Internet of Things and Wireless Physical Layer Security: A Survey

Ankit Soni, Raksha Upadhyay and Anjana Jain

Abstract Internet of Things (IoT) has been a focus of research in the last decade with emphasis on the security aspects like wireless network security, communication security, sensor data security, integrity of physical signals and actuating devices. The existing security techniques are not suitable for IoT applications as the involved devices at the ground level have limited resources, low complexity, energy constraints etc. This survey analyzes various IoT concepts in terms of IoT elements, architecture and communication standards. We also analyze the existing wireless security techniques and security attacks at all the layers of the Open Systems Interconnection (OSI) model with special attention on applicability of wireless physical layer security (WPLS) techniques to achieve security for IoT devices.

Keywords Internet of Things (IoT) · Physical layer security (PLS) · Wireless security techniques · Communication standards · Security attacks and challenges

1 Introduction

One of the key technologies that conceptualize the Internet of Things (IoT) in the real world is the wireless communication. IoT is an integrated part of future internet in which "smart things/objects" are expected to become active participants in real time processes where they are enabled to interact and communicate among themselves. The basis of the security management of IoT is laid by exploring the security

A. Soni (✉) · R. Upadhyay
Institute of Engineering & Technology, DAVV, Indore, M.P, India
e-mail: soniankit15@gmail.com

R. Upadhyay
e-mail: raksha_upadhyay@yahoo.co.in

A. Jain
Shri Govindram Seksaria Institute of Technology and Science,
Indore, M.P, India
e-mail: jain.anjana@gmail.com

S.C. Satapathy et al. (eds.), *Computer Communication, Networking and Internet Security*, Lecture Notes in Networks and Systems 5,
DOI 10.1007/978-981-10-3226-4_11

performance of wireless systems [1]. Due to the open and heterogeneous nature of the wireless medium, data exchange may suffer from various attacks, resulting major threat to the security which is a critical concern in wireless network and so in IoT [2]. Physical layer security (PLS) is the primary security solution that focuses on utilizing the physical (PHY) layer properties of the wireless channels to safeguard the confidential information transmission against various attacks and is applicable for IoT [3].

The discussion proceeds with motivation in Sect. 2, in Sect. 3 we discuss the basic elements, architecture and communication standards for IoT. Section 4 flashes on the wireless network security at different layers of OSI model, WPLS and PLS methods for IoT. Section 5 concludes the survey with some areas identified for future work.

2 Motivation

Wireless network security is a very critical issue to solve for the IoT. There are various techniques in the literature for wireless security however not all existing techniques are suitable for IoT because the IoT communication devices have some unique characteristics compared to smart phones and tablets. They generally have low data rate requirements, periodic data traffic arrivals, limited hardware and signal processing capabilities, limited storage memory and significant energy constraints [2]. Achieving security at the physical layer overcomes the energy and the hardware constraints and is the motivation behind this discussion over IoT and wireless physical layer security (WPLS).

3 IoT Concepts

IoT can be considered as network of anything, where a variety of things (like sensors, mobile phones, gadgets, people) can interact with one another from any place in the world through an infrastructure like internet to serve specific application [4]. The IoT offers a great market opportunity for equipment manufacturers, internet service providers and application developers. The IoT smart objects are expected to reach 212 billion entities deployed globally by the end of 2020 [5].

3.1 IoT Elements

This section proceeds with the functional classification and discussion over the basic IoT elements with examples of each element [4] as shown in Fig. 1.

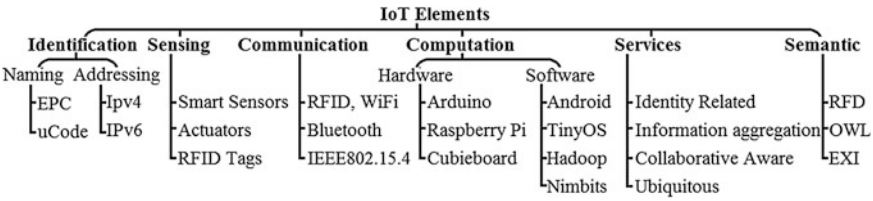

Fig. 1 Elements of IoT with their categories and examples

IoT end user devices are recognized within the network by identification. Identification broadly constitutes Naming and Addressing. Naming refers to object id (EPC: Electronic Product Code, uCode: Ubiquitous Codes) like "S1" for any sensor in the network while the addressing refers to its IP address (IPv4, IPv6) globally.

