IoT Security : ZWave and Thread

Ishaq Unwala
Computer Engineering
University of Houston Clear Lake
Houston, USA
Unwala@UHCL.edu

Zafar Taqvi
Computer Engineering
University of Houston Clear Lake
Taqvi@UHCL.edu

Jiang Lu
Computer Engineering
University of Houston Clear Lake
Houston, USA
LuJ@UHCL.edu

***Abstract*— This paper reviews the security aspects of two Internet-of-Things (IoT) protocols, *Z-Wave* and *Thread*. *Z-Wave* is one of the oldest and most commercially successful IoT protocol, while *Thread* is one of the most recent protocols. As millions of IoT systems are installed for home and industrial automation, the security of these IoT systems is a concern. There is a potential for these IoT systems to be misused. This paper looks at security challenges for an IoT system. The security features of the IoT systems are spread across many parts of the IoT protocols. Paper discusses different attacks types on the IoT systems and the manners in which the protocols handle them. One of the most venerable times for an IoT system is when a new device is added to the IoT system. To avoid an intruder from getting access, the new device must be authenticated. Authentication of new network devices is discussed for both the protocols. IoT protocols are complex and the security aspects are also very complex, this paper should serve as a starting point to further study these and other IoT protocols.**

Keywords- Internet-of-things, IoT, Z-Wave, Thread, Thread group, private area network

I. INTRODUCTION

In recent years Internet-of-Things (IoT) [1] has seen exceptional growth with projections for continuous growth in future [2]. IoT security has become a major issue with recent actual, and theoretical, cyber attacks using IoT devices [3] [4] [5] [6]. In order for public and companies to confidentially install IoT systems they need to feel that they have the full control over their devices, they need to know their data is safe and secure. This paper is going to compare security aspects of the two very different protocols, *Z-Wave* and *Thread*. *Z-Wave* is one of the oldest IoT protocol and *Thread* is one of the newest protocol. *Z-Wave* is a proprietary protocol, some details have been released by the manufacturer and others have been discovered by the researchers. *Thread* is an open protocol, built mainly on existing standards. *Thread* specification is available from the Thread Group Inc. A brief comparison of *Z-Wave* and *Thread* was presented in [8]. *Z-Wave* and *Thread* both have been earlier discussed by authors in [7].

There are other wireless systems, besides those based on IoT protocols. These wireless systems are available in the market for home and industrial automation, for example, wireless gate openers [9] and security cameras [10]. Some of these systems are analogue and others are digital. Generally, these systems are proprietary, with unknown reliability and security protocols, they are not interoperable between different vendors, and most cannot operate from across the internet.

A. Internet of Things

Internet of Things (IoT) consists of various devices connected to each other through Internet. IoT consist of sensors, controllers, actuators, communication and computing devices. Sensors collect the data, which is communicated to the computing resource, and depending on the system requirements, the response is communicated back to the actuators for action. For example, a temperature sensor communicates the local temperature, through internet, to the Cloud computing resource, if the Cloud computing program determines an action is necessary, it communicates back, through internet, to the actuator to either turn on or off the local heating or cooling system. Many types of sensors are available, for example, video, audio, temperature, humidity, light, motion, chemical detectors, etc. Similarly, many actuators are also available, for example, switches, solenoids, valves, motors, flow regulators, etc.

1) IoT Private Area Network

There are a number of IoT protocols in use today. A partial list of IoT protocol includes *Z-Wave*, *Zigbee*, *AllJoyn*, *Thread*, etc. Interoperability between these protocols is also major issue, thus creating problems in system installation and maintenance. One common feature in all the IoT protocols is a local Private Area Network (PAN).

