2015 Fifth International Conference on Communication Systems and Network Technologies

A survey on Techniques for Securing 6LoWPAN

Saniya Vohra
ME student, Computer Engineering
Parul Institute of Engineering and Technology
Vadodara, India
saniyavohra.sv@gmail.com

Rohit Srivastava
Asst. Professor, Computer Science and Engineering
Parul Institute of Engineering and Technology
Vadodara, India
rts080185@gmail.com

***Abstract*— The integration of low power wireless personal area networks (LoWPANs) with the Internet allows the vast number of smart objects to harvest data and information through the Internet. Such devices will also be open to many security threats from Internet as well as local network itself. To provide security from both, along with Cryptography techniques, there also requires certain mechanism which provides anonymity & privacy to the communicating parties in the network in addition to providing Confidentiality & Integrity. This paper provides survey on techniques used for securing 6LoWPAN from different attacks and aims to assist the researchers and application developers to provide baseline reference to further carry out their research in this field.**

Keywords*— *6LoWPAN, IEEE 802.15.4, Internet of Thing, IPv6, IDS, IPsec, MT6D

I. INTRODUCTION

Low power wireless personal area networks comprises of the IEEE 802.15.4 devices that have short range, small size, low cost, low power consumption and low processing capabilities. A LoWPAN typically includes devices that work together to connect the physical environment to real-world applications, e.g., wireless sensors [1]. Such resource constrained devices were previously impractical to be processed with Internet protocol presuming that IP was too memory and bandwidth intensive and these low cost nodes must operate unattended for multiyear lifetimes on modest batteries [3]. With the IP support , the routing process can operate either at link layer and/or at IP network layer. Therefore, it creates new opportunities to define routing protocols that fit to the LoWPAN purposes.

Without an IP-based architecture, allowing communication of such constrained devices over the Internet require an application layer gateways, which are very complex to design and manage. Hence, the Internet Engineering Task Force (IETF) created Working Groups (WGs) called 6LoWPAN to standardize necessary adaptations of IPv6 for networks that use the IEEE 802.15.4 physical (PHY) layer, and has defined how to carry IPv6 datagrams over IEEE 802.15.4 links [2].

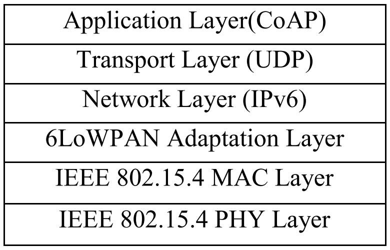
Authors in [3] also presented several challenges for supporting IPv6 over LoWPAN networks. First, IPv6 datagrams do not fit for LoWPAN due to their MTU requirements. If standard IPv6 headers are used over LoWPANs, it will result into small payloads for higher level protocols. Second, as 802.15.4 is both low power and low throughput, it is more prone to link failures and interferences. Also, IEEE 802.15.4 devices do not support for multicast and flooding due to their power and bandwidth requirements. And current IP routing solutions may not be easily applicable to such multihop mesh networks. These challenges were addressed by IETF 6LoWPAN Working Group.

II. 6LOWPAN OVERVIEW

The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices," and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things. A straightforward technical definition of 6LoWPAN would be: 6LoWPAN standards enable the efficient use of IPv6 over low-power, low-rate wireless networks on simple embedded devices through an adaptation layer and the optimization of related protocols [4].

For tackling the problems addressed in Section I, 6LoWPAN designs an adaptation layer between the link and network layer which allows IPv6 packet transmission over IEEE 802.15.4 links. A typical 6LoWPAN Layered Stack is shown in *Fig. 1.* 6LoWPAN fulfils two primary elements:

- Header Compression: IPv6 header fields can be eliminated from a packet at network layer and derived from the link layer frames.
- Fragmentation: IPv6 minimum MTU requirement is 1280 bytes and IEEE 802.15.4 supports for 127 bytes [12]. Hence to allow the cross-communication, fragmentation is done by 6LoWPAN Layer.



