American Journal of
Electronics & Communication

Arpan Garai et. al., American Journal of Electronics & Communication, Vol. II (4), 26-32

IOT Securities: A Review

Arpan Garai, Shibaprasad Sen, and Piyali Chandra
Department of Computer Science and Engineering,
University of Engineering and Management,
Kolkata, India
arpangarai@gmail.com

***Abstract*—In this current era, the demand for smart homes, cities, etc. is now increasing exponentially. Thereby, the IoT (Internet of Things) has an remarkable potential, impact, and growth. However, these IoT-enabled devices are often hacked and compromised. Typically, these devices have a limitation in computation, storage capacity, and network access. Therefore, they often become vulnerable to attacks. In this paper, we present a survey regarding major security issues often seen in these IoT devices. In the present work, firstly, the popular security issues regarding the IoT layered architecture, protocols for networking, communications, and management are categorized. Next, an outline of the security requirements and existing solutions for the attacks are discussed. We also mapped the problems and corresponding solutions found in the existing literature. The paper also provides the challenges and open research problems for IoT security.**

I. Introduction

Nowadays, smart homes, smart cities are adequate and demanding for everyone. Smart devices and high-speed networks have grown rapidly and the Internet of Things (IoT) is also widely applied in daily life. To connect and exchange data with other devices and systems over the internet Internet of Things is introduced. IoT is a network of physical objects, "things" embedded with sensors, software, and other technologies. The device can be controlled from a remote location to perform necessary tasks and information can be shared between connected devices via a network that follows standard protocols. Internet of Things devices can be used for personal purposes and to monitor patient operations, detect weather conditions, identify or track animals, track cars, etc. [1].

There are many approaches like target security at a specific layer, end-to-end security, etc. to cope with security issues in the IoT paradigm. Recently, in [2], most of the security issues found in different application, communication, data, and architecture of any IoT device is categorized. There are three kinds of threats like hardware, network, and application components. In [3], different key management systems and cryptography algorithms have been discussed and compared. A comparative study and evaluation of systems to detect intrusion are done in [4]. Sicari et al. have discussed about the different process followed to the information confidential, a secure access in IoT systems in [5]. In [6], the issues related to security occures in fog computing is described.

In this survey article, our main contributions can be summarized as follows: I

1) A parametric solution of security thread.
2) Classification and categorization of security issues in IoT concerning its layer and the counteractions used to address these issues.
3) Different solutions to resolve security issues.
4) The idea of blockchain-based security and analysis of securing IoT.
5) Future Directions regarding the possible solutions for open IoT security problems.

Section II describes the security requirements faced by each layer of the IoT architecture and the protocol stack implemented through the IoT. Section III categorizes the main protection problems, while, section IV analyzes and highlights a mapping of the proposed solutions. In Section V, we discuss the research requirements and actionable responses that are the main obstacles to protecting IoT before concluding the article in Section VI.

II. Basic architecture of IoT with security challenges

A classic IoT architecture contains a number of sensors. These sensors are interconnected through network. The devices run in low power and use small memory. They also have a limited processing capability.

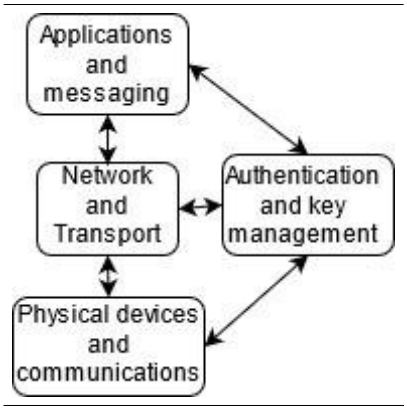

Fig. 1. IoT protocols and standards.

A. protocols and standards in IoT based systems

Fig. 1 depicts a layered architecture of the protocols and standards commonly used in low rate wireless personal area networks (LR-WPANs) [7]. Nevertheless, the currently

evolved protocols are used in the low power wide-area-network (LPWAN).

