SECURITY ANALYSIS OF INTERNET OF THINGS ADAPTATION LAYER

Syed Muhammad Sajjad *, Muhammad Yousaf
Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan
* Corresponding Author Email: muhammad.sajjad@riu.edu.pk

ABSTRACT: Internet of Things (IoT) is a model in which everyday elements possess built-in computational capabilities and are proficient of generating and distributing information. 6LoWPAN adaptation layer plays an important role in the realization of the concept of Internet of Things. Privacy and security is of prime concern in this paradigm. In order to ensure security in Internet of Things (IoT), it is imperative to have a comprehensive analysis of the exploits and attacks on the 6LoWPAN adaptation layer. Exploitation of the packet fragmentation process, defined in 6LoWPAN adaptation layer, can lead to fragmentation attack. Access control mechanism is required in order to prevent an attacker from gaining access to the network. The attacker can also exploit the Neighbor Discovery Process (NDP) defined in 6LoWPAN adaptation layer. In this paper we present comprehensive analysis of the exploits and attacks on the 6LoWPAN adaptation layer. We also discuss different approaches for addressing the aforementioned attacks.

Keywords: IoT, 6LoWPAN, Fragmentation Attack, Access Control.

1. INTRODUCTION

The idea of "Internet of Things" was first presented by Bill Gates in 1995, in his book entitled "The Road Ahead" [1]. Gates's perception didn't captivate considerable attention, due to limited technological development in the field of wireless communication and sensor networks. International Telecommunication Union (ITU) properly proposed the idea of the Internet of Thing in 2005 [2]. The concept was anticipated in detail by Kevin Ashton of the MIT Auto ID-Center in 2009 [3]. An environment in which sensors, actuators and computational components are implanted in daily life objects and these objects are then interconnected over a network is termed as smart environment [4]. These objects are generally resource constrained and are IEEE 802.15.4 [5] and IEEE 802.15.4e [6] compliant. Connecting these resource constrained devices to IPv6 had a plethora of challenges as the TCP/IP stack was not designed for these devices. The maximum transmission unit (MTU) of IPv6 is 1280 byte while IEEE 802.15.4 devices support maximum of 128 bytes' packets.

6LoWPAN adaptation layer was defined to make IPv6 and IEEE 802.15.4 devices compatible. Internet of Things (IoT) protocols stack [7] is shown in figure 1.

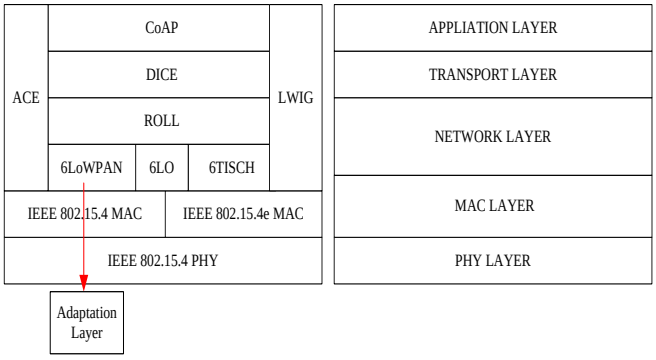

Fig. 1: (a) Internet of Things Protocol Stack (b) TCP/IP Protocol Stack

6LoWPAN adaptation layer provides fragmentation of large IP packets, compression of the IP header, neighbor discovery and stateless address auto configuration.

We intricate, in this paper, the exploitation and attacks on the 6LoWPAN protocol. The paper is arranged as follows: Section II discusses related literature. Section III offers a general idea of 6LoWPAN protocol. Section IV solicits in detail the exploitations and attacks on 6LoWPAN Protocol. Lastly, Section V concludes the paper.

2. RELATED WORK

The challenge of vulnerability detection, security assessment and evaluation in 6LoWPAN networks is addressed by a fuzzing tool suite [8]. Fuzzing scenarios for a particular node are described as per XML based defined specifications.