Sensing means collecting information from the objects such as smart and embedded sensors, actuators, RFID tags, wearable sensors etc. and sending it to the data storage units/services (memory/Cloud/Big data).

Communication involves the exchange of information between the heterogeneous nodes connected in the internet. Low power communication protocols such as Bluetooth, wifi, IEEE802.15 are applied over communication links.

Computation constitutes the hardware processing unit and the software counterpart and is considered as the "brain" of the IoT. The computation unit for IoT should be low complexity and low power consuming as compared to traditional smart devices.

The IoT services can be divided into four groups [6]: Identity-related Services: most basic services which supports other services, Information Aggregation Services: collects raw data from sensors and supplies it to the IoT applications, Collaborative-Aware Services: rely on Information Aggregation Services and take decision on the collected data, and Ubiquitous Services: provide Collaborative-Aware Services anytime they are needed to anyone who needs them anywhere.

Semantic refers to the capability of the system to extract compiled information from various available resources and provide it to the required services. It is supported by Resource Description Framework (RDF), the Web Ontology Language (OWL) and Efficient XML Interchange (EXI) format.

3.2 IoT Architecture

Billions of heterogeneous objects are interconnected in real time systems through internet in the IoT and so a robust and flexible layered architecture is required. The numerous proposed architecture in the literature has not yet converged to an authentic model [7]. In the traditional literature various models were proposed like

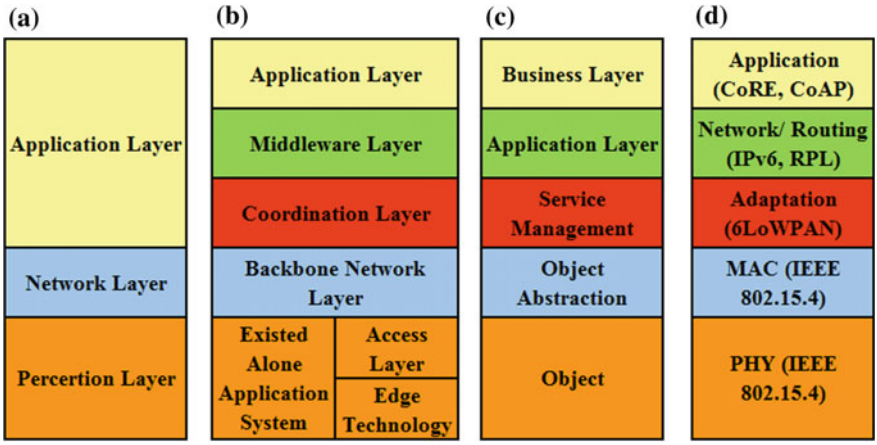

Fig. 2 Various IoT architecture models **a** 3-layer model, **b** 5-layer with enhanced perception layer model, **c** 5-layer model, **d** 5-layer low energy model

3-layer model [8], 5-layer model, 5-layer with enhanced perception layer [9, 10], low energy 5-layer model [11] as shown in Fig. 2. From a bottom-up approach, the following are the main characteristics of the various protocols in this low energy 5-layer model:

PHY Layer represents the physical sensors which collects and process information from ambient. Low-energy communications at the PHY and Medium Access Control (MAC) layers are supported by IEEE 802.15.4 [12]. IEEE 802.15.4 therefore sets the rules for communications at the lower layers of the stack and lays the ground for IoT communication protocols at higher layers.

MAC layer transfers data produced by the PHY layer to the adaptation layer. Low-energy communication environments using IEEE 802.15.4 requires much lesser bytes as compared to other counterparts.

Adaptation Layer pairs a service with its requester based on address and names. Routing over 6LoWPAN environments is supported by the Routing Protocol for Low-power and Lossy Networks (RPL) [13]. Constrained Application Protocol (CoAP) serves the end customers by supporting communication at application layer.

3.3 IoT Communication Standards

Many IoT standards are proposed to simplify the job of application developer and service providers. Basic communication standards like 6LoPAN are generally considered. Figure 3 shows IoT protocol stack with basic communication protocols.

