ISSN 2319 - 6629
Volume 6, No.4, June - July 2017
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt02642017.pdf

Security Issues for Internet of Things- State of Art

Ravinder Beniwal[1]
[1]Faculty of Telecommunications, Technical University of Sofia, Bulgaria, ravin.beniwal29@gmail.com

ABSTRACT

The Internet of Things (IoT) is the future of the internetwork in which every device having the capabilities of sensing and computing can ubiquitous interaction with other devices. The heterogeneous nature of network and ubiquitous IoT devices needs more security enhancements in the current security system, and they also must be efficient enough to implement on constrained devices. In this paper we analyze different security protocols for the IoT environment.

Key words : Internet of Things, Ubiquitous, Security, Heterogeneous Network.

1. INTRODUCTION

The Internet of Things (IoT) is a heterogeneous network in which different devices and actuators having sensing power can interact with each other without any intervention of human. The IoT includes physical devices- embedded with electronics, such as actuators, sensor devices and connected to network which enables the devices to monitor and collect all types of data from different machines and human social life. The emergence of the IoT has led to the constant universal connection of people, objects, sensors, and services. The number of connected IoT devices will grow by 21 percent annually, and will reach up to 18 billion from 2016 to 2021 [1]. The environment of internet started in mutual trust in which everyone could read, update and write information. But the expectations from IoT of public and government about security and privacy are very high, and information security is the most concerned thing for enterprises going to adopt IoT [2].

Allowing every device to connect to internet and to share information, may create more threats than ever for our secrete data and important information. These objects are our everyday use devices like fridges, ovens, washing machines, thermostats and TV sets. It will be a big threat if these devices were spying on us and revealing our information. The main objective of the IoT is to provide a network infrastructure with interoperable communication protocols and software to allow the connection and incorporation of physical and virtual sensors, personal computers (PCs), smart devices, automobiles, and items, such as fridge, dishwasher, microwave oven, food, and medicines, anytime and on any network [3]. The development of smartphone technology allows countless objects to be a part of the IoT through different smartphone sensors. However, the requirements for the large-scale deployment of the IoT are rapidly increasing, which then results in a major security concern.

The IoT devices are gathering information from different sources and sharing it like voice recognition or figure print while playing video game or accessing other devices. Attacker can use this data which can cause privacy problems for person who don't know about the device presence and unaware of the uses of that collected information [4]. The IoT communication can be exposed at unknown number and unknown locations to eavesdroppers. IoT may have some curious legitimate devices belonging to different subsystems as a potential eavesdropper [5].

IoT Layer	IoT Protocols
Application	Core, CoAP
Network/Routing	IPv6, ROLL, RPL
Adaption	6LoWPAN
MAC	IEEE 802.15.4, IEEE 802.15.4e
Physical	IEEE 802.15.4

Figure 1: IoT Communication Protocols Stack

2. SECURITY FOR IOT AND COMMUNICATION

We will go ahead by finding the protocols designed to support communication in internet with sensing devices in the IoT, which are the main focus of our analysis throughout the survey. In the following analysis we also discuss the security requirements that must be targeted by mechanism designed to secure communication using these protocols.

A. IoT Protocol Stack

The prevailing security solutions of the internet are not suitable for the IoT due to constraints of scaling factors and sensing platforms. Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force (IETF) are the groups that are working on the designing of the communication and security protocols for the future IoT applications. These solutions are designed in such a way that they can work on low power and low data rate wireless communication. The standardized protocol stack for communicating protocols is designed by IETF and IEEE is discussed in [6] and illustrated in figure 1. The following are the main characteristics of the IoT protocol stack:

1) Physical and Medium Access Control layers supports low-energy communications by IEEE 802.15.4, so it provide rules for lower layers and make ground for upper layers of IoT protocol stack.
2) IEEE 802.15.4 requires 102 bytes for transmission of data at higher layers of the stack, a much less value than maximum transmission unit [MTU] of 1280 bytes for IPv6.
3) Routing Protocol (RPL) is used for routing in 6LoWPAN environment for Low power and Lossy Networks and used as a framework for the particular requirements of the IoT applications domains. [7].
4) The (CoAP) Constrained Application Protocol is used in application layer of the stack for communication, designed by IETF.

