IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 08-12
www.iosrjournals.org

Security Aspects in 6lowpan Networks: A Study

Anitta Vincent[1], Fincy Francis[2], Ayyappadas P.S[3]

1) PG Scholar, DEPT Of Electronics and communication, Sahrdaya college of Engineering, Kerala, India
2) PG Scholar, DEPT Of Electronics and communication, Sahrdaya college of Engineering, Kerala, India
3) PG Scholar, DEPT Of Electronics and communication, Sahrdaya college of Engineering, Kerala, India

***Abstract**: Internet of Things (IoT) and Wireless Sensor Networks (WSNs) are an important trend in embedded computing which links the physical world to the world of information. Thus it crafts a smart world where all machines intermingle with each other automatically. 6LoWPAN is an IPv6 adaptation layer that labels means to make IP connectivity feasible for firmly resource constrained devices that use low power, lossy communication links such as IEEE 802.15.4. This paper studies 6LoWPAN with regard to its security threats and the counteractions to address these issues.*

***Keywords:** Internet of Things, Wireless sensor networks, IEEE802.15.4, 6LoWPAN, Fragmentation*

I. Introduction

Wireless Sensor Networks (WSNs) are an important trend in embedded computing. It connects the physical world to the world of information. The Internet of Things (IoT) connects existing objects to the internet. Thus it creates a smart world where all machines interact with each other automatically. The enormous amount of data collected by these objects, and the likelihood of far-off control will be a very significant benefit that will help many domains. An advantage that will marches towards this concept is that the internet infrastructure is already existing and is free to use, on the other hand, the type of devices used in this project do not support internet protocols that is already existing. 6LoWPAN is an IPv6 adaptation layer that labels means to make IP connectivity feasible for firmly resource constrained devices that use low power, lossy communication links such as IEEE 802.15.4. This paper studies 6LoWPAN with regard to its security threats and counteracts to address these issues.

This paper is organized as follows. Section II gives a quick look on WSNs. Section III is all about 6LoWPAN, its stack and packet structure etc. Section IV deals with Security threats and attacks. Section V is about various remedies suggested in the literature. Followed by is the conclusion and reference list.

II. Wireless Sensor Networks-A Quick Look

Wireless sensor networks include a collection of sensing devices that can communicate wirelessly. Each device can sense, process, and talk to its peers. Wireless sensor networks are enabled by three trends: Cheaper computation (Moore’s Law), compact sensing (MEMS sensors), and wireless networking (low-power radios). The Vision behind Sensor Networks is to embed numerous distributed sensor nodes into the physical world they exploit dense in situ sensing and actuation. We network these devices so that they can coordinate to perform higher-level identification and tasks.

Sensing node has 3 basic components: a CPU, a radio transceiver, and a sensor array. Sensor can be of any type and is interfaced through an ADC. Nodes are normally battery powered. On-board storage is present. It may have actuators, too. Hardware platforms include Low-end mote-class devices and high end-gate devices. Mote devices are used for sensing and basic processing. They are used for short-range, low-power radio applications. The high-end gateways are used for advanced processing and they interface to the outside world. Motes can talk to each other wirelessly. They get the data to a sink (one of their own). The sink is wired to a gateway. The gateway provides out-of-network connectivity (e.g., Internet) Irismote is an example for mote class device. CrossBow Stargate is an example for gate class device[10].

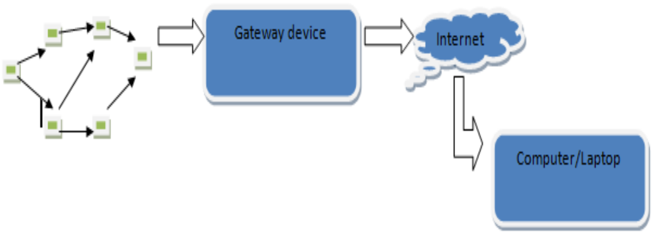

Fig. 1 A WSN based IoT

III. Overview Of 6lowpan

6LoWPAN stands for IPv6 over Low power Wireless Personal Area Networks. With the 6LoWPAN the Internet Protocol could be extended even to the smallest devices[1]. It makes possible low-power devices with limited processing capabilities to be a part of the Internet of Things.

The 6LoWPAN group has its own encapsulation and header compression mechanisms. This enables IPv6 packets to be sent and received over IEEE 802.15.4 based networks. IPv4 and IPv6 provide data delivery for LANs, MANs, and WANs. Similarly, IEEE 802.15.4 devices provide sensing and communication in the wireless domain. RFC 6282 is the base specification developed by the 6LoWPAN IETF group.

