This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2018.2797916, IEEE Wireless Communications Letters

Changing the Game: A Micro Moving Target IPv6 Defense for the Internet of Things

Kimberly Zeitz[*†], Michael Cantrell[*†], Randy Marchany[†], and Joseph Tront[*]

Abstract—**This research explores the uses of a Micro Moving Target IPv6 Defense (μMT6D). In this initial experiment we assess the power consumption overhead and detail the overall security benefits gained from use of this technique. Moving Target Defenses were seen as game changers in the security field and now we must change the game once more and look towards their application for IoT devices. With a need to provide privacy and a defense against targeted attacks on resource constrained devices that are a part of vital communication and control systems, μMT6D is a viable solution that we continue to develop and assess for future use.**

I. Introduction

In 2010, the use of Moving Target Defenses (MTDs) was characterized as a "game-changing" theme for cyber security [1] and Section III explains a small sample of the research in this area. Today, with a rapidly changing set of technologies and devices and even greater risk to security in the areas of privacy, information security, and authentication, we need to change the game once more and develop and assess security methodologies and techniques that are capable of securing the low-power and low-resource devices which are becoming common place in public and military networks and systems. The intention for MTDs is to limit the information available to attackers that can be gained from reconnaissance, by constantly changing the location of assets rendering any information gathered useless by it becoming inaccurate and no longer valid on discovery [2]. The moving property is the network information that is being altered to both provide access control through the clients that are able to connect with the system and "limit the window of utility of information that any untrustworthy clients may have gleaned about the network[2]." This research focuses on a Micro Moving Target IPv6 Defense (μMT6D), a security mechanism suitable for low-power and low-resource devices commonly utilized for IoT applications and systems and for which the design was presented in [3]. Traditional MTDs have been utilized in many varieties for large scale systems. μMT6D is designed to work on low power and low resource devices such as those utilized for IoT applications. It is a lightweight security mechanism and the "micro" meaning small is used in the name to denote this characteristic of the technique. The moving property is the rotating IPv6 addresses. Each device has a rotating address based on the use of a lightweight hashing algorithm for the address computation. Thus, the WSN motes are moving targets. The security benefits of μMT6D include protection from targeted attacks. This technique is successful preventing attacks including battery exhaustion attacks and denial of service attacks attempting to stop the functionality and disrupt service of a device, host tracking, as well as, eavesdropping passive attacks attempting to gather information from a device, to name a few. Without the use of μMT6D, attackers will have an unlimited window of time to gather information about a device and ultimately conduct an attack as the address will remain static. The experimental setup utilizes a representative operating system for small embedded devices, Contiki 3.0, and the networking and protocols suited for use with developing IoT devices and Wireless Sensor Network (WSN) applications including a WSN, 6LoWPAN to transmit packets over IEEE 802.15.4, and the Routing Protocol for Low-Power Lossy Networks, LLNs, (RPL). We present our experimental setup and initial simulated power consumption results when comparing an insecure IoT application and the same application with use of μMT6D.

II. Motivation

IoT devices and applications have privacy and information security requirements, but conventional security techniques may not be suitable for use with low-power and low resource devices. Existing mechanisms need to be assessed and adapted, or new variants and techniques developed. The typical structure and layout of networks and devices is evolving. There are IoT applications in areas ranging from health care and smart homes to the energy grid and they include sensors gathering information and/or actuators performing physical tasks. New IoT applications and protocols present new vulnerabilities. Security mechanisms suitable for the constraints of IoT devices are needed. We are now seeing an influx of research aimed at addressing current issues with new protocols, standards, and security techniques that are utilized throughout IoT devices and applications [4]. The use of IPv6 has been shown to present new vulnerabilities to systems and this includes the embedded systems commonly utilized for IoT and WSNs. Even with the vast address space made available through IPv6, vulnerabilities and weaknesses in the formation of the addresses can provide an avenue for attackers to gain information and target devices for attack. Stateless Address

[*]Bradley Department of Electrical and Computer Engineering
[†]Virginia Tech Information Technology Security Lab
Email:{kazeitz,mcantrell,marchany,jgtront}@vt.edu

This work was supported by a grant from the Naval Surface Warfare Center Dahlgren Division's In-house Laboratory Independent Research Program.

AutoConfiguration (SLAAC) may allow attackers to target and track devices. With SLAAC, the host portion of the device IPv6 address is composed from the interface identifier or IID which is often comprised of the MAC address allowing for such identification and following of devices by attackers [5], [6]. The technique of this research is targeted to address these issues. μMT6D, is a moving target defense designed for use with resource constrained devices and aims to prevent targeted attacks on IoT devices through an address rotation, drastically limiting the time window for reconnaissance.

