Investigation on 6LoWPAN Data Security for Internet of Things

Norsuhaila binti Hj Kasah
Research Center for Cyber Security
Faculty of Information Science and Technology
The National University of Malaysia
43000 UKM Bangi, Malaysia
p102055@siswa.ukm.edu.my

Azana Hafizah binti Mohd Aman
Research Center for Cyber Security
Faculty of Information Science and Technology
The National University of Malaysia
43000 UKM Bangi, Malaysia
azana@ukm.edu.my

Zainab Senan Mahmod Attarbashi
Internetwork Research Lab
School of Computing
University Utara Malaysia
06010 Sintok, Kedah, Malaysia
zainab.senan@uum.edu.my

Yousef Fazea
Internetwork Research Lab
School of Computing
University Utara Malaysia
06010 Sintok, Kedah, Malaysia
yosiffz@uum.edu.my

***Abstract*— Low-power wireless network technology is one of the main key characteristics in communication systems that are needed by the Internet of Things (IoT). Nowadays, the 6LoWPAN standard is one of the communication protocols which has been identified as an important protocol in IoT applications. Networking technology in 6LoWPAN transfer IPv6 packets efficiently in link-layer framework that is well-defined by IEEE 802.14.5 protocol. 6LoWPAN development is still having problems such as threats and entrust crises. The most important part when developing this new technology is the challenge to secure the network. Data security is viewed as a major consideration in this network communications. Many researchers are working to secure 6LoWPAN communication by analyzing the architecture and network features. 6LoWPAN security weakness or vulnerability is exposed to various forms of network attack. In this paper, the security solutions for 6LoWPAN have been investigated. The requirements of safety in 6LoWPAN are also presented.**

Keywords—Internet of Things (IoT), 6LoWPAN, IoT security, data security

I. Introduction

IoT grows in a global computer network and always have non-stop enhancement in technological innovation. Recently, the connected devices to the internet services have enlarged whether the connection wired or wireless which shows the changing of the current form of internet. IoT is an extremely large network that linked "things" and link between people-things, things-things and people-people. In 1982, the first renovated Coke machine was the early device tested linked to the internet. It showed that the machine was capable of reporting the list of inventories and detect whether the drinks were cold when loaded. "Kevin Ashton (born 1968) is a British technology innovator who formulated the terminology "Internet of Things" to interpret a structure where the Internet is related to the real world through universal sensors". IoT is also capable of connecting beyond human interference [1] and affects human's daily lives. This new view of the world presents challenges and convenience that will change the economic and political aspects. These rapid changes of Internet technology will allow people to make the economic more dynamic in two ways [2];

- various low cost, low consumption sensors and system development have been marketed by manufacturers
- cloud computing service providers have stable infrastructure to develop IoT in short-term

Recently, many industries are benefiting from the evolution of IoT platform and sensors such as healthcare, automotive and transportation. The development of IoT technology still has issues to consider such as the communications, protocols, interface, infrastructure and standards [1].

II. Internet of Things (IoT) and 6LoWPAN

Internet of Things (IoT) is the technology where system connectivity is applied and connecting lots of physical devices with the Internet to share information and collect data. It also allows devices to create, deal and use data with nominal human interference [2]. IoT is the next stage of internet which can be attractive to hackers. Various applications have been developed in different fields such as healthcare, manufacturing and logistics with different frameworks. It derived advanced potential techniques like cloud computing, wireless communication, sensors, etc. to develop different intelligent systems [3]. However, the challenges facing the IoT also increased in the way of realize its possible benefits.

IoT works on large scale that can function for long term with very minimum power consumption. In IoT, there are two categories used in network as shown in Fig. 1.

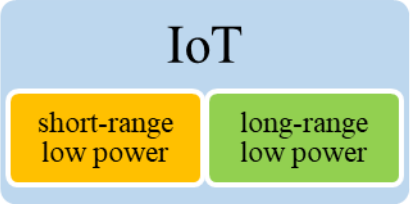

Fig. 1. IoT categories

The term long-range low-power also known as low-power wide-area network (LPWAN) is aimed for communication in long-range at low-power utilization. It

978-1-7281-5467-1/20/$31.00 ©2020 IEEE

also constrains data rate such as long-range wide area network (LoRaWAN), SigFox, narrow-band IoT, etc.

