Survey on IoT Security Issues and Security Protocols

Nikshepa
II Year M.Tech
NMAM Institute of Technology
Nitte, Karnataka

Vasudeva Pai
Assistant Professor
NMAM Institute of Technology
Nitte, Karnataka

ABSTRACT
Internet of Things (IoT) is a trending technology in the modern day. It has been so popular that there have been a millions of applications developed on this technology. The popular products of IoT include Smart home, Wearable, Smart city, Smart grid, Industrial Internet, Connected car, smart farming etc. The wide range of usage of IoT system has introduced a lot of thinking in security concerns surrounding these systems. There are back draws associated with the different security measures incorporated with the applications. The survey paper defines all the security concerns and the so far introduced security protocols in the IoT environment.

Keywords
IoT, Networks

1. INTRODUCTION
The Internet of things (IoT) environment is a collection of devices which are interconnected to each other. The devices in IoT are called as sensors/nodes. A node can be any of application specific sensors, mobiles, large computational devices etc. The IoT systems supports the identification of these nodes or sensors within the desired ranges.

The devices attached to an IoT domain are remotely controlled or accessed. This concept is being defined in the IoT framework. As a result of these IoT specifications there have been significant advantages along the proficiency, precision, and financial considerations. The errors that could have occurred due to the manual interception is also reduced. Today we find the implementation of the IoT systems around several areas of the world. These developments suggest the significant increase of the IoT networks and the devices involved in this environment, for example, smart homes, wearable, smart city, smart grids, connected cars, industrial internet, connected healthcare, smart retail, smart supply chain, smart farming.

1.1 IoT Protocol Stack
The Figure 1 depicts the protocol stack of the IoT environment. The layers of the stack are very similar to that of the IP model but there are few differences among the layers. We can learn from the figure that there are new layers and protocols included in the IoT stack. The IoT stack includes layers like:

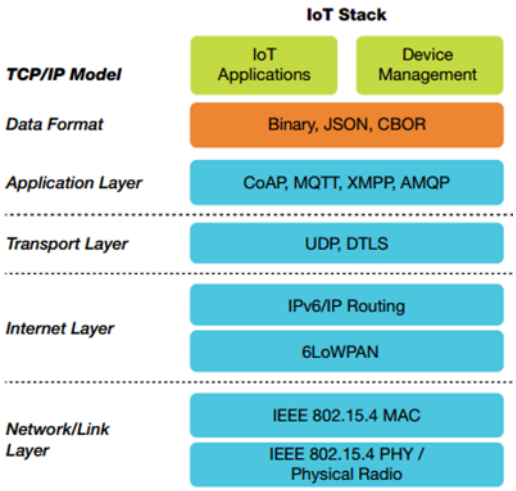

Fig. 1: IoT Protocol Stack

1. *Physical Layer/Link Layer:* The functionality associated with the link is similar to that of the IP model where the common task involves Fragmentation and reassembly, flow control, error control etc. then layer involves the transmission of the IEEE 802.15.4 ZigBee frames.
2. *Adaption Layer:* One of the new layer found in the stack called the adaption layer. The functionality of the adaption layer involves both of previous lower layers. It assists in the routing and the fragmentation. The prominent protocol used in this layer is a LowPan used for the routing in low power network.
3. *Network Layer:* The network layer have the exact function of routing the packets along the network. The other task includes managing network of the system. RPL is a most widely used routing protocol in IoT network.
4. *Transport Layer:* End to End communication across the nodes or the devices is facilitated using this layer. UDP and the DTLS protocols are widely prominent among the protocols used ion the transport layer.
5. *Application Layer:* Application layer allows users for the real of the IoT apps that have been deployed for the users. CoAP, MQTT, XMPP and several other protocols are used across this layer.