Application Layer(CoAP)
Transport Layer (UDP)
Network Layer (IPv6)
6LoWPAN Adaptation Layer
IEEE 802.15.4 MAC Layer
IEEE 802.15.4 PHY Layer

Fig. 1 6LoWPAN Layered Stack

A. *6LoWPAN Architecture*

To provide routing solution for 6LoWPAN was biggest challenge. There are certain routing requirements which 6LoWPAN routing protocol must satisfy like support for different communication & different traffic patterns, scalability, security, performance and routing in different

978-1-4799-1797-6/15 $31.00 © 2015 IEEE
DOI 10.1109/CSNT.2015.163

network condition. Traditional MANET protocols like OLSR(Optimized Link State Routing), RIP(Routing Information Protocol), DSDV(Destination-Sequenced Distance Vector), DSR(Dynamic Source Routing) etc. were unable to satisfy these requirements. Hence ROLL Working Group proposed new Routing Protocol for low power and lossy networks called RPL considering these requirements. RPL deals with limited resources, link failures, traffic control cost and it also considers node and link properties at the time of path selection. *Fig. 2* shows 6LoWPAN Architecture where WSN nodes act as a host or intermediate router that transmit packets. Through the Local border router communication happens between a node in WSN network and a host from Internet [5].

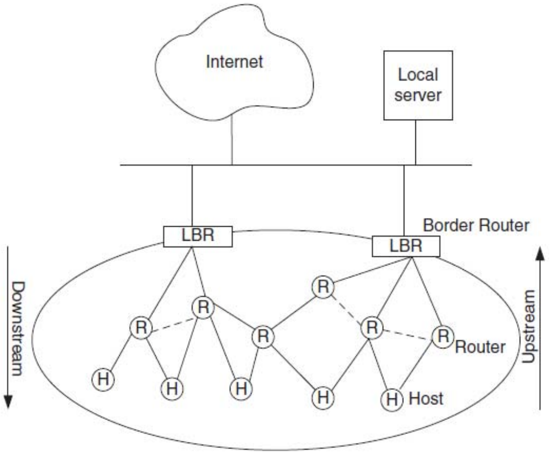


Fig. 2 6LoWPAN Architecture[5]

B. Security Threats in 6LoWPAN

As stated in [6], Security is a trade-off and costly in low rate WPAN. Also, traditional security techniques cannot be directly applied due to the inherent properties of 6LoWPAN. Attacks can be classified into external and internal attacks. External attacks can be possible from the Internet as well as from malicious nodes in other network. Internal attacks happen within the network by insider malicious nodes.

External attacks can be prevented by Cryptography mechanism but Internal attacks are hard to detect and prevent. Some of the attacks like Intrusion, Sinkhole attack and Replay attack harm the network operation and lead to several other attacks. Also, several types of DOS attack from Internet side can be possible which cryptography cannot deal with [6].

Main task of 6LoWPAN is fragmentation. So, while performing this procedure, several fragmentation attacks like Tiny fragmentation, Ping of Death etc. can lead the sensor node to critical damage. As discussed in [5], RPL is also vulnerable from Internal attacks. RPL follows some rules for optimizing network operation which again leads to Rank attack, Local Repair and Resource depletion attack.

Different attacks can be possible at each layer of 6LoWPAN Stack. This paper mainly focus on threats possible at 6LoWPAN Layer and the Security mechanism which is used till now in such resource constrained network to prevent it from those attacks.

III. Techniques used to secure 6LoWPAN

Till now several mechanism are deployed for securing different types of attacks against 6LoWPAN. This section provides brief survey of those techniques.