A significant impression in IoT is the "last 100 meters connectivity" perception which is also called short-range low power networks. It describes a big range of technologies like IPv6 over low-power wireless personal area networks (6LoWPAN), Bluetooth low energy (BLE), near-field communication (NFC) and radio frequency identification (RFID). “6LoWPAN is an important element of the IoT where the 6LoWPAN particles will interpretation for the mainstream of the ‘last 100 meters of connectivity’ things” [4].

Wireless Sensor Networks (WSN) has an important role in IoT framework. Recently, many applications are using WSNs in remote monitoring, tracking purpose and record physical condition which consists sensor nodes. WSN also organize the data collected from the main locations [5]. Sensor network can include a thousand of intelligent sensing nodes supplied by a special battery. The major challenge in IoT is to design the security and authentication efficiency scheme considering the limited functions of sensor nodes [6]. Currently, the sensor is manufactured to be smaller, economical, smarter, complete and connected wirelessly to the network for communication functions. The sensor nodes are using wireless protocols to communicate. Bluetooth, Zigbee and Wi-Fi are examples of wireless protocols used by sensor nodes constructed on the protocol of IEEE 802.15.4 [7].

IPv6 has characteristics those make it as a good option for IoT networks. IPv6 have structures by its nature which is scalable, end-to-end encrypted, auto configuration capabilities, substitute of NAT (network address translation) and security which can be a solution to the critical issues in wireless platform. In IoT framework, various embedded devices used low power, memory and processing resources. It is identified as Low power and Lossy Networks (LLNs). HTTP and TCP are not suitable in this network because they are not able to self-managing the LLNs. Therefore, IPv6 is a good choice to apply in LLNs with its capability to be auto-configured in routing protocols. IEEE and IETF developed a transformation of 6LowPAN used IPv6 over IEEE 802.15.4. It assigns IPv6 packets to be transmitted and receive in Personal Area Networks [8].

III. 6LOWPAN OVERVIEW

IPv6 over low-power personal area network (6LoWPAN) is a Wireless Sensor Network that enables IP in wireless sensor node. Fig. 2 shows the characteristics of 6LoWPAN sensor nodes [7].

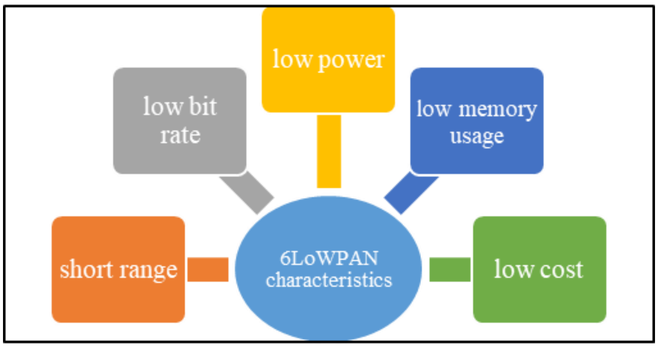

Fig. 2. 6LoWPAN characteristics

6LoWPAN was designed to allow IPv6 packet transmission over LoWPANs using a transformation layer between layer 2 and layer 3. The IPv6 packets are fragmented and reassembled in this layer [9]. The routing protocol in 6LoWPAN manages the routing tables and specify next- hop toward the IP packet destination on routers. The router uses the attached 16-bits short and 64-bits extended MAC addresses [3].

Network architecture of 6LoWPAN contains three important components which are: host node, router node and edge node as shown in Fig. 3. The host can sense physical setting and stimulating device. Packets of data from hosts will be forwarded to the edge router or to 6LoWPAN private network through routers. This connection is done over IEEE 802.15.4 protocol. The edge router will communicate with other IP networks to provide interconnection and traffic management between them [10].