2. LITERATURE SURVEY
Vikas in [1] explained the security architecture of the IoT system and the layers of the architecture. It also introduced the threats involved in different layers of the IoT [11]. Rahman et. al stated the complete working and functionality of the IoT application layer protocol CoAP[2]. In [3] the authors explained the end-to-end protocol like 6LowPan adaption layer protocol. They also explained the frame structure, compression model etc. [4] stated the current implementations that bare deployed using the IoT technology. Also listed the

several privacy and the security concerns related to the deployments. It also provided an insight on the future trends that can be optimized with the IoT. William et. al [5] explained the challenges with the IoT implementation across various sectors.[6] explained the different implementable hierarchy levels of the system. Also explained different types of the attacks that can harm the various IoT applications. [7] Surveyed the IoT stack layers in detail and mentioned the different mechanisms across each layers that could be implemented to prevent any security threats to the different layers of the IoT. Teng et. al in [8] suggested that the CAD technology that can be incorporated to design the various security procedures to prevent any types of the security violations in the IoT environment. Authors also briefed about the security threats and discussed the security designs accordingly. [9] Took to the different layer of the protocol stack and mentioned the services associated with the each layers of the IoT system. They also spoke about how the encryption mechanisms can be incorporated in the layers to enhance the security of the layers. Ponle et. al in [10] explained the routing and the adaption layer protocols like RPL and 6Lowpan respectively also explaining the various specific features and the implementation of the protocols.

3. SECURITY IN IOT- REQUIREMENTS AND ISSUES

The definition of security means to develop several optimal mechanisms to preserve the safety and integrity of any system. Meanwhile privacy can be referred as preventing external agent from intercepting onto the data communication. Security and privacy can be the major network requirements for any type of the networks. IoT system is subjected to concerns in these issues.

The major criteria required to be fulfilled in case of network security are [1]

- Confidentiality: Non-Disclosure of the information processed along the network to external factors.
- Integrity: Preserving the message structure along its transfer through the network.
- Availability: The network should be always available under any circumstances.

3.1 IoT Security Architecture and associated issues

[6] Many researches have proposed the security architecture of the IoT system made up of several layers. Each layer has an associated functionality associated with them. The figure below has depicted the IoT security architecture.

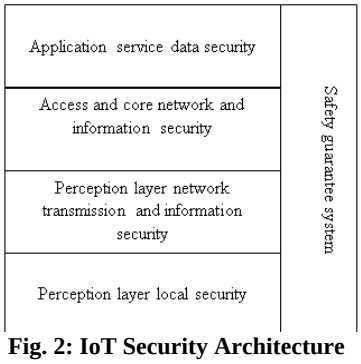

Fig. 2: IoT Security Architecture

The layering of the security architecture has not prevented the attacks from harming the system. Each layer has been associated with the associated problem of their own.

3.1.1 Perception Layer

This layer deals with the collection of all the information pertaining to the system. This layer is also called the Recognition layer. The security issues with this layer are:

1. Physical capture: It is an attempt from an intruder to harm the physical components associated with the network setup.
2. Cloning Attack: The hackers try to get an access to the network environment by creating malware node similar to the ones in the network.
3. Routing Attack: Network layer threats include Spoof attacks, alteration or replay, black hole and selective forwarding attacks, sinkhole attacks, Sybil attacks, wormhole attacks, HELLO flood attacks, and acknowledgement spoofing.
4. Brute Force Attack: Brute force is a trial and error mechanism used by external threats to decode encrypted sensitive data such as passwords etc. through extensive effort rather than implementing manual strategies.
5. DoS Attack: This attack disables any system by flooding with request messages and making it unperformed.

3.1.2 Middleware Layer

Middleware Layer does the duty of providing reliable platform for application layer via providing various services in terms of Web Services and Interfaces.

1. Unauthorized access: Any intruder trying to get the access into the system by clearing all the security obstacles.
2. Session Attack: Session hijacking, is the exploitation of a valid computer session sometimes also called a session key to gain unauthorized access to information or services in a computer system.

3.1.3 Application Layer

These layers are ought to receive the services requested by the users and provide them the actual service

1. Malicious code: The application layer activities involves a great risk when an intruder tries to hack the user system by sending malicious files containing malicious code.
2. Social Engineering: Social Engineering is the term utilized for a wide scope of vindictive exercises achieved through human communications. It utilizes mental control to trap clients into committing security errors or giving endlessly delicate data.

