www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 6 June 2017, Page No. 21802-21807
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i6.41

A Survey on Secure Communication Protocols for IoT Systems

Khaja Moinuddin[1,] Nalavadi Srikantha[2], Lokesh K S[3], Aswatha Narayana[4]

[1] Rao Bahadhur Y Mahabelwasharrppa Engineering College
Cantonment, Ballari, India
moinube@gmail.com

[2] Rao Bahadhur Y Mahabelwasharrppa Engineering College
Cantonment, Ballari, India
nalavadi@gmail.com

[3] Rao Bahadhur Y Mahabelwasharrppa Engineering College
Cantonment, Ballari, India
lokesh.kms@gmail.com

[4] Rao Bahadhur Y Mahabelwasharrppa Engineering College
Cantonment, Ballari, India
04aswa@gmail.com

Abstract* — The Internet of Things (IoT) integrates a large number of physical objects that are uniquely identified, ubiqui- tously interconnected and accessible through the Internet. IoT aims to transform any object in the real-world into a computing device that has sensing, communication and control capabili- ties. There is a growing number of IoT devices and applications and this leads to an increase in the number and complexity of malicious attacks. It is important to protect IoT systems against malicious attacks, especially to prevent attackers from obtaining control over the devices. A large number of security research solutions for IoT have been proposed in the last years, but most of them are not standardized or interoperable. In this paper, we investigate the security capabilities of existing protocols and networking stacks for IoT. We focus on solutions specified by well-known standardization bodies such as IEEE and IETF, and industry alliances, such as NFC Forum, ZigBee Alliance, Thread Group and LoRa Allianc.

Keywords — *Internet of Things; security; standard; authenti- cation; confidentiality; integrity.*

I. INTRODUCTION

The Internet of Things (IoT) represents the interconnection, through the Internet, of a large number of ’Things’– uniquely identifiable physical objects with sensing, communication and actuation capabilities. The term has been introduced by Kevin Ashton in 1999 in the context of chain supply management [1].

There are currently 5 billion smart objects connected to the Internet, and it is expected that there will be 25 billion by 2020 [3]. The integration of ’Things’ in the Internet is challenging because they may have characteristics such as limited memory, processing capacity and energy resources. Most products were initially developed as closed proprietary solutions that were incompatible with devices from other vendors [4]. The current trend however is towards standardized and interoperable protocols [5].

The number of IoT applications is growing. It includes smart home, healthcare monitoring, smart city, utilities, smart agriculture and animal farming, security and emergencies, smart water, industrial control, smart transportation, environment monitoring, etc. These IoT applications handle sensitive information regarding people and companies, which should not be disclosed to attackers and unauthorized persons.

As the field of IoT expands, attacks against IoT systems are growing in number and complexity [6]. Attacks against IoT systems aim to steal sensitive data, inject false information or disrupt the normal functionality of networks and services [2]. Recent attacks exploited vulnerabilities in smart refrigerators, in medical devices and smart cars [7]. Some attacks may involve considerable risk, for example, hacking medical devices may lead to the loss of human lives. Therefore it is important to ensure the security of critical IoT systems by providing protection against malicious attacks and failures.

In general, information security deals with confidentiality, integrity and availability (CIA) [1], [8], [9]. Schneier states that in the Internet of Things, attacks against integrity and availability are more important than attacks against confidentiality [7]. For example, in a smart home environment with a smart lock, it is more important to prevent an attacker from controlling the lock (to enter the house or block the door), than from finding out that someone has entered the house. In a similar manner it is more important to prevent an attacker from controlling your car, than from eavesdropping on your location. The main challenge in IoT security is to prevent attackers from obtaining control over the IoT system. This paper presents a survey of the most used communication protocols for IoT and their security capabilities. Although many research solutions for IoT provide security, they are generally not standardized or interoperable. In this paper, we focus on standardized protocols and networking stacks because interoperability is important for the large- scale adoption of the IoT. We investigate solutions specified by industry alliances, such as LoRa Alliance, ZigBee Alliance, Thread Group, NFC Forum, and leading standardization bodies, such as IEEE and IETF.

This paper is organized as follows. Section 2 presents the security requirements for IoT systems. Section 3 investigates the security capabilities provided by IoT communication protocols and networking stacks. Finally, Section 4 includes conclusions and future work.