Private Area Network (PAN) is a local wireless network. PAN consists of all the sensors, actuators, communication devices and a gateway router to internet. Each sensor, actuator, or network router acts as a node in the PAN. The communication between the nodes is through wireless radios, which form the edges of the PAN topology. Each node has different capability, some nodes are end-nodes and either transmit or receive data, other nodes can routing the data within the PAN. The PAN router nodes can transmit and receive data, these nodes act as PAN routers. Every PAN has at least one node that acts as a gateway node to internet. This gateway node is also called a Border Router (BR). The BR connects to the PAN router(s) on one side and internet on the other side, allowing data to pass from

2166-5478/18/$31.00 ©2018 IEEE
DOI 10.1109/GreenTech.2018.00040

PAN to internet and back. Except for BR, none of the PAN nodes can directly communicate nor are directly accessible from internet.

Some of the PAN topology in use are Peer-to-Peer connectivity, Star connectivity and Mesh connectivity [11]. All the sensors, actuators, controllers, PAN routers and BR are part of the PAN and can communicate with each other. To connect to a device or resource, like Cloud computing, outside the PAN, all communication passes through the BR. The PAN wireless connectivity is specified by the protocol, includes radio frequencies, data speed, encoding and other parameters.

In our case, both *Z-Wave* and *Thread* have chosen Mesh topology for their PAN. Mesh is a flexible, reliable and scalable topology.

II. Internet of Things Security Challenges

Attack on an IoT system can be mounted from three possible venues. First, attack can be on the data and computations performed in the Cloud. Next, attack can be mounted through the IoT gateway. Finally, the attack can be mounted on an IoT PAN directly from close proximity.

Security considerations for Cloud computing are addressed in [12]. The IoT PAN is connected to internet through the internet gateway. An attack on the IoT PAN can be mounted through this gateway. To manage and reduce the opportunities to mount an attack, IoT PAN usually allows only a limited number of gateways, normally just one. The security measures taken by the user to protect the home network, including LAN wired and wireless connections, from internet attack also protect the IoT PAN. Finally, as mentioned earlier the IoT PAN can also be attacked directly from a close proximity. Securing IoT PAN from local attacks will be the focus of this paper.

It is important to remember that most of the IoT devices are operating under low power regime. These low power restrictions mean that the IoT devices are very small. They have very low performance, small memories, low energy radios and sometimes limited operating time due to battery capacities. Even with these limitations they are expected to manage these security challenges listed below.

- Authentication. A device credentials must be verified before it can access the PAN resources.
- Authorization. It is assumed that an authenticated device has authorization, i.e. permissions and rights, to access PAN resources.
- Privacy. Privacy is an extremely important requirement for an IoT system. Since all the IoT data in the PAN is wirelessly transmitted it makes it highly venerable eavesdropping. User data (sensor, video, audio) must not be disclosed to unauthorized and unauthenticated receivers.
- Confidentiality. The data must be encrypted to protect the content of the message.
- Data Integrity. IoT data is transmitted in multiple hops from a device to router or router to device. If the data is not adequately protected with encryption it can lead to a man-in-the-middle attack. Encryption ensures that the data has not been manipulated or altered while in transit.
- Trust. How much can users trust the IoT network? This question is being actively considered by a number of researchers. These researchers are using concepts from distributed systems and social networks to construct trust models for IoT networks. [13] [14] [15].
- Physical security. IoT devices are at times exposed to physical hazards such as intentional violence, exposure to natural and man-made hazards of moisture, chemicals, weather extremes, vacuum, etc. While physical security of the IoT devices is an important aspect of IoT deployment, it is beyond the scope of this paper. It is expected that deployment of IoT would consider barriers to access, and hardened against impacts, protected from expected hazards for long and reliable operation of the IoT system.

IoT PAN is vulnerable to some well known attacks that are seen in any computer network. Here is a list of attack according to CIAA (confidentially, integrity, authentication and availability) model [16] [17] [18].

- *Distributed Denial of Service (DDOS)*. In DDOS the PAN network is bombarded with unauthorized messages. It is easy to overwhelm IoT devices with DDOS due to their constrained resources. There is very little the protocols can do to work around this situation. This particular attack makes access and control of IoT devices difficult. Although, in this attack network data is not compromised, sensor data and device control can be delayed or lost since it cannot be transmitted to its destination in time.