The IoT protocols are classified into four broad categories [4], namely: application protocols, service discovery protocols, infrastructure protocols and other

S. No.	IoT Protocol Stack (Four broad categories)	Position of basic communication protocols in IoT Protocol Stack & Layered Architecture			IoT Layered Architecture (5-Layered Model)
1	Application Protocols	CoAP	MQTT-SN	AMQP	Application Layer
		DDS	HTTP	REST	
2	Service Discovery Protocols	mDNS	DNS-SD		Network Layer
3	Infrastructure Protocols	RPL			
		6LoWPAN	IPv4	IPv6	Adaptation Layer
		IEEE802.15.4			Data Link Layer
		LTE-A	EPC Global	IEEE802.15.4	Physical Layer
4	Influential Protocols	IEEE188.3	IPSec	IEEE1905.1	

Fig. 3 IoT protocol stack with basic communication protocol located in the IoT protocol stack and 5-layered low energy model for IoT

Security Demands	Specific Objective
Authenticity	To differentiate authorized and unauthorized users.
Confidentiality	To limit the confidential data access to authorised user only.
Integrity	To guarantee the accuracy of the transmitted information.
Availability	To make sure that the authorised user can access the services any time on request.

Fig. 4 Wireless security methodologies and demands

influential protocols. However, not all of these protocols have to be bundled together to deliver a given IoT application. Moreover, based on the nature of the IoT application, some standards may not be required to be supported in an application. Basic communication protocols like Advance Message Queuing Protocol (AMQP), Message Queue Telemetry Transport (MQTT), Data Discovery Services (DDS), Representational State Transfer (REST), Routing Protocol (RPL), Hyper Text Transfer Protocol (HTTP), etc. are considered in the IoT protocol standard.

4 Wireless Network Security

Wireless networks usually follow the open systems interconnection (OSI) model constituting the basic seven layers from application to the physical layer considering the top down model. Security threats associated with these protocol layers are generally considered at individual layer level taking into account the integrity, authenticity, availability, and confidentiality [14] as summarized in Fig. 4.

OSI Layer	Basic Protocol		Attack		Security Approach
Application	HTTP	FTP	Malware Attack	FTP Bounce	Unique pairwise keys and cryptography approach.
	SMTP		SMTP Attack	Data Attack	
Transport	TCP	UDP	Desynchronisation	Flooding	Client puzzle authentication approach.
			TCP Sequence Prediction Attack		
Network	IP	ICMP	Sel. Forwarding	Hijacking	Authentication, Monitoring, Probing, Redundancy.
			Sybil Attack	Spoofing	
MAC Layer	ALOHA	CSMA/CA	MAC Spoofing	Collision	Error correcting code, Rate limitation.
	CDMA	OFDMA	Identity Theft	Exhausion	
PHY Layer	WiFi	Ethernet	Eavesdropping	Jamming	Lower duty cycle, Priority message, Spread Spectrum
	802.15.4	Bluetooth	Radio Interference	Temporing	

Fig. 5 Various wireless attacks at different layers of OSI model and the probable security approach with basic protocol applicable at each layer

4.1 OSI Model for Wireless Systems: Attacks and Security Approach

In wired networks, the communicating nodes are physically connected through cables. By contrast, wireless networks are extremely prone to the security threats due to the broadcast nature of the wireless medium. Figure 5 shows various security attacks at different layer of traditional OSI model and the probable security approach.

Since every layer in OSI model rely on different basic protocols so each of them have their own security issues [15–17]. Moreover, wireless networks are vulnerable to malicious attacks like eavesdropping attack, denial-of-service attack, etc.

4.2 Wireless Physical Layer Security

It is common to handle the issues like confidentiality, authentication and privacy in the upper layer of the protocol stack by using key based cryptosystems in the communication systems. The essential requirement of physical layer security is to perform the exchange of confidential information over a wireless medium in the presence of illegitimate user, without relying on higher-layer encryption techniques.