II. SECURITY REQUIRNMENTS

Vasilomanolakis et al. [5] classify security requirements in five categories: Network Security, Identity Management, Privacy, Trust and Resilience.

1) Network Security: Network security requirements include: confidentiality, integrity, origin authentication, fresh- ness and availability [10]. In many IoT applications, such as healthcare or military applications, the sensitive data transmitted through the net- work should not be disclosed to unauthorized entities [6]. An attacker may eavesdrop on network traffic and extract sensitive information. Message confidentiality ensures that the contents of the message cannot be understood by anyone other than the desired recipients [10].

In critical IoT applications, the modification of sensitive data or the injection of invalid data may lead to the loss of human lives, for example in remote health monitoring systems [6]. An attacker may intercept network packets, modify their contents and inject them back into the network. In order to prevent the modification of messages by malicious or faulty devices, message integrity must be ensured. Authentication refers to two different security requirements: entity authentication and data origin authentication. Data origin authentication ensures that a message originates from a certain entity [11]. In order to prevent the injection of invalid data by malicious external devices, the IoT system must provide data origin authentication.

An attacker may inject false information into the network by recording messages and replaying them. Message fresh- ness ensures that attackers cannot re-inject information.

Some IoT applications rely on real-time data collection and correct functionality of services. An attacker may disrupt the functionality of the IoT system by blocking network packets or by causing services to fail. Availability ensures that the devices and services are reachable and operating correctly whenever needed, in a timely manner [8]. Availability is directly related to resilience to attacks and failures. This paper gives an overview of standardized and popular protocols that satisfy network security requirements.

2) Identity Management: Identity management represents an important challenge in IoT systems due to the complex relationships between entities (devices, services, service providers, owners and users) [5]. Identity management requirements include authentication, authorization, revocation and accountability [5].

Entity authentication refers to ensuring that an entity is who it claims to be [11]. More specifically, device authentication refers to verifying the unique and correct identity of the communicating devices in the IoT network .

Authorization allows authenticated entities to perform certain operations in the IoT system [6]. This means that each authenticated entity has permissions to perform specific operations. Revocation refers to removing the permission to perform an operation of a certain entity.

Accountability ensures that operations are clearly bound to authenticated entities. In large scale IoT systems, it is a challenge to provide accountability due to the considerable amount of devices, access delegation and multiple organizational domains [5].

3) Privacy: Privacy requirements refer to data privacy, anonymity, pseudonymity and unlink ability [5]. Privacy is an important challenge in IoT systems because users require the protection of their personal data because it provides information about their habits, interactions and location . In IoT, the collected data may be Personally Identifiable Information (PII): data that identifies a person [12]. Data privacy implies that the collected data does not expose information about a person, for example its identity [5].

Anonymity means that a certain person cannot be identified as a source of data or action [13]. In some cases IoT applications need to comply to the data minimization laws [5].

Pseudonymity is a tradeoff between anonymity and accountability, as it links the data and actions to a pseudonym instead of a person [13]. Unlinkability means that the data or actions related to the same person cannot be linked together [5].

4) Trust: Trust requirements deal with data trust and entity trust [5]. Other dimensions of trust are processing trust, connection trust and system trust [12].

In IoT, data may be collected by potentially untrusted devices. Trustworthy data can be obtained by applying different algorithms like data aggregation or machine learning [5].

Entity trust refers to the expected behavior of entities, such as devices, services and users. Device trust relates to the interaction with reliable devices [12] and can be established through trusted computing [5].

5) Resilience: Large scale IoT systems are prone to attacks and failures due to the complexity and variety of hardware and software. Therefore, it is important to ensure resilience and robustness against malicious attacks and failures [5].

Intrusion detection and prevention systems provide protection against malicious attacks [10]. Failover and recovery mechanisms ensure resilience and help maintain normal operation [5].

III. COMMUNICATION PROTOCOL AND NETWORKING STACKS

This section provides in-depth investigation of IoT communication protocols and networking stacks and their security capabilities.