In the IEEE standard 802.15.4 for LR-WPANs, the low-level layers are roughly classified into two layers. They are the physical Layer and the medium access control (MAC) layer. The physical layer standards are related to the wireless channels. Whereas, the MAC layer describes sets the protocols for channel access and synchronization. Here, maximum transmission unit (MTU) is often used. The size of an IPv6 with respect to low-power wireless personal area network (6LoWPAN) is small. So, the adaptation layer is integrated above the link layer. It leads to enrichment of communication of the sensor node with IP-based capabilities. The RPL standard helps to communicate between multi-points and single points. With the help of an IPv6 network address, every device in IoT is uniquely identifiable. For helping 6LoWPAN, the routing Protocol can use in Low-power and Lossy Networks (RPL) [8].

The utility design in IoT contains person Datagram Protocol (UDP) [9] for conversation because of a limited payload and less complicacy than TCP. To manage messages, togetherwith specifying unreachable vacation spots, and neighbor discovery, 6LoWPAN utilize the internet control Message Pro- tocol (ICMP) [10]. The constrained software Protocol (CoAP) [11] offers a model based on a upcoming request and its corresponding response for low-strength and lossy networks current in confined environments. In assessment to a wireless WAN which calls for greater power to work with an excessive bit-charge that supports low-energy communication with low bit-rate. The LPWAN allows for a protracted range of communication. LoRaWAN protocol is used for conversation among gateways and the quit devices at the same time. A 3GPP protocol is used in LPWANs to is followed for communication in the narrow-band IoT (NB-IoT). It also helps to provide an indoor coverage as the usage of LTE spectrum. The Weightless protocol makes use of three distinct standards for conversation in LPWAN to support unidirectional, bidirectional, and low-power modes, respectively.

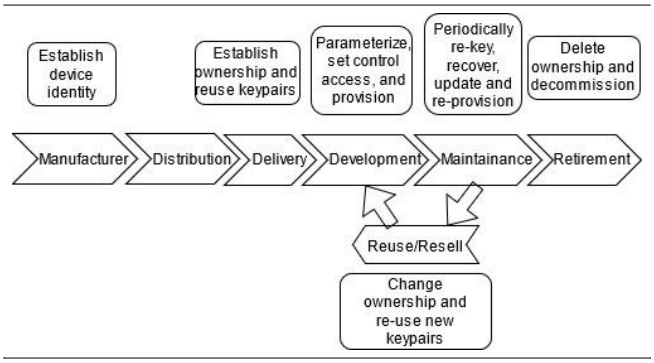

Fig. 2. IoT device life-cycle security management.

B. Security required in IoT

The life-cycle for security management is shown in Fig. 2. To deploy the IoT devices in a secure way, various parameters and mechanisms need to be computed as depicted underneath.

1) Data privacy, integrity, and confidentiality: The encryption mechanism is required to ensure the secrecy of data security as IoT facts travel through multiple hops in a network. The statistics stored on a tool are prone to privacy violation via compromising nodes current in an IoT network. Numerous integration of services, devices and networks are the cause of privacy violations.

2) Authorization, authentication, and accounting: Authentication is required between two parties to secure communication in IoT. A variety of authentication mechanisms exists as there are a diversity present in the underlying environments and architectures for IoT devices. The procedure to authorize and authenticate are implemented to ensure a comfortable conversation. Furthermore, an aid to audit and report is used to provide a reliable mechanism for security of the network control.

3) Single points of failure: IoT-based infrastructure might also expose a massive wide variety of single points of failure because of the tremendous network growth of IoT infrastructure. Improvement of tamper-proof surroundings for an enormous number of IoT devices is necessary. This is the cause of fault-tolerant networks.

4) Available services: Various attacks on IoT devices often hamper services. Different strategies consisting of sinkhole attacks, replay attacks, and adversaries jamming take advantage of IoT additives at exceptional layers to deteriorate the high-quality-of-service (QoS).

5) Efficient use of energy: The IoT devices generally have a limitation in resource. The attack upon a IoT device often cause a high consumption on energy. Generally, it is due to flooding a community and also the IoT sources are often exhausted using forged or redundant service requests.

III. Different levels of security issues

The IoT paradigm covers various devices and equipment. It ranges from a small chip embedded in a living being or any large system to large high-end servers. Therefore, it must solve different levels of security issues. In the deployment of IoT architecture, three categories of security threats (Low-level issues, Intermediate-level issues, and High-level issues) are considered which are described in the following sub-sections.

