. Outlined approach is not sufficient to achieve end to end security. While adding security at link layer, care must be taken such as every node in the path will be trusted. Authors have gone through many solutions to solve the problem of establishing session key in between server and a client with respect to Internet of Things, where client server network is formed from nodes in a Wireless Sensor Network.[11]

Rolf H. Weber [2015] has given the details about Secure Sockets Layer (SSL) which includes key exchange mechanisms. Along with confidentiality and integrity it also provides authentication between Internet hosts. But SSL has few drawbacks. Transport Layer Security (TLS) is used over TCP which is not a preferred option for smart object communication. The reason behind it is TCP connection uses inadequate resource. [07]

Table 2: IoT stack with Secutity Protocol

IoT Layer	**IoT Protocol**	**Security Protocol**
Application	CoAP, MQTT	User defined
Transport	UDP	DTLS
Network	IPv6, RPL	IPsec, RPL security
6LoWPAN	6LoWPAN	None
Data-link	IEEE 802.15.4	802.15.4 security

3.2 Securing the Network Layer

Granjal et el [2010] have described and practically implemented the usage of new compressed 6LoWPAN security headers, with the cryptographic algorithms typically used with the IP security architecture. Their practical evaluation study has shown that this is compatible with existing wireless sensor nodes, and it also gives the new technique which allows secure integration WSNs with IPsec and the internet. [12]

Raza et al [2011] have presented the very first IPsec specification and implementation for 6LoWPAN which is working on adaptation layer.

They have evaluated their implementation and verified that it is feasible to use compressed IPsec to secure communication between hosts in the Internet and sensor nodes.[13]

3.3 Securing the IoT at the Transport Layer

Kim Thuat Nguyenet el [2015] have explained that TLS has been recommended by many standards specified by IETF for security services in IoT. However, as it has been discussed earlier TLS is not a wise choice with respect to the security in IoT.TLS uses reliable transport protocol like TCP which is based on congestion control algorithm. But it is not suitable in IoT which has constrained resource devices. Therefore in tightly constrained environments Datagram Transport Layer Security (DTLS) protocol is proposed which operates on unreliable transport protocol (UDP). It provides the same high security levels as TLS. [14]

3.46LoWPAN Protocol for IoT

Konstantinos Rantos et al. [2013] have discussed about the broad deployment of low-power and lossy networks (LLNs) connected to the Internet. It has raised many security issues regarding the protection of data. Such networks now face all kind of security threats identified in traditional networks. However, solutions found in traditional networks cannot directly be adopted by LLNs, due to the inherently limited capabilities of the embedded systems that embrace them. This paper has focused on the security provided to LLN nodes using 6LoWPAN adaptation format, one of the principal solutions adopted for communicating data over IEEE 802.15.4 networks.6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) standard allows resource constrained devices to connect to IPv6 networks[15]

4. CONCLUSION

In this paper, we have carried out a thorough analysis of the security protocols and mechanisms available to protect communications on the IoT. The majority of security protocols are briefly discussed in this survey paper. From this analysis, it is observed few gaps at various IoT layers as, Fragmentation attacks protection is absent in Physical layer, Network layer, Transport layer and Application layer. It is also seen End to end security is not supported by Physical layer and Network layer. Replay Protection is not supported in the Physical layer, Network layer and 6LoWPAN layer. Internal Attack Protection is absent in Physical layer, 6LoWPAN layer, Transport layer and Application layer. So more work is expected to do in these gaps to secure Internet of Things for implementing it in a better manner.

5. REFERENCES:

[1] Friedemann Mattern and Christian Floerkemeier, “From the Internet of Computers to the Internet of Things”,Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich, 2010.

[2] Daniele Miorandi , Sabrina Sicari , Francesco De Pellegrini , Imrich Chlamtac “Internet of things: Vision, applications and research challenges ” Ad Hoc Networks 10 (2012), journal homepage: www.elsevier.com/locate/adhoc

[3] Kim Thuat Nguyen, Maryline Laurent , Nouha Oualha, “Survey on secure communication protocols for the Internet of Things”, Ad Hoc Networks 32 (2015) 17–31.

[4] S. Sicari, A. Rizzardi, L.A. Grieco , A. CoenPorisini, “Security, privacy and trust in Internet of Things: The road ahead” Computer Networks 76 (2015) 146–164.

[5] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols and Applications”, DOI 10.1109/COMST.2015.2444095, IEEE Communications, Surveys &Tutorials.

[6] Jorge Granjal, Edmundo Monteiro, Jorge Sá Silva “Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues ” ,*University of Coimbra, Portugal.* IEEE Communications Surveys & Tutorials DOI 10.1109/COMST.2015.2388550.

[7] Rolf H. Weber, *“*Internet of things: Privacy issues revisited*”* University of Zurich, Switzerland, computer law & security review 31 (2015)618– 627, Published by Elsevier Ltd

[8] Chen Qiang, Guangri Quan, Bai Yu and Liu Yang, “ Research on Security Issues of the Internet of Things” international Journal of Future Generation Communication and Networking Vol.6, No.6 (2013), pp.1-10 http://dx.doi.org/10.14257/ijfgcn.2013.6.6.01

[9] Somia Sahraoui, Azeddine Bilami, “Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things”, 1389-1286/© 2015, Elsevier http://dx.doi.org/10.1016/j.comnet.2015.08.002

[10] Reem Abdul Rahman, Babar Shah “Security analysis of IoT protocols: A focus in CoAP”, 978-1-4673-9584-7/16/$31.00 ©2016 IEEE

[11] Rodrigo Roman, Cristina Alcaraz, Javier Lopez, Nicolas Sklavos, “Key Management Systems for Sensor Networks in the Context of the Internet of Things”, Computers & ElectricalEngineering, vol. 37, pp. 147-159, 2011.

[12] Jorge Granjal, EdmundoMonteiro, Jorge SáSilva, “Enabling network-layer security on IPv6Wireless Sensor Networks”, 978-1-4244-5638-3/10/$26.00 ©2010 IEEE

[13] Shahid Raza, Simon Duquennoy, Tony Chung,DoganYazar Thiemo Voigtand Utz Roedig, “Securing Communication in 6LoWPAN with Compressed IPsec”, 978-1-4577-0513-7/11/2011 IEEE.

[14] Kim Thuat Nguyen , Maryline Laurent,, NouhaOualha, “ Survey on secure communication protocols for the Internet of Things” , http://dx.doi.org/10.1016/j.adhoc.2015.01.006 1570-8705/_ 2015 Elsevier B.V.

[15] Konstantinos Rantos, Alexandros Papanikolaou, Charalampos Manifavas, “IPsec over IEEE 802.15.4 for Low Power and Lossy Networks”, 2013 ACM 978-1-4503-2355-0/13/11,doi10.1145/2508222.2508240.