A. Compressed IPsec

IPsec provides end-to-end security at network layer. It includes two protocols: AH(Authentication header) that provides authentication and integrity of Source IP datagram and ESP(Encapsulating Security Payloads) which ensures confidentiality, integrity and source authentication. It also includes some rules that perform AH and ESP operations [8]. Both protocols can be implemented in either transport or tunnel mode but tunnel mode is impractical in case of 6LoWPAN.

IPsec requires header compression to be compatible to 6LoWPAN packet size. Authors in [7] proposes header encodings for AH and ESP extension headers and demonstrated that it is feasible to use compressed IPsec to secure communication between sensor nodes and hosts in the Internet. For this, they used already defined NHC Encoding for IPv6 Extension headers as shown in *Fig. 3*. This NHC encoding is defined for AH and ESP as shown in *Fig. 4* and *Fig. 5*.

0	1	2	3	4	5	6	7
1	1	1	0	EID			NH

EID: Extension Header ID
NH: Next Header

Fig. 3 LoWPAN_NHC header for Extension[8]

0	1	2	3	4	5	6	7
1	1	0	1	PL	SPI	SN	NH

PL: Payload Length
SPI: Security Parameter Index
SN: Sequence Number
NH: Next Header

Fig. 4 NHC header for AH [8]

0	1	2	3	4	5	6	7
1	1	1	0	SPI	SN	–	NH

SPI: Security Parameter Index
SN: Sequence Number
NH: Next Header

Fig. 5 NHC header for ESP[8]

It is also possible to use combined AH and ESP headers. Also, the NHC_ESP performs encryption for security. The drawback of compressed IPsec is that its encryption is resource intensive and increases overhead. Also, it doesnot provide security against eavesdropping and network-side attacks like DOS attack. Moreover, Combined AH & ESP approach becomes too heavy for LoWPAN nodes.

To securely communicate with 6LoWPAN node, an automatic key sharing protocol is required. Hence, Researchers in [9] proposed a lightweight IKEv2 scheme for compressed IPsec. It is a protocol for exchanging session keys between two nodes. It is based on ECC (Elliptic Curve

Cryptography) and uses Diffie-Hellmann protocol for key exchange.

B. Protection Mechanism against Fragmentation attacks

6LoWPAN adaptation layer defines fragmentation due to the large packet sizes of IPv6. Authors in [10] focused on security threats being occurred by fragmentation and re-assemble at the 6LoWPAN adaptation layer. There are various ways in which attackers can use fragmentation to infiltrate and cause a denial of service and replay attack to networks. Also, attackers can change or re-construct the packet fragmentation fields like datagram_size, datagram_tag & datagram_offset [12]. This can lead the sensor nodes to suffer from re-assemble buffer overflow and resource exhaustion. To protect against such attacks, authors in [10] proposed a mechanism of adding Timestamp and Nonce to each fragmented packets at 6LoWPAN layer. This will provide protection against replay attacks. Timestamps are used for unidirectional fragmented packets and Nonce are used for bidirectional fragmented packets between sensor nodes.

Authors in [11] addressed fragment duplication and buffer reservation attack. For this, they proposed two different scheme called Content-chaining and Split Buffer Approach. Fragment duplication means preventing the processing of fragmented packets by duplicating an overheard fragment. Buffer reservation means blocking the processing of any fragmented packet by sending a single 6LoWPAN fragment.

In content-chaining scheme, at the end of each fragment, cryptographic hashed value of next fragment is stored as shown in *Fig. 6*. This value is verified every time when the fragment is received. Hence target nodes can able to detect whether the fragment is spoofed or not. Thus preventing from fragment duplication. Split-Buffer approach increases the cost for an attacker to send his fragments in short period in order to prevent an authorized fragment from getting processed [11]. This is achieved by splitting buffer into slots of 6LoWPAN fragment size. These slots are filled until complete packet is received. Then it gets reassembled in order or gets discarded in case of buffer overload. Its disadvantage is that, it still allows a node to process interleaved packet that combined, would otherwise exceed the overall buffer resources. That means if intermediate fragment is malicious due to which the buffer gets overflows, it won't be detected and simply discard that fragment because of buffer limit.