A. IEEE 802.15.4

The IEEE 802.15.4 standard [14] was designed as a basis for a protocol stack oriented towards short range, low data-rate and energy efficient communication. It was originally introduced in 2003, with several revisions and additions over the years, and defines the physical (PHY) and Medium Access Control (MAC) layers for short range communications at 250Kbps. The latest version of the standard was released in 2015 and includes previously released amendments that add additional PHY layers and modifications to the MAC layer which better support industrial markets.

While in IEEE 802.15.4 the PHY layer does not offer any security, the MAC layer provides multiple security levels, as described in Table I. All security services as based on the AES-128 block cipher [15] coupled with the CCM* mode of operation [16]. Although the standard specifies security as optional, the effect of having AES-128 in the specification is that most IEEE 802.15.4 compatible hardware platforms (the popular CC2420 or the newer CC2520 transceivers from Texas Instruments or the ATmega128RFA1 and variants SoC from Atmel) implement some form of hardware acceleration for AES-128. This ensures that the energy cost of enabling security on these platforms is minimal. Having almost ubiquitous support for the AES-128 cipher in hardware means that higher layer protocols can also define their security services on top of AES-128 with minimal impact on the energy efficiency of the device. Even if MAC layer security is not employed in a given scenario, the device can still benefit from security at the network or application layers.

In IEEE 802.15.4 communications, secure MAC frames are identified by the Security Enabled flag inside the Frame Control field. This flag also signals the presence of the Auxiliary Security Header which contains information about how the frame is to be secured. The Security Level field selects one of the security levels from Table I applied to the frame. A security level of 0 means that the frame is sent unsecured, while security levels from 1 to 3 and 5 to 7 mean that the frames are protected by a Message Integrity Code of the given length, ensuring integrity and origin authentication. These properties apply to the entire MAC frame, except the Frame Check Sequence. Security levels 4 to 7 provide encryption for the payload part of the MAC frame, ensuring its confidentiality. All CCM* operations also use a nonce value of 13 bytes formed from the concatenation of the frame's Source Address and Frame Counter and Security Level fields from the Auxiliary Security Header which ensures freshness, as well as semantic security for the encrypted payload.

The IEEE 802.15.4 specification does not define how to do key management. The AES-128 block cipher uses 128 bit symmetric keys, but the generation, distribution and replacement of those keys is left for the upper layers. The standard does however include a key storing system inside the MAC PAN Information Base and a way of implementing a form of access control at the MAC layer, with pair-wise keys or group keys, through the use of the MAC PIB and the Key Source field inside the Auxiliary Security Header.

B. Wi-Fi

WiFi communications are defined by the 802.11 family of standards, with the first one introduced in 1997 [17]. Popular older standards include 802.11a, 802.11b, and 802.11g. Most devices support the newer standards 802.11n [18] and 802.11ac [19].

WiFi networks often operate in congested wireless environments, which might lead to interference and degradation of performance. WiFi communications use frequency bands around 2.4 GHz and 5 GHz; devices operate on frequency ranges centered on pre-set channels located within those bands. The list of available channels depends on geographical regions. For example, in the 2.4GHz range, 11 channels exist in the US while 13 channels exist in Europe. The channels are 5MHz apart, with channel 1 centered at 2.412GHz.

WiFi standards use different channel widths. For example, 802.11n can use channels with a width of up to 40MHz while 802.11ac mandates the use of channels with a width of 80MHz (and can even reach 160MHz). If two WiFi network channels overlap, interference can lead to lower throughput or even loss of connectivity. Wireless devices often support dynamic selection of channels, but in severely congested industrial environments planning which frequencies are in use can lead to better performance.

C. NFC

Near Field Communication (NFC) is a set of short-range communication technologies, operating over electromagnetic fields at a frequency of 13.56MHz over distances of about 10cm. NFC specifications are developed by the NFC Forum, an association composed of companies with interest in NFC. NFC operation is described in standards ISO/IEC 14443 [21], ISO/IEC 18092 and JISX6319-4 .

NFC devices communicate by generating electromagnetic fields. In an active communication, both devices generate their own fields. In a passive communication, one device transmits data by modulating the field generated by the active device.

NFC is used to read and write information stored in tags. Five types of tags are currently supported by the NFC forum, with types 1, 2 and 4 described in ISO/IEC 14443, type 3 in JISX6319-4 and type 5 in ISO/IEC 15693 [22].