The IoT environment is also subjected to similar vulnerabilities that are present in common networking environment [8], like Insecure Web Interface, Insufficient Authentication/Authorization, Insecure Network Services, Lack of Transport Encryption, Privacy Concerns, Insecure Cloud Interface, Insecure Mobile Interface, Insufficient Security Configurability, Insecure Software/Firmware, and Poor Physical Security

4. IOT PROTOCOLS

4.1 Introduction to IoT protocols

4.1.1 MQTT (MESSAGE QUEUE TELEMETRY TRANSPORT)

MQTT is a Client Server Communicating messaging transport protocol. The design of this protocol makes it very easy to implement due to its simple and light weight nature. The MQTT keeps running over TCP/IP or over other conventions that gave requested, lossless, two-way associations. The

features of MQTT protocol are, providing one-to-many messaging using publish/subscribe message pattern, an informing transport that is freethinker to the substance of the payload, three types of services are provided by the protocol for delivery of messages: "At most once", where messages are transmitted according to the best efforts of platform. The loss can happen and this level could be beneficial, secondly, "At least once", where message are assured to arrive but redundancy can occur. Finally, "Exactly once", where message are delivered exactly once. This that cause to drastically reduce network traffic.

4.1.2 CoAP (Constraint Application Protocol)

CoAP is a web transfer protocol designed for the constrained nodes and the constrained network called as low power or Lossy networks. The nodes in these types of networks consists 8-bit microcontroller with limited ROM and RAM memories, while the packet error rate and the throughput is calculated approximately to 10 kbps [11].This protocol designed for M2M application like traffic control, security business, telemedicine etc. CoAP provides a client-server type of communication between end points of application, build-in discovery services and resources, and includes URIs and Internet media types. CoAP is designed to have a simple and friendly interface with HTTP for integration with the Web with also considering unique requirements such as multicast support, very low overhead issues and simplicity for constrained environments.

4.1.3. QUIC

QUIC plans to be about identical to an autonomous TCP association, yet with much lessened inertness. One of the inspirations for creating QUIC was that in TCP the deferral of a solitary bundle prompts head-of-line obstructing for a whole arrangement of SPDY streams; QUIC's enhanced multiplexing bolster implies that just a single stream would stop. Round-trip times, generally characterized by the speed of light, are limited, and subsequently the best way to diminish association dormancy for a productively directed association is to make less round-trips. A great part of the work on QUIC is focused on diminishing the quantity of round outings required while building up another association, including the handshake step, encryption setup, and introductory information demands. QUIC customers would, for instance, incorporate the session transaction data in the underlying parcel. This pressure is upgraded by QUIC servers, which distribute a static setup record that is compactly alluded to. The customer additionally stores a synchronization treat it got from the server, empowering ensuing associations with acquire zero overhead inertness.

4.1.4. DTLS

The DTLS is a security protocol designed to protect data communication between the communicating applications. It is intended to keep running in working space, without making any changes to the existing system. DTLS does not guarantee the delivery of data neither it is reliable. The same is also applicable for payload information. Applications such as media streaming, Internet telephony, and online gaming this protocol for communication because of its property of security for data to be transported. The conduct of these applications is unaltered when the DTLS convention is utilized to secure correspondence, since the DTLS convention does not adjust for lost or re-requested information movement.

The premier designing principality of DTLS is the construction of "TLS over datagram". Since TLS cannot be applied directly in Datagram environment because there is a possibility of data loss or reorder. TLS has no inward offices to deal with this sort of trickiness, and in this manner TLS executions break when re facilitated on datagram transport. The purpose of DTLS is to make minor alterations to TLS that is necessary to solve the protocol issues. To the best degree conceivable, DTLS is indistinguishable to TLS. Any applications that are to be invented using the DTLS, we develop the invention in such a way that the style of TLS specification.

Unreliability creates problems for TLS at two levels:

1. TLS's activity encryption restrict the permit autonomous decoding of individual records. On the off chance that record N isn't gotten, at that point record N+1 can't be unscrambled.
2. The TLS handshake layer accept that handshake messages are conveyed dependably and breaks if those messages are lost.

4.1.5 CCIN

Information-centric networking (ICN) is a way to deal with develop the Internet foundation to straightforwardly bolster information driven and area autonomous interchanges by presenting particularly named information as a centre Internet guideline. In this protocol the access to the data is irrespective of the location, storage and application and non-monitored mobility. Increased efficiency, scalability and robustness are the pros when considered with the CCIN protocol.