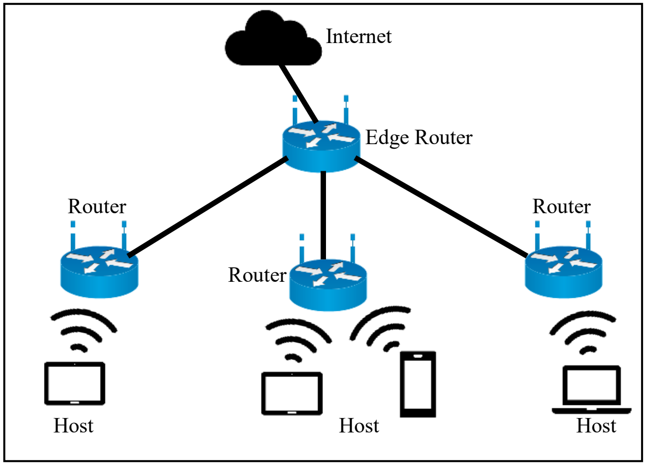

Fig. 3. 6LoWPAN network architecture

IV. SECURITY IN 6LOWPAN

Wireless sensor networks (WSN) security scheme is different than wired network. There are various ways to imply security in wired networks. The widespread implementation of IPsec and Transport Layer Security (TSL) are still major challenges in 6LoWPAN. Devices in 6LoWPAN are powered by battery and have limited computational power, processing and storage. Any existing rules for wired communication are not suitable to be applied in wireless framework [11].

Recently in IT frameworks, 6LoWPAN has make operation and integration of WSN easier. Security is one of the important parts that should be considered when the network is designed. To protect data or personal information from the attacker, the 6LoWPAN team concentrates on security afterwards. Different layers of the network have their safety and security risks which emerged with new fields of any network with different types of devices and inefficiency system [12] [13].

A. Security Requirement in 6LoWPAN

There are few important security requirements in LoWPAN networks to be applied to ensure security. Table 1 below shows the security requirements in 6LoWPAN as proposed in [14].

TABLE I. SECURITY REQUIREMENT IN 6LOWPAN

Requirements	***Descriptions***
Data confidentiality	Data is not reachable to unauthorized persons or users
Data authentication	Users need to assure the data that received comes from trusted origin sources because of message are easily attack by attacker
Data integrity	To assure the data that received by users is not modified by an attacker while transit
Data freshness	Known as key freshness. It means that the information is current and not the old data replayed
Availability	To make sure only authorized users' survivability the network services when needed, despite a DoS attack(s)
Robustness	To assure the operation vitality despite abnormalities. attacks, failed nodes, etc.
Resiliency	Capability of system to equip and sustain an adequate the security level
Resistance	Ability of the network to prevent the attacker to full control of the network via duplicate node attack if some nodes are compromised
Energy efficiency	To maximize network life time, a security system essential to be energy effective
Assurance	The capability to disseminate various information at various assurance levels

B. Security Analysis in 6LoWPAN

In the 6LoWPAN network architecture, the host node which is responsible on sensing and forming perception layer contains IoT physical devices. In this layer, the devices sense various parameters in their framework. If the device is attacked and controlled by the hacker, all the confidential data will be available to get extracted. The router node has transport or network layer can recognize the data transmitted between sensing/perception layer and application layer. The edge node at application layer will analysis the data, store it at the cloud and represent the data to end user. Therefore, securing and trusting data transmission and communication at all layers are very important [15].

In 6LoWPAN, the connection is over IEEE 802.15.4 protocol in MAC layers. It contains security services which are controlled by MAC PAN Information Base (PIB). MAC sublayer will manage the security by keeping an access control list (ACL) in MAC PIB. The security level will be determined and the needed security techniques will be specified such as access control, frame integrity, data encryption, etc. Frame security is most important function in IEEE 802.15.4 MAC that is applied to the applications layers. The security will not implement by default if the application layer does not set the security framework. Although there is a wide range of applications using IEEE 80.15.4 protocol, the authentication and key exchange process is not well-defined [9]. Keyless device is not allowed to encrypt and decrypted their messages. In 6LoWPAN, the administrator can assign a key to the device to encrypt data. A potential resolution to security issues in 6LoWPAN framework can be done by applying the security techniques in application layer such as SSL beside the link layer security. In this situation, the link layer security will defend the device from intrusion while security in application layer will defend it from attacker who is trying to peek the data [16].