D. LoRaWAN

Low-Power, Wide-Area Networks (LPWAN) are designed to integrate billions of devices in the Internet of Things[18]. LPWAN technologies complement short range and cellular networks, by providing long battery life (up to 10 years), large communication range and low cost devices [23].

Long Range Wide-Area Network (LoRaWAN) is a LP-WAN optimized to have large capacity and range, and low energy consumption and cost. LoRa Alliance is an open, non-profit association of members that collaborate to develop LoRaWAN open standard [24].

LoRaWAN networks have a star-of-stars topology, in which end-devices send messages to gateways, which relay these messages to a central server [24]. End-devices use single-hop LoRa communication with one of the gateways. The gateways communicate with the server

DOI: 10.18535/ijecs/v6i6.41

through IP connections.

LoRaWAN standard includes two security layers: one for the network and one for the application. Network-layer security ensures device authentication and Application-layer security ensures the protection of the application data (confidentiality, integrity).

When an end-device is added to the LoRaWAN network, it needs to be personalized and activated [24]. Activation of an end-device can be performed either through Over-The-Air-Activation (OTAA) or through Activation by Personalization (ABP). OTAA is executed when the device is deployed or reset, and ABP includes both personalization and activation. OTAA enables devices to execute a joining procedure before sending any data messages in the network. For this, the end-device needs to be personalized with the following information before the join procedure: a globally unique device identifier (DevEUI), an application idenitifier (AppEUI) and an AES-128 key (AppKey).

E. Z-Wave

Z-Wave is a low-power wireless communication protocol, designed by Sigma Designs, Inc., for remote control applications in residential and small-size commercial environments [25]. The protocol specification and software development kit are not open and are available only to the device manufacturers that signed a contract with Sigma Designs, Inc. Z-Wave is a complete protocol stack that covers all layers, from physical to application layer.

At the physical layer, Z-Wave operates in the Industrial, Scientific and Medical (ISM) radio frequency band, using low-bandwidth data communication frequencies: 868.42 MHz in Europe and 908.42 MHz in the United States. It adheres to the ITU-T G.9959 PHY and MAC layer specification for sub GHz radio communications. This way, it avoids interference with the wireless technologies in the 2.4 GHz range (Wi-Fi, Bluetooth, ZigBee, etc.). Z-Wave provides a range of 30 meters for point-to-point communications and allows a transmission rate of up to 100 kbps [25].

A Z-Wave mesh network consists in a controller device and up to 232 nodes. Each controller device has a unique 32-bit Home ID, which is the identifier of the Z-Wave network. This ID is written by the manufacturer on the chip and cannot be changed in software. This prevents malicious controller devices from using a spoofed Home ID and collecting information from homes. In addition, controller devices do not support promiscuous mode, so they are not able to intercept all network traffic.

When secure transmission mode is enabled, the frame payload is encrypted and an 8-byte authentication header is added at the end of the frame, before the checksum. The checksum algorithm is described in the ITU-T G.9959 standard.

F. Bluetooth Low Energy

Bluetooth Low Energy (BLE) is a technology introduced by the Bluetooth Special Interest Group (SIG) in the 4.0 version of the Bluetooth protocol specification. Also known as Bluetooth Smart, it reduces energy consumption and device costs when compared with classic Bluetooth. The Bluetooth specification [26] defines a complete communication stack for BLE composed of the physical layer, the link layer, the Logical Link Control and Adaptation Protocol (L2CAP), which multiplexes the upper layer protocols, the Attribute Protocol (ATT), which defines a way of discovering and transporting attributes (values) and the Generic Attribute Profile (GATT), which defines a framework based on ATT for defining services. The stack is split between the Controller, which implements the physical and link layers, and the Host, which implements the upper layers. These two components communicate with each other using the standardized Host Controller Interface.

G. Thread

Thread is an open standard protocol stack that provides low-power, low-cost, wireless IPv6 communication for smart home devices [27]. It has been designed by Thread Group, which is an Internet of Things standards group that includes Google’s Nest Labs, Samsung, ARM, Freescale, and others [40]. Thread protocol stack includes: IEEE 802.15.4 PHY and MAC layers, 6LoWPAN, Distance Vector Routing (DVR), UDP, and DTLS.