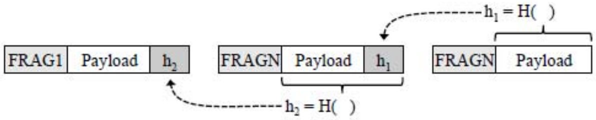


Fig 6. Content chain for packet consisting three fragments[11]

C. Detection Scheme for Botnet attack

In 6LoWPAN, attack can be possible from Internet also. One of its types is botnet attack which modifies the data and sends the wrong data to the user node. Author in [13] analysed that Botnet is the powerful attacking tool in 6LoWPAN and proposed detection mechanism for the same with some assumptions. They designed a Bot Analysis module (Fig. 7) and implemented in 6LoWPAN gateway so that all packet that passes from the gateway are analysed to find the malicious traffic.

The disadvantage of this mechanism is it increases the overhead on gateway device due to additional module and every packet gets checked independently which creates load on gateway device. It can decrease network performance for higher number of nodes in 6LoWPAN.

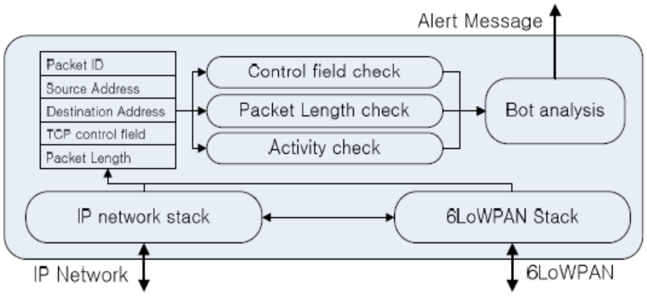


Fig. 7 Botnet Detection Module in 6LoWPAN Gateway[13]

D. IDS Approach for Internal/DOS attacks

Apart from the External attacks, there are certain Internal attacks possible in 6LoWPAN like DOS attack which makes network unavailable for indefinite period and makes jamming and power exhaustion. Authors in [5] analysed that Cryptography alone cannot provide total security due to the weak nature of LoWPANs. Hence an IDS approach is required to monitor the malicious activity in the network and acknowledge the sign of attack by raising an alarm.

The IDS are often divided by misuse, anomaly-based and specification-based types. 6LoWPAN combines 802.15.4 and IPv6 so its IDS should support traffic patterns from both. Hence, Combination of anomaly and specification-based is promising solution for 6LoWPAN [5]. They also designed RPL Specification-based IDS in combination with statistical anomaly technique in which former focuses on protecting RPL control messages and routing information, thus securing network topology and latter is used to secure node performance.

Authors in [14] listed different types of DOS attacks like Spoofing, Sybil, Selective forwarding, Wormhole, Sinkhole, Replay, Overload and Hello Flood that can disrupt the operation and performance of RPL routing protocol. To counter these attacks, the authors introduced IDS that can limit the number of transmitted and received message among the nodes based on network usage. If the limits exceeds, messages are isolated from the network. Hence if a legitimate message enters in the network after the limit occurs, then it is also discarded which is a drawback of this system. It is worth noting that, Authors have also discussed about the suitable approach where IDS agents can be implemented as well as focussed on the parameters that IDS needs to monitor to deal with DOS attacks [14].

The problem with such IDS solutions is that different IDS are required for different traffic patterns. Also, in such resource constrained network like 6LoWPAN, combined IDS is required which can add extra load to low power nodes.

E. MT6D to secure 6LoWPAN

Authors in [15] proposed a new mechanism for security called MT6D(Moving Target IPv6 Defense). They analysed that the static addressing of the nodes is the basic reason for any kind of attacks. Hence, MT6D concept was evolved with the idea of changing senders and destination IPv6 addresses so that attacker would not able to recognize the address of two communicating parties within the network. The main goal of MT6D was to maintain privacy, anonymity and protection against targeted network attacks like DOS and MITM (Man-In-The-Middle) attacks. The technique was applicable to live IPv6 network but required to be optimized to be used for resource constraint networks. Authors in [16] accomplished this and proposed the optimized version of MT6D by changing the interpreted python code to compiled C code. Significant improvements were achieved in terms of Bandwidth, Packet loss and Latency which concludes that C version of MT6D can be deployed in resource constrained environments.

Finally, Authors in [17] created a physical test bed to check the performance of MT6D for securing 6LoWPAN in Internet of Thing as shown in *Fig. 8*. They analysed that implementing such scheme on low power devices will add an additional layer of security. They implemented the structure of MT6D on Contiki OS running on a sensor node named tmote sky. The intent was to calculate the latency of packet transfer between laptop and sensor node and it was turn out to be high. It was concluded by the author that implementing MT6D on a sensor node will provide end to end security as well as it will reduce the latency. This work needs to be evaluated and more parameters should be calculated like packet loss and memory overhead so that one can decide its feasibility and scalability for wide scale applications.

The technique MT6D can greatly provide security from various attacks that can happen in 6LoWPAN. It is necessary to re-design this technique or optimize its code to be used with low power sensor nodes so that it does not degrade the network performance or increase memory overhead.

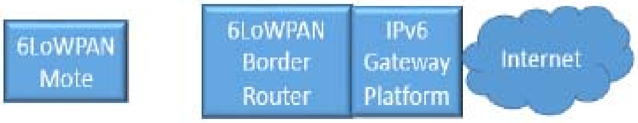


Fig. 8 6LoWPAN Test Bed[17]

IV. ANALYSIS OF DIFFERENT 6LOWPAN SECURITY TECHNIQUES

From the survey of 6LoWPAN Security, we have studied that different mechanism are proposed for particular types of attacks. In some paper, specific methods are designed to defend against attacks like fragmentation & re-assembly buffer and botnet attack. Also, different IDS Solutions are combined to fulfil the security requirements of 6LoWPAN. More or less each technique has its specific advantages and limitations considering which it is used in various applications. Among all, MT6D is the only technique which provides security solution from both Internal as well as External attacks. Hence, making usage of such strong technique is recommended in 6LoWPAN. For this, MT6D needs to be fully implemented in such resource constrained nodes and network performance should be analysed. Further the table shows short description about the techniques which helps in comparison.

TABLE I. COMPARISION OF PROPOSED TECHNIQUES

Research Proposal	Operational Layer	Security Properties	Technique Description
[7]	6LoWPAN Adaptation Layer	Confidentiality, Integrity and Authentication.	AH and ESP Header Compression using NHC Encoding for IPv6 Extension headers.
[9]		Protection of Shared Keys.	Automatic key exchange protocol based on ECC and Diffie Hellmann for use with Compressed IPsec.
[10]		Protection against Fragmentation replay attacks.	Addition of Timestamp and Nonce at each fragment for unidirectional & bidirectional packets.
[11]		Protection against Fragmentation and Buffer Reservation Attack.	Addition of hashed value at the end of each fragment. Splitting the Buffer into slots to set the limit for an attacker.
[13]		Protection against Botnet Attack.	Adding the Bot Detection Module to detect the malicious traffic in the network.
[5,14]		Protection against Internal/DOS attack.	Combined IDS Solution for detecting different network's traffic patterns.
[17]		Privacy & Anonymity	Rotating nodes addresses frequently to limit the attacker's time to track the address.

V. CONCLUSION & FUTURE WORK

Security is a prime concern in any network. With the addition of new layer that is 6LoWPAN; additional attack also came into picture. In this paper, we have undergone the survey on some of this attack and the Security mechanism that has been proposed till now to defend against them. All techniques have their own advantages and disadvantages. Some of them focuses in achieving Confidentiality and Integrity while some focuses in achieving privacy. It is necessary that security mechanism should consider attacks from both sides internally as well as from external network. One of such technique MT6D is also surveyed in this paper. Future enhancement is to study the implementation of such technique to make it deployable in low power nodes maintaining network performance.

ACKNOWLEDGMENT

We take immense pleasure in expressing our humble note of gratitude to our project guide Mr. Rohit Srivastava, Assistant Professor, Department of Computer Science and Engineering, Parul Institute of Engineering and Technology, for his remarkable guidance and useful suggestions, which helped us in completing the paper before deadline.

REFERENCES

[1] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, August 2007.

[2] JeongGil Ko and Andreas Terzis, Stephen Dawson-Haggerty and David E. Culler, Jonathan W. Hui, Philip Levis, “Connecting Low-Power and lossy Networks to the Internet”, 2011 IEEE Communications Magazine.

[3] J. Hui and D. Culler. Extending IP to Low-Power, Wireless Personal Area Networks. Internet Computing, IEEE, 2008..

[4] Shelby Z, Bormann C. 6LoWPAN: The Wireless Embedded Internet. Wiley-Blackwell: West Sussex, United Kingdom, 2009.

[5] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Mahdi Aiash, and Yuan Luo. 2012. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. Int. J. Commun. Syst. 25, 9 (September 2012), 1189-1212. DOI= http://dx.doi.org/10.1002/dac.2356.

[6] S. Park, K. Kim, W. Haddad, S. Chakrabarti and J. Laganeir, “IPv6 over Low Power WPAN Security Analysis draft-daniel-6lowpan-security-analysis-04”, March 2010.

[7] Raza, S.; Duquennoy, S.; Chung, T.; Yazar, D.; Voigt, T.; Roedig, U., "Securing communication in 6LoWPAN with compressed IPsec," Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on Distributed Computing in Sensor Systems, pp.1-8, 27-29 June 2011.

[8] Christine Hennebert, Jessye Dos Santos, “Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis”, 2013 IEEE Internet of Things Journal.

[9] Shahid Raza, Thiemo Voigt, Vihelm Jutvik, “Lightweight IKEv2: A key management solution for both the compressed IPsec and the IEEE 802.15.4 security”, Workshop of SmartObject Security, Paris, France, 23 March 2012.

[10] H. Kim. Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer. In Proc. Of ICHIT, 2008..

[11] René Hummen, Jens Hiller, Hanno Wirtz, Martin Henze, Hossein Shafagh, and Klaus Wehrle. 2013. 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, 55-66. DOI= http://doi.acm.org/10.1145/2462096.2462107.

[12] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, 2007.

[13] Cho EJ, Kim JH, Hong CS. Attack model and detection scheme for Botnet on 6LoWPAN. Proceedings of the 12th Asia-Pacific Network Operations and Management Conference on Management Enabling the Future Internet for Changing Business and New Computing Services, Springer-Verlag: Jeju, South Korea, 2009; 515–518.

[14] Anass RGHIOUI, Anass KHANNOUS, Mohammed BOUHORMA, “Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition”, Journal of Advanced Computer Science and Technology, 3 (2) (2014) 143-153.

[15] M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront (2011), “MT6D: a moving target IPv6 defense,” *MILCOM 2011*, pp.1321-1326, 7-10 Nov.

[16] Owen Hardman, Stephen Groat, Randy Marchany, and Joseph Tront, “Optimizing a Network Layer Moving Target Defense for Specific System Architectures” 978-1-4799-1640-5/13/$31.00, 2013 IEEE.

[17] Matthew Sherburne, Marchany Randy and Joseph Tront, “Implementing Moving Target IPv6 Defense to Secure 6LoWPAN in the Internet of Things and Smart Grid”, April 2014, ACM 978-1-4503-2812-8/14/04.