A. Low-level issues

The security in first level involves the physical and data link layers of communications and security issues at the hardware level. Interference attacks on wireless devices on the Internet of Things are aimed at degrading the network by transmitting signals of radio frequency without adopting a fixed protocol [12]. Radio interference seriously affects the operation of the network and may affect the transmission and reception of data by legitimate nodes, leading to system failure or unpredictable behavior. The physical layer communication should be protected to prevent unauthorized recipients.

Low-level witches and deceptive attacks. Sybil attacks on wireless networks caused by malicious Sybil nodes using

false identities to reduce IoT functionality. At the physical layer, Sybil nodes can use randomly falsified MAC values to pretend to be different devices and, at the same time, aim to deplete network resources [13]. Therefore, legitimate nodes can refuse access to resources (Insecure physical interface). Access to software through physical interfaces and testing / debugging tools can be exploited (Poor physical security) by disrupting network nodes [14]. Seizures of sleep deprivation Power-constrained devices on the Internet of Things are often attacked. Therefore, it causes the sensor nodes to stay awake [15]. When enormous tasks are customized to run in a 6LoW- PAN environment, the battery will drain.

B. Intermediate-level issues

In this level security issues involve routing, communication, and session management in the IoT network and transport layer. Replay or copy attacks are observed due to fragmentation. IPv6 packet segmentation is necessary for devices that comply with the IEEE 802.15.4 standard by its tiny frame size. The repeated fragments sent by malicious nodes will affect the reassembly of data packets, making it arduous to process other legitimate data packets [16]. It's called the discovery of unsafe neighbors. Each device must be uniquely identifiable in the IoT architecture. The messages generated for identification must be secure. Data must be transmitted to the device to reach the designated destination in end-to-end communication. Before data transmission, several steps must be performed at this stage, such as address resolution and router discovery [17].

Since the nodes at the receiving end need to reserve buffer space for reassembling incoming data packets. So, the attacker can take precedence of this by sending incomplete data packets [16]. Since incomplete data packets sent by the attacker take up space, this type of attack will result in a denial of service because other fragmented data packets are discarded.

The IoT systems that uses the IPv6 routing protocol of low-power networks (RPL) become vulnerable to various attacks. It is mainly triggered by infected nodes on the IoT network [18]. Attacks can lead to resource exhaustion and eavesdropping.

The attacking node responds to routing requests, so the data packets are routed through the attacking node, and then malicious activities can be performed on the IoT network [19]. Due to wormhole attacks, network attacks will further aggravate 6LoWPAN operations. In wormhole attack, a virtual tunnel is generated between the two nodes. Therefore, the packets arriving at one node reach to the other node, immediately [20]. These attacks have significant implications. It includes invasion of privacy, eavesdropping, and service denial.

Similar to low-level hierarchical Sybil attacks, Sybil nodes can deploy to reduce performance of the network and violate privacy of the data privacy. Sybil nodes that uses false identities sometime lead to the spread of spam, malware, or the launch of phishing attacks [21].

IoT devices and users should authenticate through a key management system. Any security breach at the network layer or a large amount of overhead to protect communicationscan expose the network to a large number of vulnerabilities [22]. For example, due to limited resources, it is necessary to minimize the overhead of Datagram Transport Layer Security (DTLS) [24].

End-to-end security at the transport level aims to provide a security mechanism so that the desired destination node can reliably receive data from the sending node [25]. It requires a comprehensive authentication mechanism to ensure secure communication of messages in encrypted form without violating privacy while working with minimal overhead [26].

The use of spoofed messages for session hijacking at the transport layer can lead to denial of service [28]. The attacking node can impersonate the victim node to continue the conversation between the two nodes. The communication node may even need to re-transmit the message by changing the sequence number.

Privacy disclosure in cloud-based IoT can launch different attacks which may undermine identity and location privacy in the cloud or network-based IoT with latency tolerant capabilities [29]. Likewise, the faulty cloud service provider based on which the IoT is implemented, may have access to sensitive information.