In the current survey we analyze and identify the security protocols and mechanisms available to secure communications using IoT technologies forming the stack described in figure 1.

B. IoT Security Requirements

It's a big challenge to fully secure a traditional system and always a concern to secure the system completely. An under development technology relying on traditional framework is much more susceptible to security threat. Providing protection to company data and IP will be very important after the development of IoT field. The following services are needed to be followed for making sure to secure an IoT device [8].

Authentication: The authentication of an IoT user is going to be a challenging task for IoT. Authentication in IoT is more complex than traditional approach due to new standard and self-configuring protocol. It is easy to control your application with a two factor authentication especially with the help of mobile phones which stays with you all the time.

Confidentiality: It is very easy to intercept a message in IoT with the help of latest technologies by third parties. If any user is accessing his home appliances from public Wi-Fi at a public place and accessing live video of home for third party, it will be easy to access the content from that network. So it's very important to have confidentiality and message secrecy from other entities. Personal information and messages need to be hidden from unauthorized devices on IoT network.

Data Integrity: Privacy is the most important part of any communication and most of the research in IoT is going on in the field of privacy. Data integrity is more important than other issues like availability because integrity may lead to someone life. Public key infrastructure (PKI) and Keyless Signature Infrastructure (KSI) are used for data security from many years. PKI is used for authentication and secure communication on network and KSI is used for integrity proof [9].

Access Control: In traditional systems where all users are known to the system, access control targets only to closed system, but in IoT open and closed systems should be considered where an unknown third party can do the damage.

3. PHYSICAL AND MAC LAYER SECURITY FOR IOT

The important task of IEEE is to produce new standards for the facilitation of common platforms of rules for new technological developments. The IEEE 802.15.4 was designed to support a healthy tradeoff between energy efficiency, range and data rate of communication. IEEE 802.15.4 was employed in IoT with a goal of supporting low-energy communication at the physical and Medium Access Layers. The IEEE 802.15.4 standard supports communication at 250 Kbit/s at a range of ten meters. The IEEE 802.15.4 was formed in 2006 and was recently updated in 2011 to include the recent scenario of the market. It has also many amendments to include the additional PHY layers, new frequency bands. Now we will discuss the operation, communication and security services provided by the IEEE802.15.4 and 802.15.4e.

A. PHYSICAL Layer Communication with IEEE 802.15.4

The IEEE 802.15.4 standard is suitable for low energy wireless communication and makes a structure for higher layers protocols such as 6LoWPAN and CoAP and is also adopted as foundation of WSN standards like ZgBee-2006, ZigBeePRO, ISA 100.11a and WirelessHART [10]. These standards provide only industry solutions and are not designed to support Internet communication with sensing devices. ZigBee defines profiles for applications for home automation and smart energy; WirelessHART and ISA 100.11a are used in industrial automation and control market and IEEE802.15.4e addendum to enable support for critical industry applications.

Channel selection, energy and signal management and physical Radio-Frequency transceiver of sensing device is managed by the IEEE802.15.4 PHY. It supports 16 channels in the 2.4 GHz ISM radio band. The different modulation techniques such as Direct Sequence Spread Spectrum (DSS), Direct Sequence Ultra-Wideband (UWB), and Chirp Spread Spectrum (CSS) are used in the standard PHY to make it more reliable. It achieves reliability with transformation of transmitted information by these modulation techniques with an improved Signal to Noise (SNR) ratio at the receiver and it occupies more bandwidth at a lower spectral power density to achieve less interference along the frequency band.

A. MAC layer Communications with IEEE 802.15.4

There are different operations other than data services such as network beaconing, accesses to the physical channel, validations of frames, guaranteed time slots, node association and security that are managed by the MAC layer. The IEEE 802.15.4 can support network topologies such as star, cluster, and peer to peer by using Full Functional Devices (FFD) and Reduced Functional Device (RFD). The IEEE 802.15.4 devices can be identified by using a 16 bit short identifier used in constrained environment or a 64 bit identifier used in IEEE EUI-64 [11]. There are four types of frames in IEEE 802.15.4:

data frames, acknowledgment frame, beacon frames and MAC command frames. Collisions are managed by CSMA/CA or the coordinator may add a super frame by which application with predefined bandwidth requirements may reserve and use excusive time slots and beacon frame act as the limits of the frame and provide synchronization to other devices and configuration information.