The XML scenario comprises of the usual messages intended to be directed to the target node as well as their corresponding responses. The tool offers rules for the injection of 6LoWPAN packets via 802.15.4 embedded driver so as to randomly alter those packets by means of an arbitrary fields or bits alterations. Penetration testing approaches and tools depict real solution for the assessment and investigation of security flaws in actual LoWPAN arrangements. An Extension to the famous Metasploit Framework is presented in [9]. The mechanism outlined can target networks in which the penetration tester gain control of one device at minimum.

Numerous traits of security in 6LoWPAN setups are analyzed by the authors of [10]. This study includes a detail discussion on security requirements in LoWPAN. Attacks at different layer of 6LoWPAN stack are also explained. Security analysis of IPv6 and IEEE 802.15.4 are performed. The authors conclude that attention must be paid towards intrusion detection and key management systems in 6LoWPAN.6LoWPAN security analysis is also carried out in [11]. It deliberates potential threats and security preferences for IPv6-over-IEEE 802.15.4 networks. But again the exploits and misuse of the 6LoWPAN adaptation layer functions are not pondered over. In this paper we present an overall, encompassing and comprehensive analysis of the exploits and attacks on the 6LoWPAN adaptation layer.

3. OVERVIEW OF 6LOWPAN ADOPTATION LAYER

IETF 6LoWPAN (IPv6 for Low-power Wireless Personal Area Network) Working Group was formed to grind the IPv6 protocol additional obligations for IEEE 802.15.4 compliant radios [12]. A document RFC 4919 [13] gives the problem statement. Transmission of IPv6 packets over IEEE 802.15.4 networks is outlined by RFC 4944 by unfolding the frame

setup, auto-configured addresses, the procedures of link-local address establishment, mesh-under routing for multi-hop IEEE 802.15.4 networks and header compression [14]. RFC 6606 offers the problem statement and routing necessities for 6LoWPANs [15]. RFC 6282 (Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks) describes unconventional header compression and updates RFC 4944 [16]. RFC 6568 (Design and Application Spaces for IPv6 over LoWPAN) explores potential application setups and uses scenarios for low-power wireless personal area networks (LoWPANs) [17]. Address resolution and Neighbor Discovery for 6LoWPAN is defined by the RFC 6775 (Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)) [18]. Low-power wireless personal area networks (LoWPANs) consist of devices that follow the IEEE 802.15.4. IEEE 802.15.4 compliant devices are regarded as low power, short range and low cost having low bit rate. Radio of these devices are restricted in their memory, computational power and energy handiness. It has a small packet size. Physical layer packet size is 127 bytes. MAC layer security enforces 9, 13 and 21 octets overhead for AES-CCM-32, AES-CCM-64 and AES-CCM-128 respectively, leaving maximum 81 octets for data Packets at link layer. On the other hand, IP has a 1280 bytes' default MTU (Maximum Transmission Unit) making it impossible to carry IP data payload on LoWPAN Link Layer. Moreover 40 byte IPv6 header would surplus the limited bandwidth of the PHY layer.