- *Man-in-the-middle attack*. A Man-in-the-middle attack happens when an adversarial node sneaks in between the PAN nodes to read or insert fake messages. The only real way an adversarial node can become a part of the PAN is if PAN is unsecure or the network security key has been compromised.

  When a device joins the network, the device must be authenticated and then provided a network key. Possessing the network key signifies that the

device is an authorized member of the PAN and it can legitimately send and receive PAN messages.

Providing network key to all the devices is a very difficult issue when many vendors are involved. If all vendors use the same network key and the key leaks out, all devices installed in the past and presently in market will become insecure. The chances for leak are very high.

There are a number of forms Man-in-the-middle attack can manifest itself. Some common forms are listed below.

- *Sinkhole attack*. An adversarial node in the network can attract all the traffic to steal or destroy data.
- *Black-hole*. A milder case of sinkhole attack where all data traffic received at the node is deleted.
- *Selective forwarding attack*. A particular case of black-hole attack, where only a few selective messages are allowed to pass through.
- *Router map attack*. An adversarial node corrupts the router mapping.
- *Rank attack*. An adversarial node changes the node rank. Device either increases or decreases its rank to affect traffic. Higher rank creates a sink-hole. Lower rank prevents traffic from arriving, effectively cutting off a part of the PAN.
- *Version number attack*. In this case the version number in the routing object is changed to affect the message routing.

In order to avoid Man-in-the-middle attack, *Z-Wave* uses a security protocol it calls S2. Similarly, *Thread* uses a security protocol called Commissioning. These two security protocols are discussed in Section IV.

- *Replay attack*. Old messages can be replayed at a later time to cause unintended behavior. These attacks can be prevented by use of Nonce, i.e. single use keys. *Z-Wave* S2 protocol addresses this concern by exchanging nonce list. *Thread* addresses this by using key rotation and message sequencing.
- *Third party attack*. If a third party can access user information, like video feed, it can be used for malicious activities. This particular attack is addressed by encrypting all communication in the PAN or passing through the gateway.

III. Network Stack

This section will discuss the network stack for both the IoT protocols *Z-Wave* and *Thread*.

Initially, *Z-Wave* was not based on an established standard. But some aspects of *Z-Wave* have now been opened to public, like *Z-Wave* radio under (ITU-T) G.9959 [19], developer resources [20], and security paper [21].

Thread protocol is essentially based on established standards and RFC, as can be seen in Figure 1.

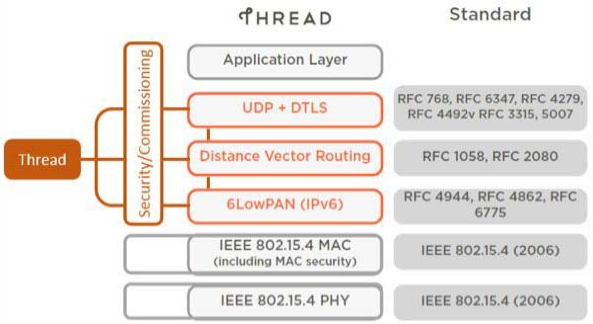

Figure 1. *Thread* Protocol stack [22]

A. Physical and Data Link Layer (PHY and MAC)

Although, Physical and Data link layers for both *Z-Wave* and *Thread* has been discussed by the authors in [7], some key aspects are repeated here for completeness.

The PHY layer specifies the physical aspects of the connection, in case of both *Z-Wave* and *Thread* the connections are established with wireless radios. The MAC layer uses the PHY connections for specification of communication frames.