B.MAC Layer Communication with Time- Synchronized Channel-Hopping

The Time Synchronized Mesh Protocol (TMSP) employs time synchronized frequency channel hopping to resist multipath fading and external interference, and is also base for WirelessHART. The IEEE 802.15.4e standard started the usage of internet communication in the context of time for critical applications. The IEEE 802.15.4e devices synchronize with a slot frame structure and a group of slots repeating over time. For every active slot a schedule indicates the devices are communicating with which device and on which channel offset. Synchronization is also required between devices of IEEE 802.15.4e channel hopping that can be frame based or acknowledgement based. In acknowledgement based the receiver calculates the difference between actual arrival and expected arrival time of the frame and sends this information to the sender to synchronize its clock with the receiver. In the frame based the receiver synchronizes its clock with the sender by adjusting it with the same difference.

C.Security in IEEE 802.15.4

Security services at MAC layer are also provided by IEEE 802.15.4-2011 standard that are designed to secure communications at data link layer but also support security mechanism designed at higher layers of the protocol stack.

Security Modes: Different security modes at the MAC layer are supported by the IEEE 802.15.4 standard are described in table 1. These security modes are differentiated by the size of the integrity data employed and security guarantees provided. In the above discussion we find the fundamental security requirements assured by security at the MAC layer.

Confidentiality: Security is optional in the current version of the IEEE 802.15.4 standard. An application may opt security for the different layers of the stack or no security. An application may opt only confidentiality of link layer communication; the data may be encrypted using AES in the Counter mode, using the AES-CTR security mode.

Data Authenticity and Integrity: The security mode AES in the Cypher Block Chaining (CBC) may provide authenticity and integrity of link layer communication for application that produce (MIC) Message Integrity Code added to the transmitted data. The different security modes to support this are AES-CBC-MAC-32, AES-CBC-MAC-64 and AES-CBC-MAC-128.

Confidentiality, Data Authenticity and Integrity: Confidentiality, Data authenticity and integrity for link layer communications can be obtained by employing CTR and CBC mode using the combined counter with CBC-MAC AES/CCM encryption mode. The current mode also supported in sensing platforms like TelosB in the CCM variant that also provides integrity only and encryption only security.

Semantic Security and Protection against Message Replay Attacks: Semantic security and message relay protection can be obtained by setting up of Frame Counter and Key Control fields of Auxiliary Security Header in all IEEE 802.15.4 security modes. The sender may set Auxiliary Security Header to provide support for semantic security and message replay protection in all IEEE 802.15.4 security modes. Frame counter sets the unique message ID and the key counter is controlled by the application, may be incremented if the Frame counter reaches the maximum value. Packets are broken into 16 byte blocks by sender and each block is identified by its block counter.

Access Control Mechanism: A sensing device can access the source and destination address of the frame to search the information of security mode and security related information for the message. Access control list is stored in IEEE 802.15.4 radio chips of the device with 255 entries; each entry contains the information required for processing of the security for communications with device. The ACL entry stores an IEEE 802.15.4 address. A security suite identifier field and security material required for processing security with the devices in the address field. The security material contains cryptographic key.

Table 1: IEEE 802.15.4 Standard Security Modes

Security Modes	Security Provided
No Security	Data is not encrypted Data authenticity is not validated
AES-CBC-MAC-32	Data is not encrypted Data authenticity using a 32 bit MIC
AES-CBC-MAC-64	Data is not encrypted Data authenticity using a 64 bit MIC
AES-CBC-MAC-128	Data is not encrypted Data authenticity using a 128 bit MIC
AES-CTR	Data is encrypted Data authenticity is not validated
AES-CCM-32	Data is encrypted Data authenticity using a 32 bit MIC
AES-CCM-64	Data is encrypted Data authenticity using a 64 bit MIC
AES-CCM-128	Data is encrypted Data authenticity using a 128 bit MIC

Security with Time Synchronized Communications: IEEE 802.15.4e adapts replay protection and semantic security to time synchronized network communication supported by addendum. The addendum defines the possibility of using null or 5-byte Frame Counter values, in the second case it should be set to global Absolute Slot Number (ASN) of the network. The ASN stores total time slots from the start of the network, allowing new devices to synchronize. Time dependent security, replay protection and semantic security can be obtained by using the ASN as a global frame counter.