6LoWPAN stack has 6 layers and the different layers are shown in fig.1. The packet structure of 6LoWPAN is shown in fig.2

Application layer
Transport layer
Network layer
Adaption layer
Data link layer
Physical layer

Fig .2 6LoWPAN stack

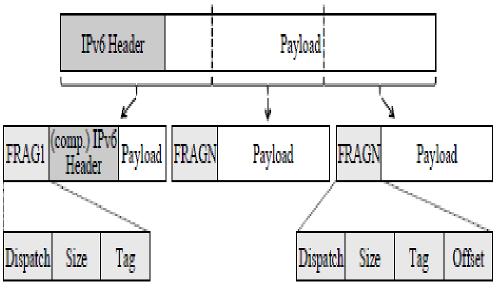

Fig.3 6LoWPAN Packet structure

IV. Security Threats

6LoWPAN is an amalgamation of two systems. So we need to analyze the attacks from the two sides on all layers of the 6LoWPAN stack. The attacks can be classified into two categories [2], internal attacks(by malicious nodes)or external attacks(by unauthorized devices). And they are classified into two categories, passive attacks (purpose to spy the network) and is difficult to detect, and active attacks can cause its malfunction eg: Denial of Service attacks.

Each layer in the 6LoWPAN stack can undergo specific attacks

1) Physical layer:

a)Jamming attack: the attacker can upset communications targeted at frequency used by nodes to communicate.

b) Tampering attack: the attacker captures and takes advantage of the node to retrieve information such as secret keys or modify its information to control the node or do some kind of spying

2) Link layer:
a) Exhaustion attack: drains the node battery as the attacker sends redundant packets in a continuous, repetitive fashion to trigger the processes in the node to make it obligatory
b) Interrogation attack: The attacker sends RTS messages in a repetitive fashion. This makes the receiver to respond with CTS messages continuously to result in energy depletion.
c) Collisions attack: the attacker sends packets with the same frequency which results in packets collision and causes the loss of information
d) Sybil attack: malicious node acts as a normal node to alter the information exchanged in the network and causes its malfunction.

3) Adaptation layer: this layer passes fragmentation and reassembly operations of 6LoWPAN packets. The main attacks on this layer are to cause disruption of these operations, modifying or rebuilding packets fragmentation.

4) Network layer:
a) Sinkhole attack: malicious node aims to divert all messages communicated to other nodes.
b) Hello flood attack: take place by sending excessive Hello messages to a node and it sends replys too, and consume more energy.
c) Black hole attack: negotiated nodes hurl received messages resulting in routing problems.
d) Sybil attack: malicious nodes create fake routes to avert the messages circulating through the network.
e) Wormhole attack: the malicious node creates a fake road to strike at the foundations of the routing within the network.
f) Spoofing attack: falsifies routing information.
g) Internet Smurf attack: the invader mimics the victim node address and sends echo messages to other nodes. Thus it floods the victim by their answers.
h) The attacks on the Neighbour Discovery protocol: affects establishing the network and the communication between nodes. A secure version of this protocol is available but it is not compatible with networks discussed. Various attacks and its security are detailed in [3].

5) Transport layer: Not many attacks target the transport layer.
a) Flooding attack: the attacker tries to exhaust the energy of the victim node via multiple connection requests.
b) De-synchronization attack: Attacker forces the victim to react with synchronization messages imitating error messages

6) Application layer:
a) The Overwhelm attack: destroys the routing by producing enormous traffic to the Edge Router
b)Path-based Dos attack: intended to deplete resources by injection of fake messages.

Some fragmentation attacks are listed in [8]. The 6LoWPAN has an adaptation layer between the network and the link layer. It offers header compression and packet fragmentation for IPv6 packets. There can be two attacks that a malicious node can accumulate against the 6LoWPAN layer. First, is a fragment duplication attack where the overhearing attacker prevent the successful processing of fragmented packets in a reactive manner by replicating an overheard fragment. Second, is the buffer reservation attack where an attacker without eavesdropping capabilities blocks processing of any fragmented packet at the target node in a pro-active manner. This is done by sending a single 6LoWPAN fragment [8].

V. Security Measures

The security in the 6LoWPAN networks are must be confidential which limit data access only to authorized users, Integral which means data must not be changed during transmission, authentic which is a term related to reliability of the data transmitter, available, capable of detecting malicious intrusion. We will analyze the two main components of the 6LoWPAN system: IEEE 802.15.4 standard and IP addressing. The IEEE 802.15.4 defines eight types of security [4]. These are located in the data link layer and all of them are based on the AES (Advanced Encryption Standard), these types are: encryption only (AES-CTR), only authentication (AES-CBC-MAC) or encryption and authentication (AES-CCM).

IPv6 stands for Internet Protocol Version 6 and is designed for non-low-resource devices. The security protocol IPSec (Internet Protocol Security) [5] works well on these devices, on the other hand it is very greedy to 6LoWPAN devices. IPSec describes two security modes: AH (Authentication Header) and ESP (Encapsulating Security Payload). AH provides integrity and authentication whereas ESP provides integrity and confidentiality. IPSec also requires another header (AH or ESP) in each packet. So it is difficult to use in 6lowpan environments. IPSec requires sender and receiver communicate to share a secret key . This is implemented dynamically with IKE (Internet Key Exchange) protocol [6]. IPv6 uses NDP (Neighbour Discovery Protocol) messages. This helps communications. The secure version of NDP is SeND (Secure ND based on asymmetric cryptography which is not compatible with 6LoWPAN devices. A new protocol LSeND (Lightweight Secure Neighbour Discovery for Low-power and Lossy Networks) is suggested in [7] which can adapt to this kind of network.