C. High-level issues

Generally, High-level security issues are involved in the different applications which are running on various devices present on the IoT. Some major High-level security issues are briefly described in the following.

The upper layers of IoT system that contains an application layer are often attacked [31]. This application layer follows a web transfer protocol named Constrained Application Protocol (CoAP). This protocol is generally used to restrict the the DTLS devices based on various security modes. In RFC7252 [11], a specific format is defined for the CoAP messagesfollow. It helps in encryption for secure communication.

There are various interfaces like mobile, web, and cloud are often used to access the IoT system. These interfaces are also often attacked and it may hamper the privacy of the data severely [14].

The firmware or other security software of the IoT system often become vulnerable. Some of them are listed in [14]. The software and the codes written in JSON, SQLi, XML, and XSS must be carefully tested to avoid the attack.

IoT middleware is used to provide a smooth communication between the heterogeneous entities present in the IoT system. Therefore, the IoT middleware must be designed such that it can deliver securely. Moreover, in some IoT systems, different interfaces need to be combined. In such cases, the middleware environments should provide a secure communication [32].

IV. Solutions for different security issues

The vulnerabilities of different components like network components, software, physical devices, firmware etc. causes the security threats in IoT. In an IoT based system, usersinteract with the mentioned components by using protocols that may even break of the security. The treatment of security threats reports the vulnerabilities observed in various layers

to obtain desired level of security. Different protocols used to deploy the mentioned components adds complexity to the treatment. This section also highlights, analyzes, and gives directs solutions for the security threats at low-level, intermediate level, and high level mentioned in the literature. The comparative analysis include the threat parameters, detailed implications, the affected layers, and corresponding remedies.

A. solutions for Low level security issues

The message collision or flooding the channels can be seen in wireless sensor networks due to jamming attacks. Authors in [33] proposed a method for jamming attacks detection where firstly the strength of signal is measured for the extraction of noise-like signals. The measurements are compared with defined threshold values to detect attacks. Authors in [12] proposed an mechanism for the detection of jamming attacks which is based on computing successful packet delivery ratio. To manage the jamming attacks channel surfing and spatial retreats strategies have been used in the work mentioned in [34]. Works mentioned through [35] stated that artificial noise can be introduced in signals for secure communication. Demirbas et al. in [36] proposed an method for the detection of sybil attacks using signal strength measurement by employing detector nodes for the computation of sender location at the time of message communication. Xiao et al. demonstrates the uses of channel estimation for sybil attack detection [13].An another work mention in [37] highlights that the legalusers and attackers can be distinguished by utilizing channel response. It has been observed that generally the devices having firmware, software access or providing utility tools for debugging and testing suffers from improper physical security. The OWASP provides guidance to enhance physical security in IoT devices [14]. The unnecessary hardware interfaces like USBs those provides access to the device firmware/software and are also not necessary can be avoided to improve physical security. To increase physical security, the tools for testing and debugging need to be disabled and the Trusted Platform Modules mechanisms should be included. To reduce sleep deprivation attacks in wireless sensor network, a novel framework has been mentioned in [15]. The described framework follows a clustering technique where clusters are again subdivided into many other sectors to avoid long distance communication and thereby energy consumption is reduced.