4. IOT NETWORK LAYER COMMUNICATIONS SECURITY

The IETF IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) working group was formed in 2007 and the main goal was to produce a specification enabling the transportation of IPv6 packets over low-energy IEEE 802.15.4 and similar wireless communication environments. Internet communication in IoT is supported by 6LoWPAN and it shows cross layer mechanism and optimizations may enable standardized communication protocols for IoT. It also enables IPv6 end to end to communication between constrained IoT sensing devices and other similar or more powerful Internet devices, thus providing the required support for the building the future IPv6 based distributed sensing applications on the IoT. IEEE 802.15.4 MAC layer services can be mapped by the 6LoWPAN adaption layer services required by IP layer.

A. 6LoWPAN Frame Format and Header compression

IEEE 802.15.4 supports PHY and MAC layer communication that enable data transportation from communication protocols at higher layers of the stack. Data payload for protocols of the higher layers of the stack is limited to 102 bytes in the absence of link layer security. The adaption layer of 6LoWPAN optimizes the limited payload space through packet header compression. The RFC 4944 [12] defines the mechanism for the transmission of IPv6 packets over IEEE 802.15.4 networks, with header compression defined in RFC 6282 [13]. All 6LoWPAN encapsulated datagrams transported over IEEE 802.15.4 MAC frames are prefixed by a stack of 6LoWPAN headers. A type field occupies first two bits of header for identifying each 6LoWPAN header and standard defines four types of header:

1. *No 6LoWPAN:* the packet is not for 6LoWPAN processing, enable to coexist with the devices not supporting 6LoWPAN.
2. *Dispatch:* supports IPv6 header compression and link layer multicast and broadcast communications.
3. *Mesh Addressing:* supports forwarding of IEEE 802.15.4 frames at the link layer requiring for the formation of multihop networks.
4. *Fragmentation:* It supports fragmentation and reassembly requires to transmit IPv6 datagrams over 802.15.4 networks.

We have observed the importance of 6LoWPAN as a convergence technology supporting an increasingly growing ecosystem of PHY/MAC communications technologies optimized for particular communication environments and applications.

B. Security in 6LoWPAN

There is no security mechanism defined for the 6LoWPAN adaption layer, but there are certain documents that discussed security vulnerabilities, requirements and approaches to consider for the usages of network layer security.

Identification of Security Vulnerabilities: Security on RFC 4944 [10] is related to the possibilities forging or duplicating EUI-64 interface address, which may lead to compromise the global uniqueness of global 6LoWPAN interface identifiers. It also discusses the Neighbor Discovery and mesh routing mechanism on IEEE 802.15.4 environments susceptible to security threats and AES security at the link layer may give a basis for the development of mechanism protecting against such threats, mainly for constrained devices. RFC 6282 focuses on the security issues from RFC 4944, which enables the compression of 16 UDP port numbers to 4 bits. It is discussed here that the overload of ports in this range may increase the risk of an application misinterpreting the content of a message. So, RFC 6282 recommends that the usages of such ports be associated with a security mechanism employing NIC codes.

Identification of Security Requirements and Strategies: RFC 4919 [14] discusses the addressing of security at various complementary protocol layers of the stack that the most appropriate approach may depend on the application requirements and on the constraints of particular sensing devices. There is a possibility of employing security at network layer using IPSec in the transport and tunnel usages modes. In RFC 6568 [15] discuss threats due to the physical exposer of wireless sensing devices, which may pose serious demands for its resiliency and survivability. It also discusses how IEEE 802.15.4 communications may facilitate attacks against the confidentiality, integrity, authenticity and availability of 6LoWPAN devices and communications.