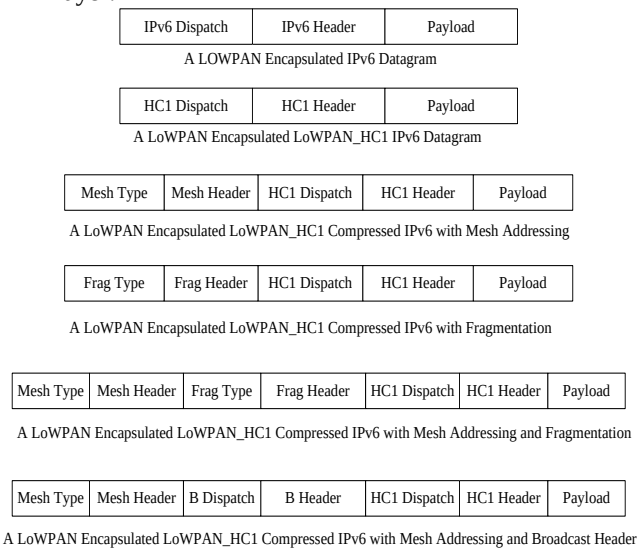

Fig. 2: 6LOWPAN Frame Format

To bridge the gap, there has to be defined a sub layer frequently called adaptation layer, having capability of packet fragmentation and reassembly. 6LoWPAN working group defines an adaptation layer in-between network layer and link layer of the protocol stack. This layer performs header compression, packet fragmentation and reassembly, multi-hop routing at link layer, neighbor discovery and addresses resolution. LoWPAN compressed datagrams are preceded with an encapsulation header stack in which it encompasses a header type and different header fields in the header stack. Figure 2 demonstrates LoWPAN header stacks used in 6LoWPAN data MPDU. These are conveyed within the frame payload of an 802.15.4. In IPv6 header, the header stack sequence is, addressing followed by hop-by-hop options, routing, fragmentation, destination options, and finally payload while a LoWPAN header contains mesh (L2) addressing, hop-by-hop selections (together with L2 broadcast/multicast), fragmentation, and lastly payload.

Table 1: Header Type and Dispatch Values

First 2 Bits	*Next 6 Bits*	*Next Header Description*
00	xxxxxx	Not a LOWPAN Header
01	000001	Uncompressed IPv6 Address Header
01	000010	LOWPAN_HC1 Compressed IPv6 Header
01	010000	LOWPAN_BC0 Broadcast Header
01	1xxxxx	LOWPAN_IPHC Compressed IPv6 Header
10	xxxxxx	Mesh Header
11	000xxx	First Fragment Header
11	100xxx	Subsequent Fragment Header

First byte of encapsulation header classifies the succeeding header. Table 1 summarizes dispatch values and corresponding next header. IPv6 packet compression is performed using the modified version of LoWPAN_HC1. Common fields (Version, TC, Flow label) are removed in order to lessen the size of the packet. IPv6 addresses are inferred from the static IPv6 link-local prefix (fe80::/64) and from the link-layer addresses present in the 802.15.4 header. The IP packet length is deduced from the length of the layer 2 frame. RFC 6282 updates RFC 4944 and describes two novel compression protocols known as LoWPAN IPv6 Header Compression (LoWPAN_IPHC) and LoWPAN Next Header Compression (LoWPAN_NHC). The LoWPAN_IPHC compression pattern implements real compression of distinctive local, global, and multi-cast IPv6 addresses, built on common conditions. A 13-bit LoWPAN_IPHC encoding field is attached to the initial 3 bits of the Dispatch value. In case some of the IPv6 header fields have to be passed in clear, they trail the LoWPAN_IPHC coding. In single hop (IPv6 link local) communication, IPv6 header is compressed to 2 bytes at minimum by LoWPAN_IPHC. The same is compressed to 7 bytes in multi-hop communication. LoWPAN_NHC encoding technique is used to compress IPv6 next-headers by 6LoWPAN. Variable-length bit-pattern indicates the compression formats of different next-headers. These variable-length straightaway follow the LoWPAN_IPHC. The order of each next header in the compressed IPv6 packet is maintained same as of its order in the original IPv6 header. RFC 6282 presents a compression plan for User Data-gram Protocol (UDP) headers by means of LoWPAN_NHC. The length field of UDP is always omitted. The length field may be inferred from the fragmentation header or from the headers of IEEE 802.15.4. Upon authorization from upper layer, checksum field may also be omitted.

The source and destination ports are compressed and subsequently carried in line. The source and destination ports follow the compression fields of LoWPAN_NHC. The resultant length of the compressed ports may vary from 8 bits to 32 bits. Partially compressed or un-compressed are also carried in-line. The order remains same as of the original

UDP header. The maximum size of the compressed UDP header may be 2 bytes, one byte for the port compression and another byte for LoWPAN_NHC encoding.

6LoWPAN also provides fragmentation and reassembly. In case an IPv6 packet does not fit in the IEEE 802.15.4 frame, it is fragmented into smaller packets. Every fragment of the fragmented packet contains fragmentation header. This fragmentation header contains data-gram tag (16 bits) and data-gram size (11 bits) fields. Data-gram offset (8 bits) field is included in the following fragment of the same IPv6 packet. The length of the entire un-fragmented IPv6 packet is termed as data-gram size. The data-gram tag ascertains the affiliation of any fragment with a specific data-gram.

A routing table is construed by the layer 3 routers. This routing table maintains the next hop information of all the destination nodes. This table also contains the network prefixes of the next hops. Link layer encapsulation is detached from the packets upon its arrival at the router. Next hop determination process is performed by matching the prefix present in the routing table. As soon as next hop is determined, the packet is re-encapsulated by the router with layer 2 trailers and headers.

4. SECURITY ANALYSIS

6LoWPAN protocol has numerous vulnerabilities that can be exploited by the attacker in order to launch security attacks. Details of such attacks are described in the following sections.

4.1. Fragmentation attack and its mitigation

The process of splitting a single large packet into various small packets is called fragmentation. IPv6 packet having maximum transmission unit of 1280 bytes is fragmented into smaller fragments at 6LoWPAN layer. The fragmentation procedure can be exploited by the attacker. An insider, standard compliant attacker possesses the capabilities of exploiting the 6LoWPAN design vulnerabilities. Such attacker can launch two types of attacks. a) Fragment Duplication Attack and b) Buffer Reservation Attack.

4.1.1. Fragment duplication attack

The receiver of a fragment cannot validate at 6LoWPAN layer as to whether the fragment is originated from the source from which the previous fragment was generated and whether the two fragments belong tSPo same IPv6 packet, making it difficult for the receiver node to distinguish between legitimate and illegitimate fragments at the reception time. Further, the receiver node proceeds all the fragments, apparently belongs to the same IPv6 packet, in accordance with the Datagram size and MAC address of the sender. An attacker may block transportation of any fragmented IPv6 packet in her surrounding area by infiltrating FRAGN for every observed packet. According to 6LoWPAN standard, a corrupt IPv6 Packet has to be dropped. This permits the attacker to enforce the target to drop the fragmented packets by injecting a duplicate FRAGN as shown in figure 3.

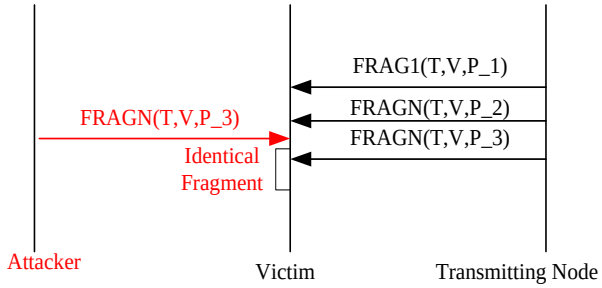

Fig. 3: Fragment Duplication Attack

4.1.2. Buffer reservation attack

The receiver of the fragmented packet performs reassembly of the fragmented packet and reserves a buffer. The size of the buffer is in accordance with the packet size as indicated in 6LoWPAN header. In case the reassembled buffer is occupied, the receiver drops the received fragments. Standard 6LoWPAN reassembly timeout is 60 seconds. Receiver drops an incomplete packet from its buffer after the expiry of this time. Attacker can exploit this by sending a fake FRAG1 with random payload as shown in figure 4. Upon receipt of this packet, the receiver will reserve a buffer for the reassembly of the packet. A nonce and timestamp based protection mechanism against these attacks is proposed by HyunGon Kim [19]. Nonce and timestamp options are being added to the fragmented packet for the security purpose.

Content chaining pattern and split buffer method with a tailor-made packet discard policy based solutions are also presented [20]. In the content chaining approach, crypto graphical verification of fragment origination is performed on per-fragment basis. Split buffer approach in conjunction with packet discard strategy provides sufficient level of protection from buffer reservation attack.