Internet technology represents a common mechanism that can protect, check and verified data exchange between devices. However, conventional security systems which are applicable in the Internet such as Internet Protocol Security (IPsec) are still not integrated with slight strained things. In IEEE 802.15.4e standard has defined the structure to accomplish data encryption and authentication [17]. Compressed IPsec has been proposed by researcher as a 6LoWPAN extension for IPsec to secure 6LoWPAN communications. It reduces the use of IPsec in low-end IoT equipment. At the same time, IPv6 protocol's stack can use IPsec to secure data exchange [18].

IPSec represents Authentication Header (AH) and Encapsulation Security Payload (ESP). The function of AH is to guarantee the data integrity and authentication. It can authenticate the original data and ensure the integrity of the sent information. However, AH does not encrypt the data or nor implement data confidentiality. ESP header has been designed to provide security facilities in IPv4 and IPv6. ESP provides security on data content and restricts traffic progress confidentiality. ESP also supports authentication facilities. IPsec is a compulsory extension in IPv6 configuration and this security protocol is applicable in earlier IPv6 frameworks [19]. A researcher [20] proposed header compression extension on IPsec for new protocol in 6LoWPAN. This procedure is performed by reset AH and ESP header compression format, add MOD field and setting various modes of working. The proposed protocol also provides authentication and encryption as flexible choices.

Many application domains apply 6LoWPAN such as military, health monitoring, automation industrial, smart home and many others. To operate these applications, the sensor nodes should sense physical data from operational framework and assign the border router (BR) where user can access the data. These constraints nodes are exposed to attackers. A node can be reprogrammed by the attacker to disobey the integrity, confidentiality or accessibility sense data from other nodes. Due to this restraint, the nodes may have failure because of attackers from inside the 6LoWPAN [21].

Researcher [21] introduces node security quantification (NSQ) model to manage the security level which combines with an intrusion detection system (IDS) alerts. The IDS will identify such attacks and generate alarms. NSQ also classify the security standard of strained nodes and the user data sensor. It also supports network administrator and user decision-making. The result from the simulation done by [21] showed that the security level of NSQ is precisely quantified and maintain the low energy and performance.

TABLE II. SUMMARY OF RELATED WORK FOR DATA SECURITY IN 6LOWPAN

Related Work	***Issue***	***Proposed Method***	***Advantages***
6LowPSec: An end-to-end security protocol for 6LoWPAN [22]	Inadequacy of authentication at the 6LoWPAN layer renders fragmentation systems	A new security protocol which is 6LowPSec, providing an advantages end-to-end security solution at adaptation layer	Operating security activity at the link layer which can be applied in the hardware
Enhanced Simulation Framework	Mobility or change of master device	A mockup framework that authorize	Enhanced traffic prioritization

Related Work	*Issue*	*Proposed Method*	*Advantages*
for Realisations of Mobility in 6LoWPAN Wireless Sensor Networks [23]	and track moveable sensors in network because of physical activities, environment modifies, router error, network features (Delay, Packet Loss, Low Signal)	mobility of end nodes in a 6LoWPAN area. Determine the application of the end node mobility structure among end-to-end coordinators within a 6LoWPAN area	structure to minimize data losses and expand quality of service. Upgraded mechanism for the recognition of micro-mobility
Secure Group Mobility Support for 6LoWPAN Networks [24]	Longer handover latency, packet losses, or even interruptions of the services in the network	A Secure Group Mobility Scheme (SGMS) is considered to certify the security defenses for handovers of several 6LoWPAN devices in similar period	Improve the security performance with significant capability to reach a fast authentication for handovers
Communication security and privacy support in 6LoWPAN [25]	6LoWPAN endure from the threats like leak of information, illegal use of resources, DoS attack	A new Communication scheme with Security and Privacy support for 6LoWPAN (CSP) is introduced. To reach the end-to-end communication security.	CSP accomplishes the communication security. Decrease communication interruption and energy consumption
6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features [26]	Security flaws reflected in threats and lack of trust	Introduced a new security protocol, Combined 6LoWPSec operating consecutively at the MAC and adaptation layers. Contribution both end-to-end and hop-by-hop security features and coping.	Secure the whole network against the attacks from internal and external with minimal energy consumption, overhead and interruption; and a robust hardware application