In the recent research many outcomes from the information theory, signal processing, and cryptography reveals that a higher degree of security can be achieved in designing the wireless networks by exploiting the inherent characteristics of physical layer. Physical layer contains definition of hardware specifications, encoding and signaling, data transmission and reception, topology and physical network design. Some key techniques in physical layer are: Multiple Input Multiple Output (MIMO), Code Division Multiple Access (CDMA), Orthogonal Frequency

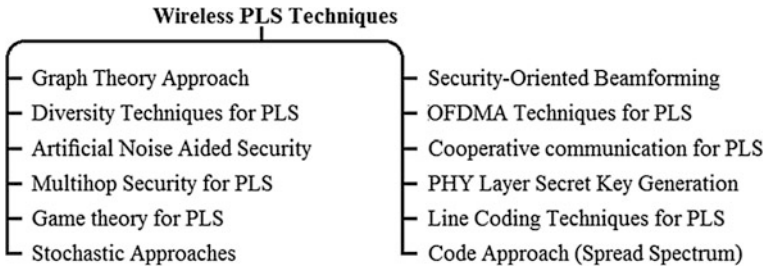

Fig. 6 Different physical layer security techniques applied to wireless networks

Division Multiplexing (OFDM), Algebraic Channel Decomposition Multiplexing (ACDM) etc. [1]. The physical layer security techniques are usually quantified in terms of complexity, secrecy rate, energy efficiency, and Channel State Information (CSI) requirements, relative SINR's, relative BER, relative MSE etc., of the legitimate and illegitimate users. Various wireless physical-layer security techniques are listed in Fig. 6.

4.3 IoT and WPLS Methods

There are some challenges to employ many of the traditional wireless physical layer security schemes in an IoT at different levels. The principal barrier is the problem of accurate CSIT acquisition that includes both channel amplitude and phase information. In the IoT, the acquisition of accurate legitimate CSIT is prevented by limited channel training opportunities and the lack of high-rate feedback channels. Transmitting frequent training signals for channel estimation is highly energy inefficient and wastes spectrum access occasions in dense IoT deployments [2]. Second, eavesdropper CSIT is also difficult to acquire when eavesdroppers are external to the IoT system and remain completely passive. Thirdly, the security techniques employed for IoT sensing applications should be of low-complexity and energy-efficient. Fourth, Considering the PLS for wireless network at the sensor level, various factors has to be considered like: multipath effects, fading, randomness, spatially distributed nature of the sensors, heterogeneity, etc. [18, 19].

Wireless physical layer security techniques such as physical layer signal processing can be applied at a gateway receiver to authenticate whether a transmission came from the expected IoT transmitter in the expected location. Investigating approaches such as ciphers or encoding for physical layer confidentiality that are efficient and have little to no message expansion is a promising direction for investigation that would greatly benefit IoT devices. There are many security methods specified in the literature for wireless sensor network security but keeping in mind the distributed nature of sensors and parallel channel access we suggest security methods like censoring, type based access, channel aware encryption

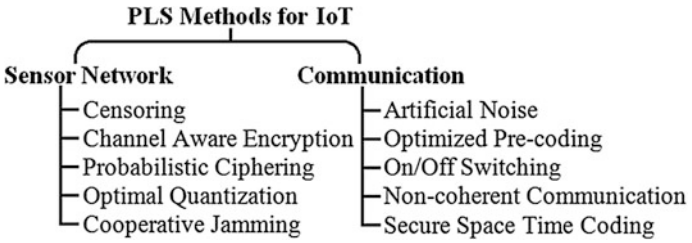

Fig. 7 Different physical layer security techniques for IoT sensor networks and communication

(CAE), optimal quantization, probabilistic ciphering for wireless network security for IoT at sensor level, among these techniques the CAE method offers best optimized combination in terms of low complexity, energy efficiency and CSI requirements [2].

Various signal processing and power approaches considering the artificial noise, Optimized precoding, RFID cryptographic techniques and coding approaches [20] including error correction coding, spread spectrum coding and secure channel analysis [21] can also be employed to achieve security at physical layer. Figure 7 lists out different physical layer security techniques suitable for IoT [2].

5 Conclusion

The IoT may represent a big step ahead for smart and efficient communication through deployment of embedded devices. It represents high degree of consideration towards their security aspects in terms of confidentiality, integrity, privacy and authenticity.