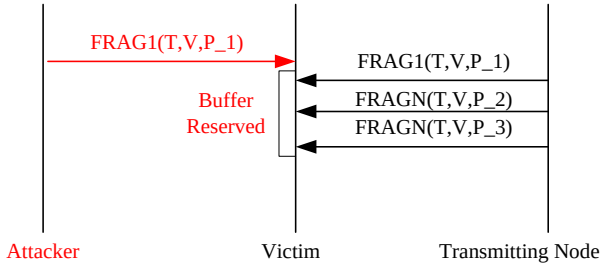

Fig. 4: Buffer Reservation Attack

4.2. Secure Neighbor Discovery

In IPv6 networks, Neighbor Discovery Protocol (NDP) [21] and Stateless Address Auto Configuration [22] are being used by both routers and nodes. These protocols facilitate the subsequent purposes:

- Getting knowledge about the prefixes and configuration parameters associated to address configuration
- Tracking down neighbor routers
- Retaining information of reachability on alive neighbors
- Detection of duplicate addresses

Neighbor Discovery Protocol (NDP) exchanges protocol messages using multicast. Keeping in view the constraint resource nature of LoWPAN devices, Neighbor Discovery Protocol (NDP) in 6LoWPAN obliges a refined approach. Neighbor discovery optimization for low power and lossy networks [18] suggests optimizations to address auto configuration, header compression, context information propagation, and duplicate address detection mechanism for low power networks. Neighbor Discovery Protocol (NDP) signaling was modified by introducing address registration mechanism as a substitution for the standard address resolution mechanism. Node address configuration related to multicast messages were interchanged with unicast messages, presenting a mechanism meant for host-originated request for Router Advertisements (RA) and removal of periodic advertisement of router using multicasting. 6LoWPAN Border Router (6LBR) has the responsibility of connecting LoWPAN to the IPv6 networks, broadcasting prefixes of IPv6 and header compression information throughout the LoWPAN. It also retains a network cache of all IPv6 addresses and 64 bit Extended Unique Identifiers (EUI-64). In this manner, 6LoWPAN Border Router (6LBR) is capable of making layer-two address resolution and carrying out Duplicate Address Detection (DAD). In addition to the Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation (RS) and Router Advertisement (RA) message types defined previously for IPv6 networks, RFC 6550 [23] defines two new Internet Control Message Protocol (ICMPv6) message types to implement Duplicate Address Detection (DAD) on 6LoWPAN networks: Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC). Upon initialization of 6LoWPAN Node (6LN) interface, a link-local address is established based on the 64 bit Extended Unique Identifiers (EUI-64) [24]. In the next step, a Router Solicitation (RS) message, demonstrating its source link-layer address, is being broadcasted by 6LoWPAN Node (6LN).

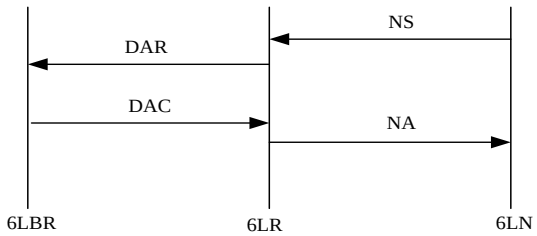

Fig. 5: 6LOWPAN Neighbor Discovery

6LoWPAN node (6LN) sends a unicast Neighbor Solicitation (NS) message to 6LoWPAN router (6LR) in order to register its configured address. The status of registration may either be successful or failure owing to a duplicated address. After that a unicast Neighbor Advertisement (NA) message is directed to the 6LoWPAN node (6LN) by the 6LoWPAN router (6LR) specifying similar status as received from the 6LoWPAN Border Router (6LBR) in the Duplicate Address Confirmation (DAC) message.

Neighbor Advertisement (NA) message has a lifetime, upon expiry of which the registration process is re-initialized. Neighbor Discovery Protocol (NDP) is not safe. If an attacker node gets knowledge of the IPv6 and the link-layer addresses earlier registered by an authentic node, through spoofing, same IPv6 addresses may be registered by the attacker either with a fabricated address or with its personal link-layer. The exploitation of these vulnerabilities causes different kind of security attacks: denial-of-service, redirection and flooded denial of service. In denial-of-service attacks, communications in-between legitimate nodes are prevented by the attacker. In redirection attacks, packets are received and re-routed to their authentic node by the malicious node. An overflow of counterfeit traffic is generated and redirected towards the victim node by the attacker in flooded denial of service attack.