1) Z-Wave Radio

Z-Wave radio was propriety till 2012, when it was added to International Telecommunication Union (ITU-T) as an open and public standard G.9959 [19]. *Z-Wave* chose sub-GHz frequencies to avoid heavily used 2.4GHz, and provide a better range for low power devices. Since there is no global sub-GHz frequency available *Z-Wave* devices have to operate at different frequencies in different parts of the world [8]. For USA, *Z-Wave* devices operate at the frequency of 908.4MHz, for Europe and parts of Asia the operating frequency is 868.4MHz, and for Australia and Japan the operating frequency is 919MHz. The radio on *Z-Wave* ICs can be tuned to any of these frequencies. The antenna filter is localized and provided as per local market frequency requirement [8].

The *Z-Wave* data encoding depends on the operating data rate. The Manchester Encoding is used at 9.6kbit/s data rate. At higher data rates of 40kbits/s and 100kbits/s, *Z-Wave* devices use NonReturnZero (NRZ) encoding.

2) Thread Radio

All *Thread* devices support one or more physical wireless interface based on IEEE 802.15.4 (2006), specifically those sections relating to 2450MHz. Although it is congested, this particular frequency was chosen for a number of reasons, global availability, readily available radio silicon, no regulatory delay and fast time to market.

3) Z-Wave (MAC)

Every *Z-Wave* PAN has a unique Home-ID embedded in the *Z-Wave* controller. This Home-ID is set at manufacturing and in not changeable by the user. Within a *Z-Wave* PAN every device is allocated a Node-ID by the controller. So every node in the PAN can be uniquely identified with combination of a Home-ID and a Node-ID. If there are multiple *Z-Wave* controllers operating within range of each other, each device will know from Home-ID to which controller it belongs.

The basic *Z-Wave* MAC frame is shown below [8]:

P	SOF	User-Data	EOF

P - Preamble (ten or more repeats of 01)
SOF – Start Of Frame (1-byte)
User-Data (12-64-bytes)
EOF - End Of Frame (1-byte)

In a *Z-Wave* Singlecast frame the User-data section consists of sub-field shown below [8]:

User-Data (Channel 1+2)						
H-ID	Src	FC	FL	Dst	App. Data	CS

User-Data (Channel 3)							
H-ID	Src	FC	FL	SQ	Dst	App. Data	CRC

H-ID - Home-ID (4-bytes)
Src – Source Node-ID (1-byte)
FC - Frame Control (2-bytes)
FL – Frame Length (1-byte)
SQ – Sequence number (1-byte)
Application Data (variable bytes)
Dst – Destination Node-ID (1-byte)
CS - CheckSum (1-byte) or CRC (2-bytes)
CRC – CRC-16

The Broadcast, Multicast, Routing and Explorer frames use different fields within User-Data section [8]. Application data can also be used to send commands and parameters, or node information. The application data can be secured by AES-128 encryption, as shown below [8]:

App. Data		
Sec-ID	WRAP	Secure App data

4) Thread (MAC)

Thread uses IEEE Std.802.15.4 (2006) [11] for its MAC layer specification with some modifications. Certain MAC capabilities and frames are required to be supported, while others are not permitted.

Capability	Support
Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)	Required
Active and Energy Detect scan	Required
Exchanging MAC data ACK	Required
Data request frames	Required
Exchanging beacon frames	Required
MAC frame security	Required
Periodic Beacon enabled	Not Permitted
Guaranteed Time Slots	Not Permitted
Generating or interpreting: association request or response, disassociation request, PAN ID conflict frames	Not Permitted
PAN coordinator frame	Not Permitted

MAC frame from IEEE 802.15.4-2006 (Section 7.2.1) [11]:

FC	SQ	DstPID	Dst	SrcPID	Src	AuxSec	UD	FCS

FC- Frame control (2-bytes)
SQ – Sequence number (1-byte)
DstPID - Destination PAN ID (0/2–bytes)
Dst – Destination address (0/2/8-bytes)
SrcPID – Source PAN ID (0/2-bytes)
Src – Source address (0/2/8-bytes)
AuxSec- Auxiliary Security Header (0/5/6/10/14-bytes) it contains these fields Security Control, a Frame Counter, and a Key Identifier
UD – User data (variable bytes)
FCS – ITU-T CRC-16 (2-bytes)

Thread also requires a 6LoWPAN adaptation layer to manage IPv6 packets, based on RFC 4944 (Transmission of IPv6 Packets over IEEE 802.15.4 Networks), updated by RFC 6282 (Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks) with minor modification.