In this survey article we provide an overview of IoT concepts and wireless security with special attention on PLS techniques. It has been concluded that since the objects employed in IoT have limited resources, low complexity design, severe energy constraints so there is a need of designing low energy and low complexity architecture and the security techniques. Further we analyze some PLS techniques for IoT applications considering heterogeneity and distributed nature of the objects at the ground level and observe the appropriateness of CAE method.

We believe that this survey may provide the researchers an overview about the IoT and various security threats in wireless network communication with an approach of WPLS for IoT applications.

Acknowledgements This work is being supported by Department of Electronics and Information Technology (DeitY), Ministry of Communications and IT, Government of India, under Visvesvaraya PhD Scheme for Electronics and IT, www.phd.medialabasia.in.

References

1. Shiu, Y., S., et. al.: Physical Layer Security in Wireless Networks: A Tutorial, pp. 66–74, IEEE Wireless Communications (2011)
2. Mukherjee, A.: Physical-Layer Security in the IoT: Sensing and Communication Confidentiality Under Resource Constraints, vol. 103, pp. 1747–1764, Proc. IEEE (2015)
3. Trappe, W.: The Challenges Facing Physical Layer Security, pp. 6–10, IEEE Communication Magazine (2015)
4. Al-Fuqaha, A. et al,: Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, vol. 17, pp. 2347–2356, IEEE Comm. Surveys & Tutorials (2015)
5. Gantz, J., Reinsel, D.: The Digital Universe in 2020: Big Data, Bigger Digital Shadows, And Biggest Growth In The Far East, vol. 2007, pp. 1–16, IDC Anal. Future (2012)
6. Gigli, M., Koo, S.: Internet of Things: Services and Applications Categorization., vol. 1, pp. 27–31, Adv. Internet Things (2011)
7. Krco, S., Pokric, B., Carrez, F.: Designing IoT architecture(s): A European perspective. Proc, pp. 79–84, IEEE WF-IoT (2014)
8. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future Internet: The IoT Architecture, Possible Applications And Key Challenges, pp. 257–260, in Proc. 10th Int. Conf. FIT (2012)
9. Yang, Z., et al.: Study and Application On The Architecture And Key Technologies for IoT.: In Proc., pp. 747–751, ICMT (2011)
10. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., Du, H. Y.: Research on the Architecture of Internet of Things.: In pp. V5-484–V5-487 Proc. 3rd ICACTE (2010)
11. Granjal, J., Monteiro, E., Silva, J.: Security for the IoT: A Survey of Existing Protocols and Open Research Issues, vol. 17, pp. 1294–1312, IEEE Comm Surveys & Tut. (2015)
12. IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer, IEEE Std. 802.15.4e-2012 (Amendment to IEEE Std. 802.15.4-2011), (2011)
13. Thubert, P. et al.: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.: RFC 6550 (2012)
14. Kolias, C., Kambourakis, G., Gritzalis, S.: Attacks and countermeasures on 802.16: Analysis and assessment, vol. 15, pp. 487–514, IEEE Comm. Surveys & Tutorials (2013)
15. Bellovin, S.: Security problems in the TCP/IP protocol suite, vol. 19, pp. 32–48, ACM SIGCOMM Computer communications Review, (1989)
16. Zargar, G., Kabiri, P.: Identification of effective network features to detect Smurf attacks.: Proc. of IEEE Student Conference on Research and Development, UPM Serdang (2009)
17. Shon, T., Choi, W.: An analysis of mobile WiMAX security: Vulnerabilities and solutions, vol. 4658, pp. 88–97, Lecture Notes in Computer Science (2007)
18. Zou, Y., Wang, X., Hanzo, L.: A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends, pp. 1–31, Proceedings of IEEE (2015)
19. Granjal, J., Monteiro, E., Silva, J.: Security in the Integration of Low-Power Wireless Sensor Networks with the Internet: A Survey, pp. 264–287, Ad Hoc Networks, Elsevier (2015)
20. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey, vol. 54, pp. 2787–2805, Computer Networks, Elsevier (2010)
21. Pecorella, T., Brilli, L., Mucchi, L.: The Role of Physical Layer Security in IoT: A Novel Perspective, vol. 7(3), Information, MDPI (2016)