In the meantime, the Secure Neighbor Discovery (SEND) protocol [25] was anticipated for IPv6 networks to safeguard Neighbor Discovery Protocol (NDP) against such attacks. The Secure Neighbor Discovery (SEND) protocol uses:

- A procedure for the verification of the router identity based on the authorization delegation detection
- A Cryptographically Generated Addresses (CGA) based verification procedure of the claimed addresses
- A Digital Signatures intended for each Neighbor Discovery Protocol (NDP) message
-

In Secure Neighbor Discovery (SEND) protocol, a Cryptographically Generated Addresses (CGA) technique is used to fix an IPv6 address to a Rivest, Shamir and Adelman (RSA) public key. All Neighbor Discovery Protocol (NDP) messages are digitally signed using this mechanism. But, RSA, due to its high computational power [25], is not appropriate for low power and resource constrained devices. To overcome this problem, the Lightweight Secure Neighbor Discovery for low-power and lossy networks (LSEND) [26] presents Cryptographically Generated Addresses (CGA) generation based on Elliptic Curve Cryptography (ECC) and signs the Neighbor Discovery Protocol (NDP) messages with Elliptic Curve Digital Signature Algorithm (ECDSA). In reality, Elliptic Curve Cryptography (ECC) offers similar level of security as RSA with considerable smaller keys [25][27]. The increase in the computational overhead of both RSA and Elliptic Curve Cryptography (ECC) is given by O(N3), where N represents the bit length. Message size and computational weight of Elliptic Curve Cryptography (ECC) and Elliptic Curve Digitally Signature Algorithm (ECDSA) is

much smaller than the message size and computational weight of RSA [28]. For each network interface a public and private key pair is generated by every node, so as to create their individual Cryptographically Generated Addresses (CGA) and to generate the digital signatures [25], essential for signing the Neighbor Discovery Protocol (NDP) messages. The digital signature is basically a hash code which depend upon the private keys of nodes, the IPv6 addresses of source as well as destination, the value of header checksum (16 bits), header type protocol (8 bits), the header of Neighbor Discovery Protocol (NDP) message and a 128 bits constant. The algorithms based on Elliptic Curve Cryptography (ECC), intend to create Cryptographically Generated Addresses (CGA) by taking three parameters: the interface public key, the 64 bits Extended Unique Identifier (EUI-64) and security parameter. No public key structure is required for both Secure Neighbor Discovery (SEND) and Lightweight Secure Neighbor Discovery for low-power and lossy networks (LSEND) protocols. Attacker nodes may possibly create and register legal Cryptographically Generated Addresses (CGA), however it cannot proceed with a Cryptographically Generated Address (CGA) formerly registered by valid node, avoiding in this manner the earlier defined attacks. As soon as a Route Advertisement (RA) message is received by 6LoWPAN Node (6LN) from 6LoWPAN Router (6LR), it starts configuring its personal Cryptographically Generated Address (CGA) and initializes the address registration procedure by directing a Neighbor Solicitation (NS) message with both the Cryptographically Generated Address (CGA) options and configured address. The 6LoWPAN Router (6LR)
accepts the Neighbor Solicitation (NS) message and starts two verification phases based on its Cryptographically Generated Address (CGA) options:

- It validates the source address by means of the claimed IPv6 source address and
- It initializes a cryptographic check of the incorporated signature in the Neighbor Solicitation (NS) message

If both phases are successful, the 6LoWPAN Router (6LR) carries on the address registration procedure. In this case, in addition to 6LoWPAN Node (6LN) IPv6 addresses, the 6LoWPAN Border Router (6LBR) also caches its public key.

4.3. Network Access Control

In 6LoWPAN networks, restricting the network access merely to qualified nodes and restraining the inflow of messages from outsider node is a critical task. Further, outsiders cannot overhear, amend or counterfeit packets from entitled nodes inside the 6LoWPAN network. 6LoWPAN needs to be capable of allowing and awarding users the entrance to the network. Alternatively, it needs to bring together statistics composed by sensors in such a manner that an unauthorized individual cannot make random enquiries. This limits the network admission merely to qualified nodes, whereas requests from strangers will not be responded to or advanced by nodes.