Some security measures in literature are given below:

To protect resource-constrained devices against these attacks, we propose two complementing, Two lightweight mechanisms to protect the resource constrained devices are stated in[8].One of them is the content-chaining scheme alleviate the fragment duplication attack by contributing efficient sender authentication per fragment. Besides, there can be a split buffer approach cultivates competition for the limited buffer resources between lawful nodes and an attacker on a per-packet basis. Packet discard strategy for the split buffer purges packets with doubtful sending activities from the buffer in case of a buffer overload situation.

A Key Management System is mentioned in [9]. Cryptographic keys are of two types namely public keys and private keys. The public key cryptography consumes a lot of energy, making it unsuited with 6LoWPAN networks. But for 6LoWPAN networks that have two fields of involvement, internal communications between nodes, in particular the communication between the host nodes and router nodes (within the network LoWPAN), and between nodes and Edge Router and, communications with external IP hosts via the Internet, there is the possibility to use public key cryptography in machines that have enough power to use, especially in communications between internal and the external networks. The private key cryptography is most convenient in 6LoWPAN since it does not consume much energy. But there is not a pattern defined by this standard. Several studies have been conducted to find valid solutions, several suggestions were proposed based on the proposed schemes for WSNs, among them. Key management system in LoWPAN is a wide research field. Four major frameworks of KMS are key pool framework, mathematical framework, negotiation framework and public key framework. Cluster based dynamic key management schemes seem the most appropriate.

Intrusion Detection is a security approach that is based on analyzing network data .

This is done in order to detect signs of intrusion to trigger an alarm and discover the anomaly. There are no IDS implementations in 6LoWPAN networks, but it can be very beneficial for this type of network in addition to cryptography. Since 6LoWPAN combines between IEEE 802.15.4 and IPv6, we will need a specific IDS system has the ability to monitor the traffic of two sides.

VI. Conclusion

This paper studied 6LowPAN based on its security parameters and presented various attacks a network is susceptible to, and attacks for each layer of the 6LoWPAN stack. Also some methods recommended in literature for network safety is also reviewed. This can solve majority of problems. Major of these security measures include Key Management System and Intrusion Detection System. 6LoWPAN network security remains a major challenge and should be studied of these different sides to find suitable and adequate solutions.

Reference

[1]. Mulligan, Geoff, "The 6LoWPAN architecture", EmNets '07: Proceedings of the 4th workshop on Embedded networked sensors, *ACM*, 2007

[2]. S. Park, K. Kim, W. Haddad, S. Chakrabarti, J. Laganier, IPv6 over Low Power WPAN Security Analysis, draft-daniel-6lowpan-security-analysis- 05, Mar. 15, 2011, Expires: Sept. 16, 2011

[3]. J. Arkko, J. Kempf, B. Zill, P. Nikander, Secure Neighbour Discovery (SEND), Request For Comments(RFC): 3971, Mar. 2005

[4]. Y. Xiao, HH. Chen, B. Sun, R. Wang, S. Sethi, MAC Security and Security Overhead Analysis in the IEEE 802.15.4Wireless Sensor Networks, Hindawi Publishing Corporation, EURASIP Journal on Wireless Communications and Networking, May 2006

[5]. R. Thayer, N. Doraswamy, R. Glenn, IP Security Document Roadmap, Request For Comments(RFC): 2411, Nov. 1998

[6]. C. Kaufman ,Internet Key Exchange (IKEv2) Protocol, Request For Comments(RFC): 4306, Dec. 2005

[7]. B. Sarikaya, F. Xia, G. Zaverucha, Lightweight Secure Neighbour Discovery for Low-power and Lossy Networks, draft sarikaya-6lowpan-cgand- 03, Apr. 30, 2012, Expires: Nov. 1, 2012

[8]. René Hummen, Jens Hiller, Hanno Wirtz, Martin Henze, Hossein Shafagh, Klaus Wehrle, "6LoWPAN Fragmentation Attacks", WiSec'13, April 17-19, 2013, Budapest, Hungary. Copyright 2013 ACM 978-1-4503-1998-0/13/04

[9]. Anass RGHIOUI, Mohammed BOUHORMA, Abderrahim BENSLIMANE, "Analytical study of security aspects in 6LoWPAN networks", 2013 5th International Conference on Information and Communication Technology for the Muslim World.

[10]. Bhaskar Krishnamachari, "An Introduction to Wireless Sensor Networks", Second International Conference on Intelligent Sensing and Information Processing (ICISIP), Chennai, India, January 2005.