TABLE III. ANALYSIS OF 6LOWPAN CHARACTERISTICS & REQUIREMENTS FOR THE RELATED WORK

6LowPAN Characteristic & Security Requirement	*Related Work*				
	[22]	*[23]*	*[24]*	*[25]*	*[26]*
Short Range	/			/	/
Low Power	/			/	
Low Memory					/
Low Cost			/		
Data confidentiality	/			/	/
Data authentication	/	/	/	/	/
Data integrity	/			/	/
Data freshness	/			/	
Availability	/		/	/	/
Robustness	/	/			/
Resiliency		/			
Resistance	/		/		
Energy efficiency	/		/		/

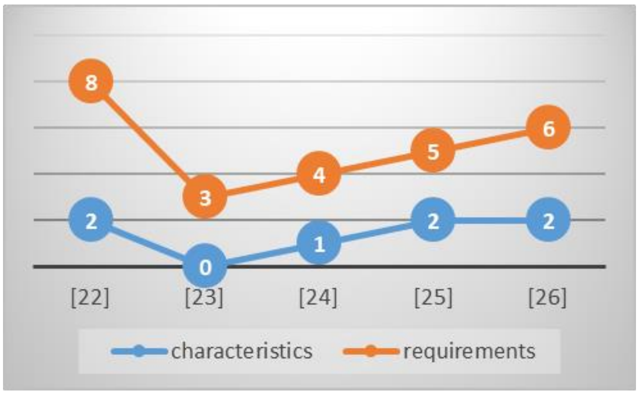

Fig. 4. Number of 6LoWPAN characteristics and requirements for the related work

There are various data security analysis those have been published focusing on communication security for 6LoWPAN networks, and proposing new methods to increase the security. These methods have been analyzed merely on the attacks which can influence different layers in the network. Table II shows the summary of proposed methods by researchers. While table III shows the comparison of 6LoWPAN characteristics and security requirements for each of the proposed methods. Fig. 4 quantitatively compares the number of characteristics and requirements discussed in the related works. From the figure it is shown that work in [22] has significantly considered most of the characteristics and requirements needed in 6LoWPAN data security.

V. CONCLUSION

In this study, features of data security in 6LoWPAN networks are studied. The researchers presented dissimilar features to achieve the security of data communication in the IoT. It is significantly discussing the security requirements for the new proposed methods in order to secure data in 6LoWPAN networks. The efforts to govern and control the structure for data security and privacy are also presented. However, all related works must consider the source authentication and the data confidentially. It is to make sure the data are not being modified or corrupted by the attackers. Security in 6LoWPAN networks is one of the main challenges in IoT security and the enhancements are still needed for future generation networks. Therefore, 6LoWPAN should be studied from all angles to identify the vulnerabilities, the appropriate and capable security solutions.

Acknowledgment

The authors are grateful to Faculty of Information Science and Technology, The National University of Malaysia (UKM) for all their support and contribution to this study. This research is funded by research grant FRGS/1/2019/ICT03/UKM/02/1 and GGPM-2019-030.

References

[1] R. M. Yawson, D. Woldeab, and E. Osafo, "Human Resource Development and the Internet of Things," *Proc. 25th Annu. Acad. Hum. Resour. Dev. Int. Res. Conf. Am.*, p. 25, 2018.

[2] R. H. MZ Ibrahim, "The Implementation of Internet of Things Using Test Bed in The UKMnet Environment," *Asia-Pacific J. Inf. Technol. Multimed.*, vol. 2019, no. 8 (2).

[3] M. Seliem and K. Elgazzar, "IoTeWay: A Secure Framework Architecture for 6LoWPAN Based IoT Applications," *2018 IEEE Glob. Conf. Internet Things, GCIoT 2018*, no. December, 2019.

[4] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, 2019.

[5] H. Mojib, G., Aman, A.H.M., Khalaf, M. & Hassan, "Simulation analysis for QoS in Internet of Things wireless network.," *3C Tecnol. Glosas innovación Apl. a la pyme.*, no. November 2019, pp. 77–83, 2019.

[6] M. R. Farooqi, N. Iqbal, N. K. Singh, M. Affan, and K. Raza, "Wireless sensor networks towards convenient infrastructure in the healthcare industry: A systematic study," *Sensors Heal. Monit.*, vol. 5, pp. 31–46, 2019.