The Thread standard is based on IEEE 802.15.4 PHY and MAC layers [14], using the 2.4 GHz frequency band and 250 kpbs. The MAC layer provides message confidentiality and integrity protection based on keys that are obtained by the higher layers of the stack. The network layer is build on top of this MAC layer and provides reliable end-to-end communication [27]. Thread ensures data confidentiality, integrity, and authentication.

In Thread the IEEE 802.15.4 MAC layer secures frames using a network-wide key. This provides weak security and is not the only method of securing the messages. However, the network-wide key is used to differentiate between a Joiner device and an authenticated and authorized Thread device. This key will be delivered securely (using a Key Encryption Key) to a Joiner device.

H. ZigBee

ZigBee is a wireless communication specification [28] defined by the ZigBee Alliance for use in sensor networks applications. It provides a complete protocol stack to foster interoperability between devices from different manufacturers. The ZigBee stack builds on top of the IEEE 802.15.4 standard, which provides the PHY and MAC layers. This makes the ZigBee specification compatible with all 802.15.4 hardware. ZigBee defines a network layer (NWK) which supports star, tree and mesh routing and a framework for building the application layer composed of the application support sub-layer (APS) and the ZigBee device objects (ZDO), which the application uses to build its own application objects. As for the communication stack, the security of ZigBee is built on top of the security services provided by the IEEE 802.15.4 standard [28]. Although ZigBee doesn’t directly use the MAC layer security defined in 802.15.4, it uses the same AES-128 block cipher and CCM* mode of operation to secure transmissions at both the NWK and APS layers. The principle that ”the layer that originates a frame is responsible for initially securing it” is employed, which means that if a NWK command frame needs protection, the protection will be applied at the NWK layer. Because the specification is targeted at low-cost devices, no security separation is assumed between stack layers. The consequence of this is that the same key can be shared by multiple layers, decreasing complexity and storage costs associated with security keys. The ZigBee specification also defines a set of security levels that mirror the security levels of IEEE 802.15.4 and, depending and the level, provide the same protections (i.e integrity, origin authentication, confidentiality and/or freshness) . Unlike the 802.15.4 standard, in ZigBee the security level is common to the whole network and cannot be changed on a per frame basis.

IV. CONCLUSIONS

As the internet of things continues to expand, the diversity and complexity of IoT applications increases. such networks are vulnerable to attacks that aim to steal sensitive information, take control over devices and disrupt services. many protocols and networking stacks for IoT have been developed. some of them are standardized, and provide interoperability between devices and connectivity over the internet. they have been specified by standardization bodies such as ietf and ieee or by industry alliances, such also rawan alliance and thread group.

This paper analyzed the security requirements specific to IoT systems, by taking into consideration network security, identity management, privacy, trust, and resilience. next, the standardized protocols and networking stacks for IoT, and the mechanisms they provide for satisfying communication security requirements are investigated. we presented the mechanisms that ensure data confidentiality, integrity, origin authentication and freshness for each IoT technology. A large selection of IoT technologies was analyzed, from single-layer protocols (such as 6lowpan) to full protocol stacks (such as thread). their functionality and security capabilities are presented, and summarizes the protocol layers and security requirements that are covered by the investigated technologies.

As a future work, we would like to investigate standardized solutions for IoT that meet other security requirements, such as trust and resilience. another interesting area of research would be how the security properties of the various specifications transfer to practical implementations, given the limitations of IoT devices and the possible variations inherent in a complete stack.

REFERENCES

[1] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT),” International Journal of Computer Applications, vol. 111, no. 7, pp. 1–6, 2015.

[2] V. Bhuvaneswari and R. Porkodi, “The internet of things (IOT) applications and communication enabling technology standards: An overview,” in *International Conference on Intelligent Computing Applications, ICICA 2014*, 2014, pp.324–329.

[3] “Gartner says 4.9 billion connected ”things” will be in use in 2015,” 2014. [Online]. Available: http://www.gartner.com/ newsroom/id/2905717

[4] I. Ishaq, D. Carels, G. Teklemariam, J. Hoebeke, F. Abeele, E. Poorter, I. Moerman, and P. Demeester, *IETF Standardization in the Field of the Internet of Things (IoT): A Survey*, 2013, vol. 2, no. 2. [Online]. Available: http://www.mdpi.com/2224-2708/2/2/235/htm.