B. solutions for Intermediate level security issues

The timestamp and the nonce option does well for both unidirectional and bidirectional packets. The timestamp value in the fragment helps in elimination of redundant advertisement and redirection in the network. Whereas, nonce option confirms the response to fresh solicitation. Authors in [16] proposed a content-chaining mechanism to transmit the IPv6 packets fragments in 6LoWPAN. The fragments are verified when its contents are added to hash-chain generation. Riaz et al. have developed a security framework that helps in secure neighbor discovery, authentication, key generation and data encryption [17]. The Elliptic Curve Cryptography [38] can be used for secure neighbor discovery. The ECC public key signatures help to find and locate the neighbor nodes. The concepts of symmetric and asymmetric key management are used so that the encrypted data can be communicated for node-to-node security purpose. buffer reservation attack may block the reassembly buffer of certain nodes and can be alleviated by adopting split buffer approach where fragmented packets are transmitted through short bursts [16]. In this procedure every node tracks the completion status of a packet and also keep a note on sending fragments. As a consequence, to avoid overloading condition, a node is allowed to discard the packets with low completion percentage or having huge variations in fragment pattern. Dvir et al. proposed Version Number and Rank Authentication technique to reduce adversary attacks when used IPv6 routing protocol for LLN (Low power and Lossy networks). This procedure uses hash fuction, MAC function and digital signatures to authenticate version number and rank. Weekly et al. proposed the remedy of sinkholeattacks in [19] that is based on failover and authentication technique. A one way hash function along with hash chain function was used to verify the rank correspond to DestinationInformation Object (DIO) message. A different approach to detect wormhole attacks has been proposed by the authorin [20] where broadcasting distances between neighbours are measured in wireless sensor network. There are manymore works for the detection and to avoid sinkhole attacks mentioned in the literature through [39]. The sybil attacksis also a severe threat to distributed and IoT. Generally in social networks, the creation of sybil identities are limitedby including trust relationship. Sybil nodes can be detected using social graph traversal using random walk or by adopting algorithms like community detection [21], [40]. To secure network layer of 6LoWPAN, Granjal et al. [22] introduced a new dispatch type value. The authors have used the reserved values for payload byte [41]. Among the 6 bits of such dispatch type value, first 3 bits represent security header and the usage mode, last 3 bits represents the type for addressing headers (6LoWPAN). Depending on the cryptographic algorithms used to extract information and the keys applied to process the packet, a two byte Security Parameter Index has been used. To secure IoT against DoS, man-in-the-middle, and replay attacks Mahalle et al. proposed a protocol in [23]. The DoS attacks mainly arises due to the message sent from the attackers to utilize the resources. The proposed Identity Authentication and Capability based Access Control approach generates secretkeys by utilizing Diffie Hellman algorithm based on Elliptic Curve Cryptography. The capability based access mechanism firstly verifies the two devices before any communication is made. Moreover, the capability of the device is checked in prior to perform the desired functionality. Kothmayr et al. [42],
[43] highlighted an efficient security procedure that follows two-way authentication by using public key cryptography. Zhou et al. in [29] highlighted an efficient authentication technique for secure packet forwarding that aims to pre- serve privacy of identity and location for cloud based IoT. Their proposed method considered symmetric homomorphic

mapping scheme to delay tolerant networks that lacks of constant end-to-end connection and thus intermediate nodes require to collaborate at the time of message transmission. To provide end-to-end security at transport level, a lots of header compression techniques are present in the literature. Raza et al. [44] mentioned a method that compress the record of DTLS and handshake headers along with various handshake-messages so that it can fit within a 6LoWPAN single MTU. Shahid et al. have implemented Internet Key Exchange (IKE) which is lightweighted and improves the key management for 6LoWPAN [27]. Generally, IPSec applies the IKE protocol to manage keys. However, this protocol is not suitable in a situation where there is constrain of resource devices. Hence, the authors have introduced a compressed IKEv2 version that uses compressed UDP format known as IKE header.

C. solutions for High level security issues

In order to provide security for Low-power and Lossy Network working with Constrained Application Protocol (CoAP), Brachmann et al. proposed approach in [30] that is basedon TLS and DTLS. This approach works in a situation where 6LoWPAN Border Router makes connection with LLN for accessing the devices in remote mode. The LLN nodes provide the services to the clients working with CoAP and HTTP. To ensure security for LLNs from attacks coming frominternet, a mapping of TLS and DTLS has been proposed.The authors in [45] have used a security model with 6LBR to filter messages to ensure end-to-end security for IoT basedon IP networks. Sethi et al. have built a security model for CoAP which is based on public key cryptography [31]. The prescribed security model uses Resource Directory and MP (Mirror Proxy). MP helps the server to provide servicesto the requests at sleep state. Resource Directory lists theresources on the server/endpoints. Key role of MP is to register the endpoints, addition of resources in a resource tree, and to store endpoint public keys. The client can access the resources by using resource identifiers. Public keys that are transferred to clients are used to authenticate data updating in subsequent phases. Conzon et al. have shown the effective- ness of VIRTUS- a middleware to secure distributed systems working on IoT environment [32]. This middleware follows a communication technique that includes TLS, and SASL to maintain data integrity, the XML stream encryption and verification. Authentication technique confirms that the data access and exchange takes places for authorized users only. Authors in [46] built a standard architecture to help M2M (machine to machine) communication in IoT environment. They have mentioned an architecture that involves different layers of security (environment, security functionality, and abstraction). The encryption of resource contents must be done with secure message exchange to provide M2M service layer security.