[7] P. Krishnendu and T. M. John, "Development of 6lowpan Mote for IOT," vol. 13, no. 3, pp. 48–54, 2018.

[8] S. S. Vidhya and S. Mathi, "Investigation of next generation internet protocol mobility-assisted solutions for low power and lossy networks," *Procedia Comput. Sci.*, vol. 143, pp. 349–359, 2018.

[9] H. R. AHM Aman, R Hassan, AHA Hashim, "Investigation of Internet of Things Handover Process for Information Centric Networking and Proxy Mobile Internet Protocol," *Mehran Univ. Res. J. Eng. Technol.*, no. 38 (4), pp. 867–874, 2019.

[10] I. Alaoui, A. Azyat, N. Raissouni, N. Ben Achhab, A. Chahboun, and M. Lahraoua, "Comparative Study of ZigBee and 6LoWPAN Protocols: Review," pp. 2–10, 2019.

[11] S. Chakraborty and A. Majumder, "6LoWPAN Security : Classification , Analysis and Open Research Issues," pp. 8–12, 2018.

[12] D. V. Jose and A. Vijyalakshmi, "An overview of security in internet of things," *Procedia Comput. Sci.*, vol. 143, pp. 744–748, 2018.

[13] Y. K. AS Ahmed, R Hassan, NE Othman, NI Ahmad, "Impacts evaluation of DoS attacks over IPv6 neighbor discovery protocol," *J. Comput. Sci.*, no. 15 (5), pp. 702–727, 2019.

[14] S. Hameed, F. I. Khan, and B. Hameed, "Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review," *J. Comput. Networks Commun.*, vol. 2019, 2019.

[15] K. M. Sadique, R. Rahmani, and P. Johannesson, "Towards security on internet of things: Applications and challenges in technology," *Procedia Comput. Sci.*, vol. 141, pp. 199–206, 2018.

[16] M. Sharma, A. Tandon, S. Narayan, and B. Bhushan, "Classification and analysis of security attacks in WSNs and IEEE 802.15.4 standards : A survey," *Proc. - 2017 3rd Int. Conf. Adv. Comput. Commun. Autom. (Fall), ICACCA 2017*, vol. 2018-Janua, pp. 1–5, 2018.

[17] R. Ali, Z., Aman, A.H.B.M. & Hassan, "Cloud Query Processing Analysis : Encryption and Decryption," *3C Tecnol. Glosas innovación Apl. a la pyme*, no. November 2019, pp. 65–75, 2019.

[18] T. Gomes, F. Salgado, S. Pinto, J. Cabral, and A. Tavares, "A 6LoWPAN Accelerator for Internet of Things Endpoint Devices," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 371–377, 2018.

[19] J. F. Eric Conrad, Seth Misenar, "Chapter 3 - Domain 3: Security engineering," *Elev. Hour CISSP® (Third Ed.*, pp. 47–93, 2017.

[20] H. Wang and Z. Sun, "Compression method for IPSec over 6LowPAN," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 4, pp. 1819–1831, 2018.

[21] A. Ramos, R. T. P. Milfont, R. H. Filho, and J. J. P. C. Rodrigues, "Enabling online quantitative security analysis in 6LoWPAN networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5631–5638, 2019.

[22] G. Glissa and A. Meddeb, "6LowPSec: An end-to-end security protocol for 6LoWPAN," *Ad Hoc Networks*, vol. 82, pp. 100–112, 2019.

[23] R. V. Vasilev and A. M. Haka, "Enhanced simulation framework for realisation of mobility in 6LoWPAN wireless sensor networks," *2019 28th Int. Sci. Conf. Electron. 2019 - Proc.*, pp. 1–4, 2019.

[24] Y. Qiu and M. Ma, "Secure Group Mobility Support for 6LoWPAN Networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1131–1141, 2018.

[25] X. Wang and Y. Mu, "Communication security and privacy support in 6LoWPAN," *J. Inf. Secur. Appl.*, vol. 34, pp. 108–119, 2017.

[26] G. Glissa and A. Meddeb, "6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features," *2017 13th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2017*, pp. 264–269, 2017.