[5] E. Vasilomanolakis, J. Daubert, and M. Luthra, “On the Security and Privacy of Internet of Things Architectures and Systems,” in *Secure Internet of Things (SIoT2015)*, 2015, pp. 49–57. [Online]. Available: https://www.informatik.tu-darmstadt.de/fileadmin/user_________ upload/ Group TK/filesDownload/Published_Papers/SIoTpaper.pdf.

[6] K. Lingaraj, N. Sreekanth, M. Kaja, K. M. S. Lokesh, K. Prashanth, and V. B. Nagaveni, Information Security Emergency Plan Management System. Singapore: Springer Singapore, 2017, pp. 129–137.

[7] “Real-world security and the internet of things,” 2016.

[8] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of Things (IoT) Security : Current Status , Challenges and Prospective Measures,” in *10th International Conference for Internet Technology and Secured Transactions (ICITST)*,2015, pp. 336–341.

[9] Z. Z.-K., C. M.C.Y., and S. S., “Emerging security threats and countermeasures in IoT,” in ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 2015, pp. 1–6. [Online]. Available: http://www.scopus.com/inward/record. url?eid=2-s2 84942523308*{*&*}*partnerID=40*{*&*}* md5=3c4a207d85900014161844 68e21e3d27

[10] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp.2–23, 2006. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4109893

[11] A. Barki, A. Bouabdallah, S. Gharout, and J. Traore, “M2M Security: Challenges and Solutions,” *IEEE Communications Surveys & Tutorials*, no. c, pp. 1–1,2016.

[12] J. Daubert, A. Wiesmaier, and P. Kikiras, “A view on privacy& trust in IoT,” in 2015 IEEE International Conference on Communication Workshop, ICCW 2015, 2015, pp. 2665–2670.

[13] A. Pfitzmann and M. Hansen, “A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,” Tech. Rep.,2009.

[14] *Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Std. 802.15.4, 2011. [Online].

[15] K. Lingaraj, R. V. Biradar, and V. C. Patil. A survey on middleware challenges and approaches for wireless sensor networks. In 2015 International Conference on Computational Intelligence and Communication Networks (CICN), pages 56–60, Dec 2015. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CICN.2015.20.

[16] K. Lingaraj, R. V. Biradar, and V. C. Patil. A survey on mobile-agent middleware design principals and itinerary planning algorithms. In 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pages 749–753, Oct 2015. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICATCCT.2015.7456983.

[17] IEEE, “802.11-1997 standard,” Tech. Rep.

[18] K. Lingaraj, R. V. Biradar, and V. Patil, “Eagilla: An enhanced mobile agent middleware for wireless sensor networks,” Alexandria Engineering Journal, pp. –, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1110016817300947

[19] Lingaraj.K, Ranjana.V, and Pruthvi.H.M, “An evolutionary based data mining technique in engineering faculty evaluation using weka,” International Journal of Computer Applications Technology and Research, vol. 3, no. 7, pp. 494–499, 2014. [Online]. Available:http://www.ijcat.com/archives/volume3/issue8/ijcatr03081002.pdf

[20] E. Tews and M. Beck, “Practical attacks against wep and wpa,” in *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, pp. 79–86.

[21] ISO, “ISO/IEC 14443,” Tech. Rep.

[22] ISO, “ISO/IEC 15693,” Tech. Rep.

[23] “LPWA Technologies. Unlock New IoT Market Potential.” LoRa Alliance, Tech. Rep. November, 2015.

[24] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, “LoRaWAN Specification,” LoRa Alliance, Inc., Tech. Rep., 2015

[25] “About z-wave technology.”

[26] *Specification of the Bluetooth System*, Bluetooth SIG Core Specification, Rev. 4.2, Dec. 2014. [Online].

[27] "Thread Stack Fundamentals," Thread Group, Tech. Rep.,2015.

[28] G. Dini and M. Tiloca, "Considerations on security in zigbee networks," in *International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC).* IEEE, Jun. 2010, pp. 58–65.

[29] Linga Raj. K, Nagaveni V Biradar and Girisha. H. Article: Application of Wireless Communication Tools in Managing Construction Projects. International Journal of Computer Applications 73(5):15-19, July 2013. https://doi.org/10.5120/12736-9608.