RFC 6606 [16] gives guidelines for designing specific routing approaches; it identifies importance of addressing of security and the usefulness of AES/CCM available at hardware of IEEE 802.15.4 sensing platform. It also discusses the designing security mechanism to adapt to changes in the network topology and devices. This document also discusses time synchronization, self-organization and security localization to provide security for data and multi hop routing control packets.

5. SECURITY FOR ROUTING IN THE IOT

The IETF formed the Routing Over Low-power and Lossy Network (ROLL) working group for designing routing solutions for IoT solutions. Routing Protocol for Low power and Lossy Network (RPL) is used to routing in 6LoWPAN environments. RPL provide a framework that is adaptable to the requirements of particular classes of applications. In the

following section we discuss the security mechanism designed to protect communications for routing operations.

1B	1B	2B
Type	Code	Checksum
Security		
Base		
Option(s)		

Figure 2: RPL Secure control message

1b	7b	1B	2b	3b	3b	1B
T	Resvd	Algorithm	KIM	Resvd	LVL	Flags
Counter						
Key Identifier						

Figure 3: RPL secure control message's security section

Security in RPL: Security versions of various routing control messages and three basic security modes are defined in the RPL specifications [7]. The format of the secure RPL control message is described in figure 2. The high order bit of RPL code field identifies that the security is applied or not to RPL message. Security field format is described in figure 3. Security field illustrate the information about the level of security and the cryptographic algorithms employed to security of the message.

Integrity and Data Authenticity Support: The RPL specifications [7] describe the employment of AES/CCM with 128-bit keys for MAC generation supporting integrity and of RSA with SHA-256 for digital signatures supporting integrity and data authenticity. The LVL field indicates the security provided at packet and allows different levels for data authenticity and options for confidentiality. Presence of confidentiality, integrity and data authenticity with MAC-32 and MAC-64 authentication codes, also 2048 and 3072-bit signatures using RSA can be identified by various values defined by RFC 6550.

Semantic Security and Protection against Replay Attacks Support: Sensing node issue a challenge reponse enabled by Consistency Check (CC) control message with the goal of validating another node's current counter value. Counter field is used to transport a timestamp, indicated by the T in Fig. 3, provides semantic security and protection against packet replay attack. The next byte identifies the security suite, while the Flags field is currently reserved.

Confidentiality Support: Confidentiality may also supported by secure variant of RPL control messages. AES/CCM is adopted as the basis to support security in the current specification [7], other algorithms may also be adopted in the future in the security section of RPL message. RPL control messages may be protected using both an integrated encryption and authentication suite, such as with AES/CCM, as well as schemes employing separate algorithms for encryption and authentication.

Key Management Support: The *Security* section of the *KIM* (Key Identifier Mode) field section illustrated in Fig. 3 indicates whether the cryptographic key required to process security for this message may be determined implicitly or explicitly. RFC 6550 [7] defines different values for this field to thus supports different key management approaches, namely group keys, keys per pair of sensing devices, and digital signatures. This field supports various levels of details of packet protection, and is divided in a key source and key index subfields. The key source subfield indicates the logical identifier of the originator of a group key, while *key index* subfield allows unique identification of keys with the same originator.

RPL Security Modes: Security is applied to routing control messages are defined by RPL and this specification also defines the following security modes:

a) *Unsecured:* Default use mode RPL in which no security is applied.

b) *Preinstalled:* It is employed by a device using a preconfigured symmetric key in order to join an existing RPL instance, either as a host or a router. This key is employed to support confidentiality, integrity and data authentication for routing control messages.

c) *Authenticated:* This security mode is for routers that may initially join the network using preconfigured key and preinstall security mode, and then obtain a different cryptographic key from authority by which it may start functioning as router.

The current RPL soecification [7] defines that the authenticated security mode must not be supported by symmmetric key cryptograhy. A more clear definition of such mechanisms is required, and future versions of the RPL standard may more clearly define how to support them.

6. IOT APPLICATION-LAYER COMMUNICATION SECURITY

Application layer communications are supported by the CoAP [18] protocol, designed by the Constrained RESTful Environments (CoRE) working group of IETF. WE will discuss the mechanisms available to apply security to CoAP communications.

Security in CoAP

The CoAP protocol [17] defines bindings to DTLS (Datagram Transport Layer Security) to secure CoAP messages, with few configurations appropriate for constrained environments.