IV. AUTHENTICATION OF NETWORK DEVICES

To add node devices to any private area network, the new devices have to be authenticated. After authentication the device is provided with network encryption key, routing table and other information, thus authorizing the device to

participate in the PAN activities. *Z-Wave* terminology for the process of adding and removing a device from PAN is "inclusion" and "exclusion" correspondingly. *Thread* terminology for adding and removing a device is "commissioning" and "decommissioning".

A. Z-Wave

Although *Z-Wave* always has made encryption available, for example, early *Z-Wave* series 100 had TDES (Triple Data Encryption Standard) [23]. *Z-Wave* has historically left up to the vendors to use the encryption [24]. As not all vendors used the encryption option, there have been a number researchers showing the venerability of *Z-Wave* devices [25] [26]. *Z-Wave* has started taking actions. Recently, *Z-Wave* devices have been evaluated by UL for security applications according to press release by Sigma Design, "*Z-Wave* modules models ZM5101, ZM5202, and ZM5304 with protocol SDK version 6.60 have been evaluated to UL's standards for home security" [27]. As security of the IoT devices is become a bigger issue, with millions on IoT devices captured by BotNet for DDOS [3], *Z-Wave* has announced that S2 security framework is now mandatory for certification [28]. S2 security framework, discussed below, is based on AES-128 for data links and ECDH for key exchange [21] [29].

The *Z-Wave* S2 protocol divides the network into three security classes S2 Access Control, S2 Authenticated and S2 Unauthenticated. Devices joining the *Z-Wave* PAN must fall into one of these classes. Each S2 security class has its own network key, thus there are three different AES-128 keys [21]. Access Control is the most secure class and is used for devices, like door lock and garage openers, where access control is critical. Authenticated class is next lower level and is used for normal household devices like sensors and light control. Unauthenticated class is lowest level and is used for devices which due to constrained interface cannot be fully authenticated. A device can belong to multiple security classes. These device need to use the key appropriate to connect to other devices in each class.

To receive a network key from the controller, the controller and device have to establish a secure communication. However, without an encryption key a secure communication cannot be established. To resolve this problem, *Z-Wave* uses Elliptic Curve Diffie-Hellman (ECDH) technique. ECDH allows an exchange of temporary keys for secure communication [21] [30]. Once using the ECDH temporary keys a secure connection is established, the network key can be sent securely to the device. On the new Series 500 processors, the network keys are kept in the on-board flash memory. This flash memory is clear after a new firmwire is loaded, to avoid someone reading the network key.

Z-Wave controller, which connects to Internet on one side and PAN on the other side, uses TLS (Transport Layer Security, RFC 5246) to connect to all the LAN and WAN host systems [21]. In case of multiple controller system, DTLS (Datagram Transport Layer Security, RFC 6347) is used to communicate to the other controller [21].

B. Thread

To allow a device to join *Thread* PAN, device must be commissioned by the Commissioner. However before that happens, the Commissioner device itself must be first authenticated.

The Commissioner is usually a device in control of a human administrator, typically a mobile phone with WiFi connectivity, or a *Z-Wave* remote control. In order for the Commissioner and *Thread* PAN to discover each other for the first time, the BR broadcast's its availability by whatever means appropriate. The BR connects *Thread* PAN to the Internet and LAN. The Commissioner has to first present its credentials, a passphrase 6-255 bytes. This passphrase is used in generating a Pre-Shared Key for Commissioner (PSKc) (using PBKDF2, RFC 2898). PSKc is then used to establish a secure Commissioner Session using DTLS or TLS. Before the Commissioner is fully authenticated, an approval of PAN Leader node is required. Once approved, the Leader will update its internal dataset with the Commissioner credentials and propagate the PSKc to all nodes in the PAN. Now that the Commissioner has been authenticated, the authentication of a generic device will be discussed next.

A new device desiring to be part of a *Thread* PAN is called a Joiner. A Joiner, that is not part of any PAN, can transmit an unsecured Discovery request with a number of options for Source address, Destination PANID, etc. The Discovery request message frames are specified in Mesh Link Establishment [22].

The *Thread* Joiner Routers (JR) and Router Enabled End Device (REED) nodes must process the Discovery requests and send back Discovery responses frame, based on the original message frame data.

However, to protect against DDOS attack (flooding the PAN with Discovery requests), JR and REEDs must process *Thread* PAN messages before Discovery requests. The JR and REEDs must also minimized the resources given to Discovery requests and dispatch Discovery responses as quickly as possible to free resources, and if needed JR and REEDs can stop responding to Discovery requests completely.

If the Joiner does not received a Discovery response before the watchdog timer expires, it has to assume that the joining

the PAN is disabled. If the Joiner receives Discovery response with "Steering Data", it will include the UDP ports. The Joiner, using unsecure channel, will send records required on the specific UDP port, given in the Discovery response, using DTLS to the JR or REED. The JR will relay these to BR, which will further relay this to Commissioner in a Commissioner Session. The JR and the BR do not know the contents of the messages between the Commissioner and the Joiner. Commissioner can closed the Joiner Session at any time and for any reason, thus rejecting the Joiner. After trading messages with Joiner, if the Commissioner is satisfied with the Joiner responses than it will authenticate it. After authentication Joiner may require some configuration by Commissioner, or provisioning from appstore or from a URL. The Joiner Session is ended by Commissioner by sending Accept and providing a KEK (Key Encryption Key) using DTLS to the Joiner. The KEK is the shared secret between the Joiner and the JR. The JR transmits a "join" message to the Joiner, the message includes the network encryption key, and the message itself is encrypted at MAC-level with the KEK.

V. CONCLUSION

This paper first discusses the building blocks of an IoT system. Security features and capabilities expected from any IoT system are also discussed. IoT systems operate under many constraints, e.g. low power, indoor environment, limited user interface. In today's world, IoT systems face many security challenges and possible attacks. These security attacks are discussed and how IoT systems handle these attacks.

Two very different IoT system protocols, *Z-Wave* and *Thread* are introduced. PHY and MAC of both these protocols are discussed. The security structure of the two IoT protocols is quite similar at Data Link and Transport Layer. One reason for this is that the *Z-Wave* has been updating it security protocols to the latest standard. *Z-Wave* changed its Data Link encryption from TDES to AES-128.

Both of these systems were designed with very different philosophies, one is based on propriety design, and the other is based completely on standards and RFCs. *Z-Wave* is over 15 years, while *Thread* is latest IoT protocol specified. *Z-Wave* has shown that it can change with time and survive changes in technology. *Thread* is still so new that it is hard to find any products in the market with *Thread* logo, only time will tell how *Thread* fares with changing times.

Given the tremendous projected growth of IoT systems [2], and a potential for major cyber attacks [3] [25] [26], the IoT security issues will remain in the forefront for the foreseeable time. The IoT protocol designers and manufacturers are trying their best to make security foolproof as possible, but they will have to stay vigilant and one step ahead of new hacking techniques.

Both *Z-Wave* and *Thread* are complex protocols, each protocol consists of hundreds of pages of detailed documents containing every aspect of protocol use. Each device interaction has many sub-cases of possible scenarios, limits and options in messages and responses. This brief paper couldn't describe all the details of these protocols, but it is hoped that it will serve as a starting point for further research and study.

Disclaimer: At the time of writing of this paper, none of the authors were affiliated with either *Z-Wave* or Thread Group Inc.

REFERENCES

[1] Aston, Kevin. "That 'Internet of Things' Thing", Available: http://www.rfidjournal.com/articles/view?4986, accessed on June 2, 2017.

[2] Gartner, Inc. "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016", http://www.gartner.com/newsroom/id/3598917, accessed on June 2, 2017.

[3] G. Kambourakis, C. Kolias and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies," *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, Baltimore, MD, 2017, pp. 267-272. doi: 10.1109/MILCOM.2017.8170867

[4] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," *2017 North American Power Symposium (NAPS)*, Morgantown, WV, 2017, pp. 1-6. doi: 10.1109/NAPS.2017.8107363

[5] K. Sonar H. Upadhyay "A Survey: DDOS Attack on Internet of Things Intl", *Journal of Engineering Research and Development*, vol. 10 no. 11 pp. 58-63.

[6] S. A. P. Kumar, B. Bhargava, R. Macêdo and G. Mani, "Securing IoT-Based Cyber-Physical Human Systems against Collaborative Attacks," *2017 IEEE International Congress on Internet of Things (ICIOT)*, Honolulu, HI, 2017, pp. 9-16. doi: 10.1109/IEEE.ICIOT.2017.11

[7] Ishaq Unwala, Jiang Lu, "IoT Protocols : Z-Wave and Thread", November 17 Volume 3 Issue 11 , *International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRSCE)*, PP: 355 – 359

[8] Paetz, Christian. Z-Wave Essentials. Prof. Dr. Christian Paetz

[9] http://www.gatedepot.com/landing-category-small/access-radio-remotes/ , accessed on Feb 2, 2018

[10] Lorex Technology, https://www.lorextechnology.com/, accessed on Feb 2, 2018.

[11] IEEE Standards, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) IEEE Std 802.15.4 ™ -2006

[12] J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," in *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269-284, June 2016. doi: 10.1109/JIOT.2015.2460333

[13] J. Jiang, G. Han, F. Wang, L. Shu and M. Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228-1237, May 1 2015. doi: 10.1109/TPDS.2014.2320505

[14] V. Suryani, Selo and Widyawan, "A survey on trust in Internet of Things," *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Yogyakarta, 2016, pp. 1-6. doi: 10.1109/ICITEED.2016.7863238

[15] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Computer Science Information System*, vol. 8, no. 4, pp. 1207–1228, 2011

[16] H. Sándor and G. Sebestyén-Pál, "Optimal security design in the Internet of Things," *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, Tirgu Mures, 2017, pp. 1-6. doi: 10.1109/ISDFS.2017.7916496

[17] M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, Abha, 2017, pp. 93-97. doi: 10.1109/Anti-Cybercrime.2017.7905270

[18] G. Glissa, A. Rachedi and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, 2016, pp. 1-7. doi: 10.1109/GLOCOM.2016.7841543

[19] ITU Telecommunication article number E 40186 . https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.9959-201501-I!!PDF-E&type=items , accessed on Feb 2, 2018

[20] Z-Wave the Public Standard, http://zwavepublic.com/

[21] "Introduction to the Z-Wave Security Ecosystem", available from Sigma Design, Inc., on the company website: http://Z-Wave.sigmadesigns.com/wp-content/uploads/2016/08/Z-Wave-Security-White-Paper.pdf , accessed on Feb 2, 2018

[22] Threadgroup Inc. website: http://*Thread*group.org/What-is-*Thread*/Connected-Home , accessed on Nov. 6, 2017

[23] M. Zareei, A. Zarei, R. Budiarto and M. A. Omar, "A comparative study of short range wireless sensor network on high density networks," *The 17th Asia Pacific Conference on Communications*, Sabah, 2011, pp. 247-252. doi: 10.1109/APCC.2011.6152813