Right now, the access and admission to the 6LoWPAN network is considered as a stern security service in 6LoWPAN, as it may well be cast-off to circumvent mischievous nodes from gaining access to the network and instigating insider attacks. If a mischievous node is prohibited from entering the network, it cannot link with any network component and, as a result, the quantity of potential security attacks is considerably reduced. In order to grant network access only to authorized node and prevent the malicious node from exchanging data with authentic node or using the 6LoWPAN Border Router (6LBR) for communication with internet, it is imperative to imply a network admission control technique.

Administrative authorization based network access control technique is proposed by [29]. A test bed is also implemented for the validation of the proposed mechanism.

A novel network access control framework is also presented in [30]. In the suggested technique the nodes proof of identity is constructed using Cryptographically Generated Addresses (CGA), security compliance estimation of the device and mote remediation with protected faraway software installation.

The analysis is summarized in table 2.

5. CONCLUSION

The Internet of Things (IoT) is a leading development area that targets association of substances with the Internet. IEEE 802.15.4 for Low Power Wireless Personal Area Networks (LoWPANs) and IPv6, having enormous address planetary, let the integration of millions of devices to the internet. 6LoWPAN provides a suitable way out for this task. However, 6LoWPAN protocol, as it is, is vulnerable to numerous security attacks. In this paper we explore the exploitation of 6LoWPAN protocol. We also discuss different approaches for addressing the aforementioned attacks.

Table 2: Security Analysis

Process	*Exploits*	*Attacks*	*Mitigation*
Fragmentation	Fragment Duplication	Fragment Duplication Attack	Nonce and time stamp based Protection, Content Chaining [19] [20]
Buffer Reservation	Buffer Already Occupied	Buffer Reservation Attack	Split Buffer Approach [19] [20]
Neighbor Discovery	Un-authorized Entry	DoS and DDoS	Light Weight Secure Neighbor Discovery (LSEND) [26]
Network Admission	Illegal access	Internal Attacks	Network Admission Control [29] [30]

REFERENCES

[1] Gates, Bill, Nathan Myhrvold, Peter Rinearson, and Donald Domonkos. "The road ahead." (1995), Viking Penguin, ISBN 978-0-670-77289-6.

[2] Strategy, I. T. U., and Policy Unit. "ITU Internet Reports 2005: The internet of things." Geneva: International Telecommunication Union (ITU) (2005).

[3] K. Ashton. "That 'Internet of Things' thing." *RFID Journal*. [Online] June 2009. Available: http://www.rfidjournal.com/article/view/4986, (10 July 2016).

[4] Weiser, Mark, Rich Gold, and John Seely Brown. "The origins of ubiquitous computing research at PARC in the late 1980s." *IBM systems journal* 38, no. 4 (1999): 693.

[5] IEEE 802 Working Group. "IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)." *IEEE Std* 802 (2011): 4-2011.

[6] LAN/MAN Standards Committee. "IEEE Std 802.15. 4e-2012. IEEE Standards Association." *IEEE Computer Society* (2012).

[7] Sajjad, Syed Muhammad, and Muhammad Yousaf. "Security analysis of IEEE 802.15. 4 MAC in the context of Internet of Things (IoT)." In*Information Assurance and Cyber Security (CIACS), 2014 Conference on*, pp. 9-14. IEEE, 2014.

[8] Lahmadi, Abdelkader, Cesar Brandin, and Olivier Festor. "A testing framework for discovering vulnerabilities in 6LoWPAN networks." In *2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems*, pp. 335-340. IEEE, 2012.

[9] Tomasi, Riccardo, Luca Bruno, Claudio Pastrone, and Maurizio Spirito. "Meta-exploitation of IPv6-based WSNs." In *Security and Communication Networks (IWSCN), 2011 Third International Workshop on*, pp. 39-44. IEEE, 2011.