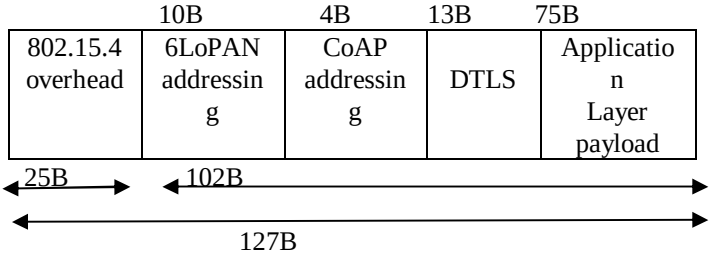

Figure 4: Payload space with DTLS on 6LoWPAN environments

Confidentiality, Authentication, Integrity, Non- Repudiation and Protection Against Replay Attacks Support: Security is supported at transport layer with adoption of DTLS rather than application layer protocol. DTLS provides guarantees in terms of confidentiality, integrity, authentication and non-repudiation for application-layer communications using CoAP. Availability of payload space for applications in IEEE 802.15.4 and 6LoPWAN communication environments in the presence of CoAP and DTLS are described in figure 4.

DTLS adds a limited per-datagram overhead of 13 bytes after initial handshake completion. The impact of DTLS on constrained wireless sensing devices is due to the cost of supporting the initial handshake plus the processing of DTLS adds a limited per-datagram overhead of 13 bytes after initial

handshake completion. The impact of DTLS
on constrained wireless sensing devices is due to the cost of supporting the initial handshake plus the processing of security .for each exchanged CoAP messages. AES/CCM is adopted as the cryptographic algorithm to support fundamental security requirements in the current CoAP [17] specification.

CoAP Security Modes: CoAP defines four security modes that applications can employ in addition with adoption of DTLS.These security modes are:

(a. NoSec: this security mode provides no security, and CoAP messages are transmitted without security applied.

(b. PreSharedKey: this security mode may be applied to sensing devices that are preprogrammed with symmetric cryptographic key required for communication with other devices.

(c. RawPublicKey: The security mode is appropriate for the devices which requires authentication based on public keys, but unable to participate in public key infrastructure. The device must be preprogrammed with asymmetric key pair that may be validated using out of band mechanism and programmed in manufacturing process without a certificate.

(d. Public key infrastructure. The device must be preprogrammed with asymmetric key pair that may be validated using out of band mechanism and programmed in manufacturing process without a certificate.

Table 2: Security Techniques and Proposals for IoT Communication

Operational Layer	**Security Properties and Functionalities Supported**	**Context of Application of Security**	**Details**
6LoWPAN adaption	Confidentiality, Authentication, Integrity, Non-repudiation	Transport end to end security	Stateless compression of AH and ESP security headers for 6LoWPAN
6LoWPAN adaption	Resistance against fragmentation attacks	Communication between 6LoWPAN devices	In 6LoWPAN header timestamp and nonce is added
Transport Layer	Confidentiality, Authentication, Integrity, Non-repudiation	Security for CoAP multicast Communications	DTLS record layer is added for group messages
Transport Layer	Confidentiality, Authentication, Integrity, Non-repudiation	Transport end to end security	Compression of DTLS headers for 6LoWPAN using IPHC
Routing Layer	Confidentiality, Authentication, Integrity, Non-repudiation	Protection of RPL routing control messages	Defining RPL control messages with two security modes
Routing Layer	Resistance against internal attacks	Protection of RPL routing operations against updates	Using of version no and rank authentication security scheme
Application Layer	Confidentiality, Authentication, Replay protection	protection of CoAP messages using DTLS	Definition of binding to DTLS to protect CoAP messages
Application Layer	Confidentiality, Authentication, Integrity, Non-repudiation	Transparent and granular end to end security	CoAP security options allows for granular security authentication of clients

Certificates: It supports authentication based on public keys for those application which can participate in a certification chain validation purpose. The device has an asymmetric key pair with an X.509 certificate which binds it to Authority Name signed by some common trusted root.