4.1.6 6LowPan

6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. The naming of 6LoWPAN was done by the IETF organization. The purpose behind the 6LowPan development was to develop a protocol for the low power networks like IoT systems and Wireless sensor networks. The basic idea behind IoT development was to make the low power devices able to participate in IoT kind of networks which involves high processing power etc.

The data transmission across the low power networks are supported by the IoT group defines Encapsulation and the Header Compression mechanisms. The devices of the IoT network group are supported with the sensing communication capability along the wireless environment.

5. SECURITY ARCHITECTURE AND PROTOCOL IMPLEMENTATION

The IoT structure has enable a standardized protocol stack that has an OSI similar layer format. The naming associated with IoT stack is similar to the OSI layering but with small variations. The stack is formed in such a way that it specifies a communicable path for the end point applications. The additional considerations associate here are the minimal requirement of the power and other requirement with the additional adaption layer forming its existing between the data link and the network layer. [4]. the following figure depicts the protocol stack of the IoT and then follows the various layers and the characteristics of each layer.

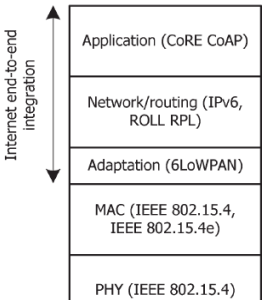

Fig. 3: IoT protocol stack

5.1 Physical Layer – IEEE 802.15.4

The general idea behind the physical layer is to provide a path for the data transmissions. The IEEE 802.15.4 standard also suggest in providing the security measures. This also supports in designing security controls to higher layers of the protocol stack. Efficient symmetric cryptography is implemented at the hardware levels of the sensing platforms. The very popular AES encryption method is used for the cryptography purposes.

Security Modes*:* The Mac layer supports various modes of security as specified by the IEEE 802.15.4 standard. Following details explains the different modes according to the levels of the security and the size of the data integrity.

Security mode	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

Fig.4: Security Modes in MAC layer

The figure below depicts the frame format of the data for the link layer with the suitable security application. At the beginning of the frame in the header section, the Security Header Field of the Frame Control Field is set which indicates that a frame as a protected frame. The usage of the Auxiliary security defines the way the security has been implemented into the data frame and within the field there is a Security control field determining the type of the security mode applied in the frame. The field also determines the type of the cryptographic key that requires to process the security must be selected among senders and receiver based on the security mode selected. The keys may be selected based on the agreement by the two parties or either by the fields among the frame. The Key Source and Key Index subfields within the Key Identifier Field processes the necessary information to choose the key to be used for the communication.

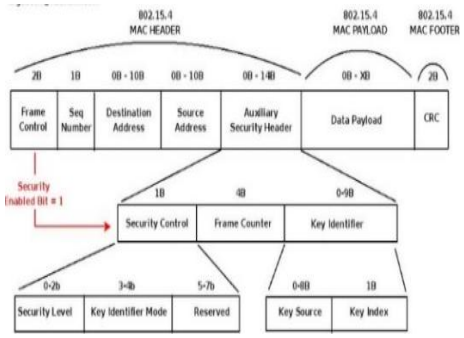

Fig 5: IEEE 802.15.4 Packet Format

5.2 Adaption Layer – 6LowPan

The 6LowPan header consists of 4 header types:

No 6LoWPAN: This header type clearly indicates that the packet has not 6LowPan features enabled and thus cannot be considered for further processing.

• **Dispatch**: The header field is useful in performing multicast and broad cast communications in the link layer as well as supports IPv6 header compression.

• **Mesh addressing**: Forwards the relevant frames at the link layer of the 802.15.4 standard.

• **Fragmentation**: This identifies the need for the fragmentation and reassembly of the frames.

The early disadvantage mentioned with regard to the 6LowPan is the defining of a specific security mechanism associated with the protocol. The protocol still relies on the security mechanisms implemented by the other IoT protocols.