[10] Rghioui, Anass, Mohammed Bouhorma, and Abderrahim Benslimane. "Analytical study of security aspects in 6LoWPAN networks." In *Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference on*, pp. 1-5. IEEE, 2013.

[11] Park, S., et al. J. Laganier, "IPv6 over Low Power WPAN Security Analysis," Internet Draft draft-daniel-6lowpan-security-analysis-05, 2011.

[12] Vasseur, Jean-Philippe, and Adam Dunkels. *Interconnecting smart objects with ip: The next internet*. Morgan Kaufmann, 2010.

[13] Kushalnagar, Nandakishore, Gabriel Montenegro, and Christian Schumacher. *IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals*. No. RFC 4919. 2007.

[14] Montenegro, Gabriel, Nandakishore Kushalnagar, Jonathan Hui, and David Culler. *Transmission of IPv6 packets over IEEE 802.15. 4 networks*. No. RFC 4944. 2007.

[15] Kim, E., D. Kaspar, C. Gomez, and Carsten Bormann. *Problem statement and requirements for IPv6 over low-power wireless personal area network (6LoWPAN) routing*. No. RFC 6606. 2012.

[16] Hui, J., and P. Thubert. "Compression Format for IPv6 Datagrams over IEEE 802.15. 4-Based Networks, IETF RFC 6282." (2011).

[17] Kim, Eunsook, and Dominik Kaspar. "Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)." (2012).

[18] Shelby, Zach, Samita Chakrabarti, E. Nordmark, and C. Bormann.*Neighbor discovery optimization for IPv6 over low-power wireless personal area networks (6LoWPANs)*. No. RFC 6775. 2012.

[19] Kim, HyunGon. "Protection against packet fragmentation attacks at 6lowpan adaptation layer." In *Convergence and Hybrid Information Technology, 2008. ICHIT'08. International Conference on*, pp. 796-801. IEEE, 2008.

[20] Hummen, René, Jens Hiller, Hanno Wirtz, Martin Henze, Hossein Shafagh, and Klaus Wehrle. "6LoWPAN fragmentation attacks and mitigation mechanisms." In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pp. 55-66. ACM, 2013.

[21] Narten, T., E. Nordmark, and W. Simpson. *H. soliman," neighbor discovery for ip version 6 (ipv6)*. RFC 4861, September, 2007.

[22] Thomson, Susan, Thomas Narten, and Tatuya Jinmei. "IPv6 Stateless Address Autoconfiguration RFC 4862." (2012).

[23] Winter, T., P. Thuber, and B. Brandt. "RFC 6550: IPv6 Routing Protocol for Low-Power and Lossy Networks." *Internet Engineering Task Force (IETF) Request for Comments* (2008).

[24] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[25] Arkko, Jari, James Kempf, Brian Zill, and Pekka Nikander. *Secure neighbor discovery (SEND)*. No. RFC 3971. 2005.

[26] Sarikaya B., Xia F., "Lightweight Secure Neighbor Discovery for Low-Power and Lossy Networks; draft-sarikaya-6lo-cga-nd-02 (work in progress)", {\em IETF 6lo WG}, September 10,2015.

[27] Driessen, Benedikt, Axel Poschmann, and Christof Paar. "Comparison of innovative signature algorithms for WSNs."
In *Proceedings of the first ACM conference on Wireless network security*, pp. 30-35. ACM, 2008.

[28] Jian-wei, Jiang, and Liu Jian-hui. "Research on key management scheme for wsn based on elliptic curve cryptosystem." In *2009 First International Conference on Networked Digital Technologies*, pp. 536-540. IEEE, 2009.

[29] Oliveira, Luis ML, Joel JPC Rodrigues, Carlos Neto, and Amaro F. de Sousa. "Network admission control solution for 6LoWPAN networks." In*Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on*, pp. 472-477. IEEE, 2013.

[30] Oliveir, Luís ML, Joel JPC Rodrigues, Amaro F. de Sousa, and. Jaime Lloret. "A network access control framework for 6LoWPAN networks. *"Sensors* 13, no. 1 (2013): 1210-1230.