V. CHALLENGES

The challenges associated during security implementation of IoT devices has been discussed below.

A. limitations of Resources

The constrain in resource is a challenge in providing arobust security mechanism in IoT. Cryptographic algorithms must be limited to work within this constrains compared to the conventional paradigms. The exchange of keys, certificates, storage, or energy requirements in broadcasting/multicasting need to be well suited for effective implementation of communication protocol with security mechanism in IoT.

B. Heterogeneous devices

The implementation of multi layer security framework is a challenging task when considering Heterogeneous devices for both small low power devices and high end servers. The implemented framework must be working well with existing resources, selects suitable security protocols at IoT layers before providing service to the end user.

C. Single points of failure

When considered Heterogeneous networks, protocols, and architectures, IoT paradigm faced challenge with Single points of failure. Researchers need to explore more to ensure adequate availability of IoT elements. It requires different standards and techniques to introduce redundancy by keeping a balance between reliability and cost for the whole framework.

D. Hardware/firmware vulnerabilities

The IoT architecture may face challenge due to hardware vulnerabilities for low cost and low power devices. Hence, along with physical malfunctioning, implementation of security mechanisms in packet processing, hardware, and routing needs to be checked before IoT deployment.

E. Trusted updates and management

To provide scalable and trusted management, software updates to IoT devices is an open challenge to the researchers. Furthermore, the issues concerning trusted and secure governance of IoT device ownership, data privacy and supply chain are still open research problems and demanding solutions to provide scale adoption for IoT.

VI. CONCLUSION

In modern days, the security of the IoT devices have become vulnerable. So, the constrains of the resources of the IoTdevices needs to be updated. A robust hardware for security must be included. A software may also be designed for better security. This paper depicts a brief survey and review of the primary security issues of any IoT system. These issues are categorised depending on the IoT layers into three levels i.e. low, intermediate and high level. The mechanisms suggested in the literature to solve these issues are also discussed in this paper. The future scope and open research problems are also addressed here in this paper.

REFERENCES

[1] M. Rouse, I. Wigmore, Internet of things, 2016. URLhttp://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[2] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: A survey, J. Netw. Comput. Appl. 88 (Suppl. C) (2017) 10–28. http://dx.doi.org/ 10.1016/j.jnca.2017.04.002.

[3] J. Granjal, R. Silva, E. Monteiro, J.S. Silva, F. Boavida, Why is IPSec a viable option for wireless sensor networks, in: 2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2008, pp. 802–807. http: //dx.doi.org/10.1109/MAHSS.2008.4660130.

[4] I. Butun, S.D. Morgera, R. Sankar, A survey of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 16 (1) (2014) 266–282. http://dx.doi.org/10.1109/SURV.2013.050113.00191.

[5] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Comput. Netw. 76 (Suppl. C) (2015) 146–164. http://dx.doi.org/10.1016/j.comnet.2014.11.008.

[6] S. Yi, Z. Qin, Q. Li, Security and privacy issues of fog computing:A survey, in: Wireless Algorithms, Systems, and Applications the 10th International Conference on, 2015, pp. 1–10.

[7] IEEE, IeEEE Standard for Local and metropolitan networks–Part 15.4: LowRate Wireless Personal Area Networks (LR-WPANs), 2012. URL https:// standards.ieee.org/findstds/standard/802.15.4-2011.html.

[8] T. Winter, P. Thubert, A. Brandt, J.W. Hui, R. Kelsey, Rfc 6550 - rpl: ipv6 routing protocol for low-power and lossy networks, 2012. URL https://tools.ietf.org/ html/rfc6550.

[9] J. Postel, User datagram protocol, 1980. URL https://tools.ietf.org/html/ rfc768.

[10] A. Conta, S. Deering, M. Gupta, Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification, 2006. URL https: //tools.ietf.org/html/rfc4443.

[11] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (CoAP), 2014. URL https://tools.ietf.org/html/rfc7252.

[12] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. http://dx.doi.org/ 10.1145/1062689.1062697.

[13] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-Based detection of sybil attacks in wireless networks, IEEE Transa. Inf. Forensics Secur. 4 (3) (2009) 492–503.

[14] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index.php/Top_ IoT_ Vulnerabilities.

[15] T. Bhattasali, R. Chaki, A survey of recent intrusion detection systems for wireless sensor network, in: D.C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, D. Nagamalai (Eds.), Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15–17, 2011, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 268–280.

[16] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN Fragmentation attacks and mitigation mechanisms, in: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, ACM, New York, NY, USA, 2013, pp. 55–66. http://dx.doi. org/10.1145/2462096.2462107.

[17] R. Riaz, K.-H. Kim, H.F. Ahmed, Security analysis survey and framework design for IP connected LoWPANs, in: 2009 International Symposium on Autonomous Decentralized Systems, 2009, pp. 1–6. http://dx.doi.org/10.1109/ ISADS.2009.5207373.

[18] A. Dvir, T. Holczer, L. Buttyan, VeRA - version number and rank authentication in RPL, in: 2011 IEEE Eighth International Confer- ence on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 709–714. http://dx.doi.org/10.1109/MASS.2011. 76.

[19] K. Weekly, K. Pister, Evaluating sinkhole defense techniquesin RPL networks, in: Proceedings of the 2012 20th IEEE In- ternational Conference on Network Protocols (ICNP), ICNP '12, IEEE Computer Society, Washington, DC, USA, 2012, pp. 1–6. http://dx.doi.org/10.1109/ICNP.2012.6459948.

[20] W. Wang, J. Kong, B. Bhargava, M. Gerla, Visualisation of wormholes in underwater sensor networks: A distributed approach, Int. J. Secur. Netw. 3 (1) (2008) 10–23.

[21] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things, IEEE Internet Things J. 1 (5) (2014) 372–383. http://dx.doi. org/10.1109/JIOT.2014.2344013.

[22] J. Granjal, E. Monteiro, J.S. Silva, Network-layer security for the Internet of Things using TinyOS and BLIP, Int. J. Commun. Syst. 27 (10) (2014) 1938– 1963. http://dx.doi.org/10.1002/dac.2444.

[23] P.N. Mahalle, B. Anggorojati, N.R. Prasad, R. Prasad, Identity authentication and capability based access control (iacac) for the internet of things, J. Cyber Secur. Mobility 1 (4) (2013) 309–348.

[24] D.U. Sinthan, M.-S. Balamurugan, Identity authentication and capability based access control (IACAC) for the Internet of Things, J. Cyber Secur. Mob. 1 (4) (2013) 309–348.

[25] J. Granjal, E. Monteiro, J.S. Silva, End-to-end transport-layer security for internet-integrated sensing applications with mutual and delegated ecc public-key authentication, in: 2013 IFIP Networking Conference, 2013, pp. 1–9.

[26] G. Peretti, V. Lakkundi, M. Zorzi, BlinkToSCoAP: An end-to-end security framework for the Internet of Things, in: 2015 7th International Conference on Communication Systems and Networks (COMSNETS), 2015, pp. 1–6. http: //dx.doi.org/10.1109/COMSNETS.2015.7098708.

[27] S. Raza, T. Voigt, V. Jutvik, Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security, in: Proceedings of the IETF Workshop on Smart Object Security, vol. 23, 2012.

[28] N. Park, N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors 6 (1) (2016) 20–20.

[29] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, Security and privacy for cloud-based IoT: Challenges, IEEE Commun. Mag. 55 (1) (2017) 26–33. http://dx.doi.org/ 10.1109/MCOM.2017.1600363CM.

[30] M. Brachmann, S.L. Keoh, O.G. Morchon, S.S. Kumar, End-to-end transport security in the IP-based Internet of Things, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–5. http://dx.doi.org/10.1109/ICCCN.2012.6289292.

[31] M. Sethi, J. Arkko, A. Kernen, End-to-end security for sleepysmart object networks, in: 37th Annual IEEE Conference onLocal Computer Networks - Workshops, 2012, pp. 964–972. http://dx.doi.org/10.1109/LCNW.2012. 6424089.

[32] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M.A. Spirito, The VIRTUS middleware: An XMPP based architecture for secure IoT communications, in: 2012 21st International Conferenceon Computer Communications and Networks, ICCCN, 2012, pp. 1–6. http://dx.doi.org/10.1109/ICCCN.2012. 6289309.

[33] M. Young, R. Boutaba, Overcoming adversaries in sensor networks: A survey of theoretical models and algorithmic approaches for tolerating malicious interference, IEEE Commun. Surv. Tutor. 13 (4) (2011) 617–641. http://dx. doi.org/10.1109/SURV.2011.041311.00156.

[34] W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel surfing and spatial retreats: Defenses against wireless denial of service, in: Proceedings of the 3rd ACM Workshop on Wireless Security, WiSe '04, ACM, New York, NY, USA, 2004, pp. 80–89. http://dx.doi.org/10.1145/1023646.1023661.

[35] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Process. Mag. 30 (5) (2013) 29–40.

[36] M. Demirbas, Y. Song, An RSSI-based scheme for sybil attack detection in wireless sensor networks, in: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM '06, IEEE Computer Society, Washington, DC, USA, 2006, pp. 564–570. http: //dx.doi.org/10.1109/WOWMOM.2006.27.

[37] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, Fingerprints in the ether: Using the physical layer for wireless authentication, in: 2007 IEEE International Conference on Communications, 2007, pp. 4646–4651. http://dx.doi.org/10. 1109/ICC.2007.767.

[38] R. Harkanson, Y. Kim, Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications, in: Proceedings of the 12th Annual Conference on Cyber and Information Security Research, CISRC '17, ACM, New York, NY, USA, 2017, pp. 6:1–6:7. http://dx.doi.org/10.1145/3064814.3064818.

[39] I. Raju, P. Parwekar, Detection of sinkhole attack in wireless sensor network, in: S.C. Satapathy, K.S. Raju, J.K. Mandal, V. Bhateja (Eds.), Proceedings of the Second International Conference on Computer and Communication Technologies: IC3T 2015, Volume 3, Springer India, New Delhi, 2016, pp. 629– 636.

[40] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, A. Panconesi, SoK: the evolution of sybil defense via social networks, in: Proceedingsof the 2013 IEEE Symposium on Security and Privacy, SP '13, IEEE Computer Society, Washington, DC, USA, 2013, pp. 382–396. http://dx.doi.org/10.1109/SP.2013.33.

[41] G. Montenegro, N. Kushalnagar, J.W. Hui, D.E. Culler, Transmis- sion of IPv6 Packets over IEEE 802.15.4 Networks, 2007. URL https://tools.ietf.org/html/ rfc4944.
[42] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle, 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 956–963. http: //dx.doi.org/10.1109/LCNW.2012.6424088.
[43] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle, DTLS based secu- rity and two-way authentication for the Internet of Things, Ad Hoc Netw. 11 (8) (2013) 2710–2723. http://dx.doi.org/10.1016/j.adhoc.2013.05.003.
[44] S. Raza, D. Trabalza, T. Voigt, 6LoWPAN compressed DTLSfor CoAP, in: 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, 2012, pp. 287–289. http://dx.doi.org/10.1109/DCOSS.2012.55.
[45] M. Brachmann, O. Garcia-Morchon, S.-L. Keoh, S.S. Kumar, Security considerations around end-to-end security in the IP-based Internet of Things, in: 2012 Workshop on Smart Object Security, in Conjunction with IETF83, 2012, pp. 1– 3.
[46] OneM2M, Security solutions –OneM2M Technical Specification, 2017. URL http://onem2m.org/technical/latest-drafts.
[47] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V.C.M. Leung, Y.L. Guan, Wireless energy harvesting for the Internetof Things, IEEE Commun. Mag. 53 (6) (2015) 102–108. http://dx.doi.org/10.1109/MCOM.2015.7120024.
[48] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the se- curity of blockchain systems, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j. future.2017.08.020.