5.3 Network Layer – RPL Protocol

When a low power network was developed there was a need for the routing protocol to be designed as the major source of energy was consumed for the packet routing purpose. Realizing the requirement the IETF Group strived for the purpose of developing a routing protocol. The Routing Over Low-power and Lossy Networks (ROLL) working group of the designed a RPL protocol for the same cause.[11] The RPL protocol has considered secured message transactions apart from just routing the packets. As a result of this enabling security among the sensor devices it has defined the three modes of security among the devices in the network layer.

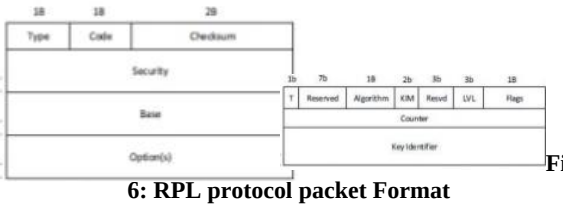

Fig. 6: RPL protocol packet Format

Like the various other protocols of the lower layers the RPL has also the format for the data to be transmitted along with the previously stated security modes. All these are implemented in order to define an uttermost level of security. In the frame format the CODE field determines if the security has been enabled or not. The higher order bit of the field determines if the control messages of the RPL are secured or not. [3].As similar to the link layer packet format the Security field decides on the mode of the security selected and the usage of the encryption/decryption algorithms accordingly.

The other security features supported and implemented by the RPL network layer routing protocol includes:

Support of Integrity and Data Authenticity: Authenticity refers to the phenomenon of allowing appropriate user to

access the system for data communication. Integrity refers to the non-modification of the data along its traversal along the network .In order support these features RPL uses the AES/CCM with 128 bit keys for integrity and accordingly digital signature algorithm like SHA-256 along with RSA to allow authentication. The *LVL* (Security Level) field provides information regarding the security implementation performed along the traffic.

Support of Semantic Security and Protection against Replay Attacks*:* This supports the detection of the any kind of attack that can happen against the system deployed along the network layer. A very common field CC or in full Consistency Check determines any false message being delivered at the destination by checking the CC counter value of both the sender and the receiver.

Support of Confidentiality*:* Confidentiality refers to non-disclosure of any sensitive information to any external third parties other than the communicating end systems. In order to support the confidentiality feature the RPl secure protocol uses the cryptographic algorithms like RSA, AES/CCM etc.

Support for Key Management*:* whenever in any real world application if cryptography plays a part then the necessity of a key to carry out the encryption/decryption has a important role to play. The *KIM* (Key Identifier Mode) field of the in the security section of the RPL frames format defines if any usage of the key has been made for securing the system. Further the RFC system has provided various options within the frame format for selecting the keys, key pairs etc.

5.4 Application layer – CoAP Protocol

The application layer in any layered architecture allows the user to have a access to the system to the GUI or any other means. As a result the application layer provides a Constrained Application protocol or CoAP protocol. This convention executes an arrangement of systems to pack application-layer convention metadata without trading off application between operability which is a requirement defined form the Web architecture called REST or Representational State Transfer. CoAP support the UDP messaging format which is similar to that of the IoT adaption Layer 6Lowpan Protocol. But there is a significant work performed that proposes a TCP variant to be also used along the CoAP.

Application-layer communications may supports the deployed IoT sensor devices to work along the already present internet applications without performing any modifications to the existing devices. The working of the CoAP follows the structure of the HTPP request and response between the end points of the applications.Also the usage of the URI is enabled for better message communication among the energy limited devices.

The following figure depicts the packet format and the related information of the various messages used in the CoAP.