[24] M. Knight, "Wireless security - How safe is Z-Wave?," in *Computing & Control Engineering Journal*, vol. 17, no. 6, pp. 18-23, Dec.-Jan. 2006. doi: 10.1049/cce:20060601

[25] Bahrang Fouladi, Shand Ghanoun: Honey, I am Home!!, Hacking Z-Wave Home Automation Systems, Black Hat USA 2013, Las Vegas July 27-Aug1st, 2013, Slides available at http:// www.slideshare.net/ sensepost/ hacking-zwave-home-automation-systems

[26] Joseph Hall and Ben Ramsey: Z-WAVE PROTOCOL HACKED WITH SDR, Hackaday 16. January 2016, Story available at http:// hackaday.com/ 2016/ 01/ 16/ shmoocon-2016-Z-Wave-protocol-hacked-with-sdr/

[27] Sigma Design press release, "Sigma Designs Announces Break-Through Z-Wave(R) UL Component Recognition", http://www.sigmadesigns.com/news/sigma-designs-announces-break-through-Z-Waver-ul-component-recognition , accessed on June 2, 2017.

[28] Z-Wave Alliance Announces New Security Requirements for All Z-Wave Certified IoT Devices, Press Release Z-Wave Alliance, Nov. 17th, 2016, http:// Z-Wavealliance.org/ Z-Wave-alliance-announces-new-security-requirements-Z-Wave-certified-iot-devices

[29] J. Daemen and V. Rijmen, AES Proposal: Rijndael, version 2, 1999. Available from URL: http://www.esat.kuleuven.ac.be/~rijmen/rijndael

[30] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo and L. Zhou, "On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age," in *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 237-248, May-June 1 2017. doi: 10.1109/TDSC.2016.2577022

[31] M. B. Yassein, W. Mardini and A. Khalil, "Smart homes automation using Z-Wave protocol," *2016 International Conference on Engineering & MIS (ICEMIS)*, Agadir, 2016, pp. 1-6. doi: 10.1109/ICEMIS.2016.7745306

[32] Galeev, M.T., S. Engineer, and M. Inc, "Catching the Z-Wave". *Embedded Systems Design*, 2006. 19(10): p. 28.

[33] Federal Information Processing Standards , "Announcing the Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197 November 2001 [online] Available: http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[34] G. Gaubatz, J. P. Kaps, E. Ozturk and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks," *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, Kauai Island, HI, 2005, pp. 146-150. doi: 10.1109/PERCOMW.2005.76

[35] S. Zamfir, T. Balan, I. Iliescu and F. Sandu, "A security analysis on standard IoT protocols," *2016 International Conference on Applied and Theoretical Electricity (ICATE)*, Craiova, 2016, pp. 1-6. doi: 10.1109/ICATE.2016.7754665

[36] M. B. Yassein, W. Mardini and A. Khalil, "Smart homes automation using Z-Wave protocol," *2016 International Conference on Engineering & MIS (ICEMIS)*, Agadir, 2016, pp. 1-6. doi: 10.1109/ICEMIS.2016.7745306

[37] "The *Thread* Group Expands Influence through Partnership with ZigBee Alliance, TCLA and Innovation Enabler Award", (Accessed June 7, 2017) http://mysmahome.com/news/5905/the-*Thread*-group-expands-influence-through-partnership-with-zigbee-alliance-tcla-and-innovation-enabler-award-2/

[38] M. Al-Zyoud, T. Atkison and J. Carver, "An Overview of Emerging Privacy Issues in the Internet of Things," *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, 2016, pp. 212-217. doi: 10.1109/CSCI.2016.0047

[39] L. Nastase, "Security in the Internet of Things: A Survey on Application Layer Protocols," *2017 21st International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, Romania, 2017, pp. 659-666. doi: 10.1109/CSCS.2017.101

[40] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker and H. Chen, "Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)," *2014 IEEE Joint Intelligence and Security Informatics Conference*, The Hague, 2014, pp. 232-235. doi: 10.1109/JISIC.2014.43