Elliptic Curve Cryptography (ECC) [18, 19] is used to support the RawPublicKey and Certificates security modes in CoAP security using DTLS. Device authentication is done by using Elliptic Curve Digital Signature Algorithm (ECDSA), supported by ECC, and key agreement is done by using ECC Diffie-Hellman counterpart, the Elliptic Curve Diffie-Hellman Algorithm with Ephemeral keys (ECDHE). The NoSec security mode corresponds to a device making communication between CoAP client and CoAP server using the "coap" scheme and there must be DTLS exist between them.

7. CONCLUSION

IoT is the future of networks in which sensing devices are interconnected with the internet and different IP based standard technologies will be providing basic functionalities for the development of new IoT applications. Security may be the key enabling factor for such applications, designing a secure mechanism for IoT application will be an important activity. With these things in mind, we have done a survey on existing security protocols and available mechanism for secure communication on IoT.

REFERENCES

1. Ericsson, Ericsson Mobility Report, November 2016, available at: **https://www.ericsson.com/mobility-report**
2. Gartner, Forecast: IoT Security, Worldwide, 2016, available at: https**://www.gartner.com/doc/3277832/forecast-iot-security-worldwide**
3. M. Aazam, M. St-Hilaire, C. H. Lung, I. Lambadaris. **PRE-Fog: IoT trace based probabilistic resource estimation at Fog**. In Proceedings of the 13th IEEE Annual Consumer Communications and Networking Conference (CCNC) 2016, pp. 12-17.
4. Robin Wilton. **Four Ethical Issues in Online Trust**. Issue brief no. CREDS-PP-2.0. Internet Society, 2014
5. Qian Xu, Pinyi Ren, Houbing Song and Qinghe Du. **Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations** special section on Internet of Things (IoT) in 5G Wireless Communications June 2016
6. M. Palattella et al., "**Standardized protocol stack for the Internet of (Important) things**," IEEE Commun. Surveys Tuts., vol. 15, no. 3, pp. 1389– 1406, 2013.
7. P. Thubert et al., **RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks**, RFC 6550, 2012.
8. Hong Yu, Jingsha He, Ting Zhang, Peng Xiao, and Yuqiang Zhang. **Enabling end-to-end secure communication between wireless sensor networks and the internet**. World Wide Web, pages 1–26, 2012. http://www.mtsi-us.com/blog/part-hardening-pki-ksi/.
9. Hong Yu, Jingsha He, Ting Zhang, Peng Xiao, and Yuqiang Zhang. **Enabling end-to-end secure communication between wireless sensor networks and the internet**. World Wide Web, pages 1–26, 2012.
10. http://**www.mtsi-us.com/blog/part-hardening-pki-ksi/**
11. A. Kim et al., **When HART goes wireless: Understanding and implementing the WirelessHART standard**, in Proc. IEEE Int. Conf. ETFA, 2008, pp. 899–907.
12. The IEEE Standard Association, Guidelines for 64-bit Global Identifier (EUI-64), (accessed Nov. 2014), 2013. [Online]. Available: http://**standards.ieee.org/db/oui/tutorials/EUI64.html**
13. G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. **Transmission of IPv6 Packets Over IEEE 802.15.4 Networks**, RFC 4944, 2007.
14. Hui and P. Thubert. **Compression Format for IPv6 Datagrams Over IEEE 802.15.4-Based Networks**, RFC 6282, 2011.
15. N. Kushalnagar, G. Montenegro, and C. Schumacher**. IPv6 over Low- Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, Goals**, RFC 4919, 2007.
16. E. Kim, D. Kaspar, and J. Vasseur. **Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)**, RFC 6568, 2012.
17. C. Bormann, A. Castellani, and Z. Shelby. **CoAP: An application protocol for billions of tiny Internet nodes**, IEEE Internet Comput., vol. 1, no.2,pp.62–67,Mar./Apr.2012.
18. S. Suman, Shubhangi. **A Survey on Comparison of Secure Routing Protocols in Wireless Sensor Networks**, International Journal of Wireless Communications and Networking Technologies, Vol. 5, No.3, April – May 2016, pp. 16-20.
19. SECG-Elliptic Curve Cryptography-SEC 1, (accessed Nov. 2014). [Online]. Available: http**://www.secg.org**