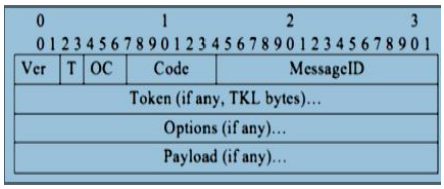

Fig. 7 CoAP protocol packet format

Message contents	Description	Bytes
Version	• Protocol version	2 bits
Type	• Confirmable (CON) - Must be acknowledged by the receiver with an ACK packet. • Non-Confirmable (NON) - messages that do not require acknowledgement • Acknowledgement (ACK) - Acknowledge a confirmable message • Reset (RST) - Reject a confirmable or remove an observer	2 bits
Token Length	• Specifies the length of the token as 0 to 8 bytes	4 bits
Code	• Response code analogous to HTTP response codes, can be a success message, client error, or server error	8 bits
Message ID	• Identifier for each message sent, which in most implementations are likely sequentially assigned; not very effective for security purposes	16 bits
Options	• Can be set to include one or more options, including a subset of what's available via HTTP headers	-
Payload	• Body of message or specific format, if any	-

Fig.8: Packet Description of CoAP

5.4.1 Security Implementation in the CoAP

Just like the other protocols the application layer protocol strives to ensure protection by combining with the popular DTLS to secure the messages. [2] Siad that DTLS implents security and provides the following security features i.e. Support for Confidentiality, Authentication, Integrity, Non-Repudiation and Protection against Replay Attacks.

5.4.2 Security Modes of the CoAP

• **NoSec**: This mode defines that the CoAP doesn't guarantee any security and the message share not secured dueing the transmissions.

• **PreSharedKey:** This security mode maybe used when a system has the communicating devices and the end devices already programmed with the cryptographic keys agreed upon the usage.

• **Raw Public Key**: This mode allows the devices that are not a participant in the PKI and has to get authenticated for the usage of the predefined public keys.

• **Certificates**: This security mode also supports authentication based on public-keys, but for applications that are able to participate in a certification chain for certificate validation purposes.

6. CONCLUSION

IoT system proposes several requirements in their design for implementing the security methods like CIA trends and few more. As required, IoT also impends a security architecture incorporated from ISO Protocol stack including layering architecture consisting of protocols at each layer. The protocols define their security proposals according of the requirement of their layers. The important protocols among the IoT can be CoAP, IEEE 802.15.4, RPL, Quic, CCIN, etc. Every protocol consists of their own header format and frame format. These includes own fields differing from one protocol to another. The security mechanism implemented also varies from one protocol to another. Thus all these works together in a layered fashion providing necessary security for the IoT environment.

7. REFERENCES

[1] Vikas B O, Department of Computer Science and Engineering, SCE Bangalore,"Internet of Things (IoT): A Survey on Privacy Issues and Security".

[2] Reem Abdul Rahman,College of Technological Innovation and Babar Shah College of Technological Innovation,"Security analysis of IoT protocols: A focus in CoAP"

[3] Somia Sahraoui LaSTIC laboratory, Computer Science Department University of Batna and Azeddine Bilami LaSTIC laboratory, Computer Science Department

University of Batna,"Compressed and Distributed Host Identity Protocol for End-to-End Security in the IoT"

[4] Surapon Kraijak, Panwit Tuwanut, King Mongkut's Institute of Technology Ladkrabang,"A survey on iot architectures, protocols, applications, security, privacy, real-world implementation and future trends"

[5] William M.S. Stout, Vincent E. Urias Sandia National Laboratories,"Challenges to Securing the Internet of Things"

[6] Arsalan Mohsen Nia, Student Member, IEEE and Niraj K. Jha, Fellow, IEEE,"A Comprehensive Study of Security of Internet-of-Things"

[7] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva,"Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues"

[8] Teng Xu, James B. Wendt, and Miodrag Potkonjak Computer Science Department, University of California, Los Angeles,"Security of IoT Systems: Design Challenges and Opportunities"

[9] Minela Grabovica, Drazen Pezer, SRdan Popic,Vladimit Knezevic,"Provided security measures of enabling technologies in Internet of Things (IoT): A survey"

[10] Surapon Kraijak, Panwit Tuwanut, Information Technology Faculty,King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand,"A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends"

[11] Prashanth Pomple Gurunath Chavan,"A Survey: Attacks on RPL and 6LoWPAN in IoT"

[12] Poulami Das, Debapriya Basu Roy, and Debdeep Mukhopadhyay,"Secure Public Key Hardware for IoT applications"

[13] S. Zamfir, T. Balan, I. Iliescu, F. Sandu, Department of Electronics and Computers, "Transilvania"University, Brasov, Romania,"A Security Analysis on Standard IoT Protocols"

[14] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva,"Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues"