Implementing Moving Target IPv6 Defense to Secure 6LoWPAN in the Internet of Things and Smart Grid

[Extended Abstract]

Matthew Sherburne, Randy Marchany, and Joseph Tront
IT Security Lab
Bradley Department of Electrical Engineering and Computer Engineering
Virginia Tech
Blacksburg, VA 24061
{msherbur, marchany, jgtront}@vt.edu

ABSTRACT
The growing momentum of the Internet of Things (IoT) has shown an increase in attack vectors within the security research community. We propose adapting a recent new approach of frequently changing IPv6 address assignment to add an additional layer of security to the Internet of Things. We examine implementing Moving Target IPv6 Defense (MT6D) in IPv6 over Low-Powered Wireless Personal Area Networks (6LoWPAN); a protocol that is being used in wireless sensors found in home automation systems and smart meters. 6LoWPAN allows the Internet of Things to extend into the world of wireless sensor networks. We propose adapting Moving-Target IPv6 Defense for use with 6LoWPAN in order to defend against network-side attacks such as Denial-of-Service and Man-In-The-Middle while maintaining anonymity of client-server communications. This research aims in providing a moving-target defense for wireless sensor networks while maintaining power efficiency within the network.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – *Security and protection;* C.4 [**Performance of Systems**]: Reliability, availability, and serviceability

General Terms
Security, Design

Keywords
6LoWPAN, IPv6, Wireless Sensor Networks, Internet of Things

1. INTRODUCTION
The IoT is beginning to take off thanks, in part, to the global implementation of IPv6, improvements in the 6LoWPAN standard, and an operating system optimized for low-powered devices known as ContikiOS. These devices that make up the IoT, such as temperature sensors and power sensors, can report sensitive data and therefore should have more security.

We will discuss the background of research into the security of 6LoWPAN, IPv6, MT6D, and 6LoWPAN in Section 2. In Section 3 we will discuss a typical 6LoWPAN design and our 6LoWPAN test bed design. Section 4 will discuss our analysis of how TCP communications over 6LoWPAN occur. Finally Section 5 and 6 presents our Future Work and Conclusion.

2. BACKGROUND
Why should the IoT, including Home Automation, Industrial, and Smart Grid applications, be protected with MT6D? We need to look at how the Internet of Things connects to the Internet and security risks associated with 6LoWPAN and IPv6. Authors in [11] discuss a security framework in protecting the modern home that may contain numerous Internet-connected devices. It is clear that devices in the home, as well as industry, need to be protected and secured in order for data to remain confidential, available, and with integrity. Attackers could use the data to perform reconnaissance on a household or perform more malicious actions such as draining the battery power of the low-powered devices with Denial-of-Service attacks. Attackers could also carry out more nefarious schemes such as setting a thermostat further than the normal for the season and result in a higher energy bill for the home or business owner.

Researchers in [1] examined security risks in the routing protocols and adaption layers contained in 6LoWPAN. They proposed an Intrusion Detection System in order to monitor malicious activity instead of relying on cryptography alone. An IDS within 6LoWPAN should be able to monitor the backbone network to the border router and within the 6LoWPAN network in order to detect malicious behavior internal or external. Researchers in [8] expanded known IPv6 fragmentation attacks to 6LoWPAN. They propose the use of a content-chaining scheme to prevent fragment duplication attacks and the split buffer approach to prevent buffer reservation attacks. Authors in [7] wanted to enable IPsec communications directly on a 6LoWPAN device by using compression much like how 6LoWPAN compresses the IPv6 header. Implementing a compressed form of IPsec allows end-to-end integrity and confidentiality of the communications in a 6LoWPAN design, but side-channel analysis attacks can still correlate this data enough to determine if a wireless device on the Internet of Things is transmitting data in such a way, duration, or periodicity to reveal more information to attackers. Researchers

CISR '14, Apr 08-10 2014, Oak Ridge, TN, USA
ACM 978-1-4503-2812-8/14/04.
http://dx.doi.org/10.1145/2602087.2602107

in [10] proposed the use of Moving Target IPv6 Defense to defend the Smart Grid by rotating the IPv6 addresses of the source and destination host devices, yet they did not specifically address how to implement such a resource intensive scheme on low-powered devices within 6LoWPAN. We plan to further carry out this work within 6LoWPAN in order to add an additional layer of protection to the Internet of Things.

2.1 IPv6

IPv6, developed by the Internet Engineering Task Force, was developed in response to IPv4 address exhaustion and to incorporate additional security such as IPsec. The main specification, RFC 2460 [2], extends the size of the IP address from 32-bits in IPv4 to 128-bits. The sheer size of the IPv6 address space scales perfectly with the ability to assign an IP address to all the devices that will be a part of the Internet of Things.

2.2 Moving Target IPv6 Defense

Researchers from Virginia Tech, M. Dunlop et. al [5] developed a technique to dynamically assign changing IPv6 addresses in order to obfuscate communications between two hosts. This is analogous to frequency hopping in the radio communications. Taking advantage of the immense address space in a /64 subnet, the researchers were able to conduct both UDP and TCP communications with great success. In their implementation using Guru Plugs, they were able to send a 500 MB file rotated across 500 different IP addresses with below 3% packet loss. MT6D tunnels the encrypted payload of data through UDP and requires a total of 62 Bytes in overhead: adding 40 Bytes to the IPv6 header, 8 Bytes to the UDP header, and 14 Bytes to the Ethernet frame. Their implementation not only encrypts the packets, but it also keeps attackers from being able to follow the communications to conduct side-channel analysis because the IP addresses of the source and destination are constantly rotating on a completely random basis.

2.3 6LoWPAN

Low-powered wireless sensor networks have been around since 2003 when IEEE developed the standard for low-data rate transmission between low-powered devices called 802.15.4. UC Berkeley helped design Moteiv's Tmote Sky that became one of the most popular wireless sensor platforms on the market at the time. Yet, these platforms did not yet have access to the IP layer. It was not until RFC 4919 [4] and RFC 4944 [6] that researchers began to tackle the problem of assigning IP addresses to these devices projected to number in the millions. It was clear that IPv6, with the ability to provide 667,000 addresses to every square nm of the Earth's surface, would be needed if the Internet of Things was going to truly be a part of the Internet. The base specification of 6LoWPAN, RFC 6282, came in September 2011 [3]. An update to the 6LoWPAN Neighbor Discovery process came with RFC 6775 [9].

3. 6LoWPAN DESIGN

3.1 TYPICAL DESIGN

A typical 6LoWPAN design includes an edge border router that connects the 802.15.4 wireless sensor network to an IPv6 network. A series of motes that run the 6LoWPAN protocol can either connect directly to the 6LoWPAN border router or relay through other motes in an ad-hoc mesh network. The border router itself is usually an identical mote that is connected to a larger computing platform such as a laptop. The 6LoWPAN border router does not connect directly to the Internet itself, but rather, a larger computing platform that is connected to the Internet.

3.2 TEST BED DESIGN

Current implementations of MT6D run directly on end devices such as laptops and cell phones to enable secure point-to-point IP communications. The process of rotating the EUI-64 address of a wireless sensor can execute at three different locations of the wireless sensor network seen in Figure 1: 1) on the 6LoWPAN mote, 2) the 6LoWPAN border router, or 3) the IPv6 Gateway platform.

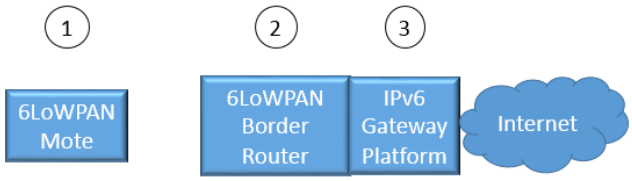

Figure 1 6LoWPAN Test Bed

The 6LoWPAN low-power wireless sensors for this design are the Tmote Sky motes. These represent one of the lowest computing wireless sensor devices and serve as an excellent test bed in conducting dynamic assignment of IPv6 addresses. These motes are equipped with an 8 MHz TI MSP430 microcontroller, 10kB of RAM, 48kB of ROM, 1MB of external flash memory, and a TI CC2420 IEEE 802.15.4 compliant radio. We used ContikiOS 2.7 on these platforms in order to establish a test bed 6LoWPAN network that used one Tmote Sky as an RPL Border Router with the Contiki example program RPL-Border-Router that establishes a tunnel interface, tun0, using the program, tunslip6 on a Rasbperry Pi. The Raspberry Pi we used is a model B with 512MB of RAM running the latest distribution of Debian Wheezy. The Raspberry Pi's eth0 interface was connected to the Virginia Tech's network that provides both IPv4 and native IPv6 connectivity. Virginia Tech does not, however, provide routable IPv6 subnets. We utilized Hurricane Electric's tunnelbroker.net service that assigns /48 subnets. We then created an interface labeled *he-ipv6* that terminates a 6in4 tunnel in the Raspberry Pi. A 6in4 tunnel, in contrast to a 6to4 tunnel, provides a /64 prefix outside the 2002::0/16 network, establishes a dedicated fixed endpoint for the tunnel, and maintains a much more reliable and easier to troubleshoot link. From here we assign a /64 subnet within the /48 to the tun0 interface created when we execute the RPL Border Router program. We specify the IPv6 prefix from the /64 subnet during execution. This allows the Border Router to broadcast the prefix to its 802.15.4 wireless network and allow motes to establish their Global-Link addresses.

We loaded two other Tmote Sky's with the Contiki example program Sky-Websense. This program allowed us to establish TCP communications over IPv6 the Tmote Sky and any other platform capable of TCP communications and HTML support. Upon boot-up, these Tmote Sky's attach a portion of their MAC address to the IPv6 prefix to form their Global-Link address. This method has security concerns because an attacker could find out the MAC address of a device and try to correlate that with the Global-Link address. This provides yet another motivation to

change IPv6 addresses to protect against IP address to physical device correlation.

4. ANALYSIS

Implementing MT6D on the 6LoWPAN mote itself will improve true end-to-end security. The mote must push its new address to the border router causing additional traffic on the channel. Additionally, there is extra overhead involved in the MT6D tunnel resulting in more fragments traversing the 802.15.4 network than under normal 6LoWPAN operation. Although we could reduce the amount of traffic on the already resource constrained 802.15.4 networking environment by performing the MT6D process on the IPv6 Gateway Platform such as a Raspberry Pi, this still leaves static IPv6 addresses on the motes. Internal attackers can take advantage of this lack of end-to-end security.

6LoWPAN was created in order to compress IPv6 packets to fit within the constraints of the 802.15.4 frames. In doing so, IPv6 source and destination addresses where shortened with any zeros omitted and the packets themselves fragmented. MT6D functionality rests upon the ability to tunnel IPv6 packets and for the host running the MT6D software to process the re-binding of IP addresses and maintain an IPv6 address table. The 6LoWPAN process of fragmenting the standard IPv6 packet size of 1280 Bytes in order to communicate over the 802.15.4 link-layer max frame size of 127 Bytes adds additional complexity in performing successful communications with the implementation of MT6D. We must then look at how long it takes to conduct a HTTP GET request from a user across the network to the wireless sensor that is the Contiki Sky-Websense webserver. Sky-Websense provides the display of the Tmote Sky's current light and temperature sensor reading in the form of a HTML page. This page is 181 Bytes. Ten trials were conducted as seen in Table 1 with an average transfer time of 5.06 seconds and 28 packets

Table 1. HTTP Data Transfer between Laptop and Mote

Trial	Time (sec)	# of Packets
1	4.30	30
2	4.20	27
3	5.97	30
4	5.37	26
5	4.47	26
6	4.25	26
7	4.45	27
8	5.11	28
9	5.24	27
10	7.20	28
Average	**5.06**	**28**

These 28 packets include the start of the TCP session with a SYN from the laptop request the HTML page and end with a FIN packet from the mote. The mote maintained a window size of 60 Bytes and an average maximum segment size of 48 Bytes. 6LoWPAN test bed latency tests show there was an average 47 millisecond round trip time for ICMP packets to move between the laptop host and the Border Router tun0 interface. Round trip time for ICMP packets to move from the laptop host to the Tmote Sky averaged 241 milliseconds. This means that 80.5% of the network latency is found in the 802.15.4 wireless network. This is the portion of the network that the Tmote Sky uses in order to communicate its new IP address with the Border Router.

This information is needed to formulate the optimal IPv6 address rotation frequency. Rotating the address too quickly on the order of seconds will result in the Tmote Sky spending more time pushing the new address to the Border Router than sending data and ultimately resulting in packet loss. Rotating the address too slowly on the order of days could result in an attacker being able to successfully identify the current IP address being used and more effectively identify which hosts are communicating.

5. FUTURE WORK

In our future work we will implement MT6D directly onto a Tmote Sky and conduct analysis of RAM and ROM overhead, end-to-end packet loss, IPv6 address rotation frequency, and power-draw using an oscilloscope and voltage amplification circuit. We will then proceed to conduct the same tests on the latest home automation system, WigWag, which operates on a Freescale MC1322x MCU.

6. CONCLUSION

Moving target defense within the Internet of Things is applicable and provides an additional layer of security. Securing the communications between home automation, industrial control, medical monitoring, or smart grid devices and the cloud or other hosts is critical.

We have presented other related work in the field of 6LoWPAN security including defense against fragmentation attacks and the importance of encrypting traffic using IPsec. Frequently rotating the IPv6 address of a 6LoWPAN device limits the opportunity for an attacker to successfully identify the IP address in time to launch a malicious fragment at the target node thus increasing availability, while MT6D tunnels traffic through encryption adding confidentiality and integrity.

7. REFERENCES

[1] 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.

[2] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[3] Hui, J., Ed., and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011.

[4] 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.

[5] 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.

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

[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] 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.

[9] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

[10] Stephen Groat, Matthew Dunlop, William Urbanksi, Randy Marchany, and Joseph Tront. 2012. Using an IPv6 moving target defense to protect the Smart Grid. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT '12). IEEE Computer Society, Washington, DC, USA, 1-7. DOI=http://dx.doi.org/10.1109/ISGT.2012.6175633.

[11] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. 2013. Computer security and the modern home. Commun. ACM 56, 1 (January 2013), 94-103. DOI= http://doi.acm.org/10.1145/2398356.2398377.