III. Related Work

As mentioned in the introduction, MTDs were considered to be a "game-changing" theme in 2010 [1]. Different variants of MTDs were researched to discover their impact and assess their attack prevention capabilities [7], [2]. The effectiveness and evaluation of MTD systems is an ongoing topic [8], [9]. MTDs can be categorized as passive and active defense systems, some implementing the use of attack indicators to aid decisions and system responses [10] and other MTDs vary in the techniques used for obfuscation [11], [12]. A Moving Target IPv6 Defense (MT6D) was introduced as a viable security mechanism for preventing targeted attacks, host tracking, and eavesdropping [13]. It employs address rotation to obscure the communication of the devices [14]. MT6D was furthered to include a network layer client-server implementation utilizing a Distributed Hash Table (DHT) Blind Rendezvous for session establishment [15], [16], [17]. Most MTDs have been developed for full-scale systems and devices. However, there is a need for IoT security. Looking towards small embedded systems, the dynamic address change on low-powered devices was explored [18], [19] and then a design developed to make the entire MT6D viable for IoT devices as μMT6D [3]. The underlying algorithm utilized within μMT6D is based on the algorithm first utilized in MT6D. Anonymity is achieved through the rotating addresses and privacy due to an attacker not being able to track the rotating addresses [13]. Once a lightweight encryption is added to this implementation to encrypt packets before they are tunneled, μMT6D will also prevent traffic correlation and observation [13]. This paper shows the implementation and the results of an initial power analysis of μMT6D compared to a control application on a medium sized IoT device.

IV. Implementation & Setup

A. Address Change Algorithm

As mentioned in Section III, and following the same principles of MT6D, μMT6D aims to obscure the communication of resource constrained devices through the use of address rotation to prevent targeted attacks. It limits the amount of time an attacker has to conduct reconnaissance and therefore limits the viability of an attack. The underlying address rotation utilized in both MT6D and μMT6D was first introduced in [14] and utilized in [15]. The initial Interface Identifier, or IID, of the source host, a shared session key, and a timestamp are concatenated together and then hashed. The first 64 bits of this result are then concatenated with the 64-bit network address of the host yielding the 128-bit address. This is done also for the destination host so that both clients or a client and a server have a source and destination address calculated. This can be seen with the equation:

$$IID'_{x(t_i)} = H[IID_x||K_S||t_i]_{0\to 63}$$

The IID is the μMT6D IID where x represents the host and t_i is the time at instance i. IID_x is the statically defined IID from the host x. K_S is the shared session key, and H is a cryptographically strong hashing algorithm which returns a result over 64 bits. The hashing for MT6D utilized SHA256 hashing algorithm, and the initial implementation of μMT6D utilizes SHA256 as well. In progress work includes other lightweight hashing algorithms. A window of the previous and next addresses is also kept in case there are any inaccuracies in the network time used for the timestamp. The addition of changing source and destination ports can also be utilized.

B. Implementation

This experiment consisted of an implementation of an application with no security mechanisms as our reference base, and the same application with the added security of μMT6D added to each WSN device and enabling them to change their own address. The setup consists of the architecture design given in [3], with the addition of the connection to the full scale MT6D server left to upcoming future work. This implementation includes a gateway device as the router operating over 802.15.4. The WSN mote is connected via the gateway device and a Serial Line Internet Protocol, SLIP, bridge provided from the Contiki Tunslip utility to an Ubuntu Virtual Machine on an external IPv6 network with an IPv6 router connected via the Hurricane Electric IPv6 Tunnel Broker. Future testing will include results when connected to the native operational IPv6 network of Virginia Tech. The selected lightweight operating system was Contiki 3.0 which is an open source operating system for the IoT. It provides the IPv6 network support including methods and evaluation techniques utilized in this research for our implementation and initial power testing [20]. The Contiki virtual machine also provided the means for simulation with Cooja, the Contiki network simulation tool. The WSN motes for the simulations and the physical testbed are composed of WisMotes which are considered medium low power wireless motes complete with light and temperature sensors and are IEEE 802.15.4 compliant. The current gateway in this implementation is also a WisMote. The IPv6 router was configured on a Raspberry Pi 3, Model B. The implementation will in the future be loaded on both simulated and physical hardware, but these initial test were completed through the Cooja Simulator. In this implementation the WSN motes run a process in which they periodically send a udp packet. The gateway is an RPL, Routing Protocol for LLNs, Border Router. The RPL provided through the Contiki implementation is utilized for this research for routing the packets within the WSN.

C. Experiment

This simulation was the first power analysis for this research and involved one WSN mote sending a packet every minute

TABLE I
SAMPLE POWER DATA CONTROL

CPU	LPM	TX	RX	Total
0.022811746	0.162809311	0.0259469	59.89313	60.1047
0.019732352	0.162902548	0.01028	59.98838	60.1813
0.019155155	0.162920024	0.0079588	59.99101	60.18104
0.01941208	0.162912245	0.0081228	59.99082	60.18127
0.019311014	0.162915305	0.0076338	59.99137	60.18123
0.01860041	0.162936821	0.0053795	59.99392	60.18084
0.019358325	0.162913873	0.0076525	59.99135	60.18128
0.019361828	0.162913767	0.0068486	59.99226	60.18139
0.018870003	0.162928658	0.0070592	59.99202	60.18088
0.021601892	0.162845943	0.0139545	59.98423	60.18263

TABLE II
SAMPLE POWER DATA μMT6D

CPU	LPM	TX	RX	Total
0.058267544	0.161735788	0.1334499	59.84921	60.20266
0.047051261	0.162075392	0.0843805	59.90465	60.19816
0.046639202	0.162087869	0.0834725	59.90568	60.19788
0.046620038	0.162088449	0.082983	59.90623	60.19793
0.04733535	0.162066791	0.0865022	59.90226	60.19816
0.045130284	0.162133555	0.0768674	59.9143	60.19843
0.053393258	0.161883371	0.1065978	59.87955	60.20142
0.045960831	0.162108408	0.0797556	59.90811	60.19594
0.045772896	0.162114098	0.0794926	59.91018	60.19756
0.046634855	0.162088	0.0808337	59.90866	60.19822

and one WSN mote sending a packet every minute while it was also rotating its IPv6 address every five minutes with the μMT6D technique. Power measurements were taken for comparison of each. The Contiki ENERGEST and Collect View tools were utilized to collect the measurements every minute. Both the control application and μMT6D application sent a UDP packet every minute. The address rotation for μMT6D was set for every five minutes. Data was collected over a 24 hour period simulation for both. The data collected included measures of power consumption of radio transmission time (TX), radio receiving/listening time (RX), full power CPU time (CPU), and reduced power CPU time (LPM). These were then utilized to calculate the total energy consumption in milliwatts. A small sample of data collected for each of the respective implementations for the motes can be seen in Tables I and II. The averages included in the analysis were from the entire simulations spanning 24 hours and totaling over 4000 values of data for each type.

V. RESULTS & ANALYSIS

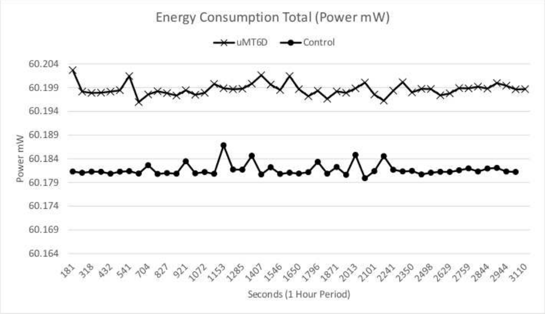

Fig. 1. Total Power Consumption One Hour Sample

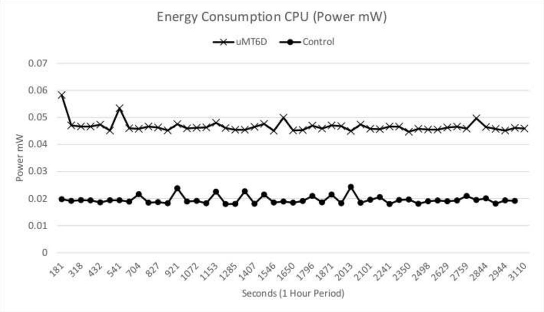

Fig. 2. CPU Power Consumption One Hour Sample

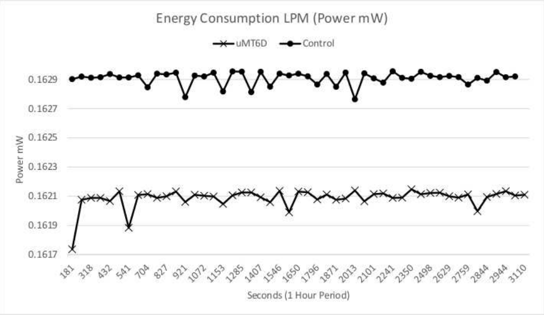

Fig. 3. LPM Power Consumption One Hour Sample

The Contiki Energest results of a one hour sample from the experiment can be seen in Figures 1, 2, 3, 4, and 5. The total averages can be seen in Table III. This initial experiment shows that there is some, but not an unmanageable amount of overhead when μMT6D is added to an IoT application. The increases in power consumption from our simulated experiment are seen in the total, CPU, and TX. This is expected because the WSN node is doing computation for the address rotations. The graphs show the natural variances in the power consumption. Taken as a whole, there were no extreme peaks or increases. The slight peaks appear during times when the device would be transmitting a packet. The μMT6D mote has the additional overhead of when it would compute a new address which keeps the average power consumption consistently higher than the control. For the added security benefits provided by μMT6D, this overhead, although a challenge for some IoT applications, can certainly be worth accepting for use with critical applications and communications in which security is required to prevent target attacks.

VI. FUTURE WORK

This initial implementation is the first step in a progression of planned optimizations and additions. On-going and

TABLE III
AVERAGE POWER CONSUMPTION MW

Power in mW	Control	uMT6D
Total	60.182	60.199
CPU	0.019	0.046
LPM	0.163	0.162
RX	59.992	59.909
TX	0.008	0.018

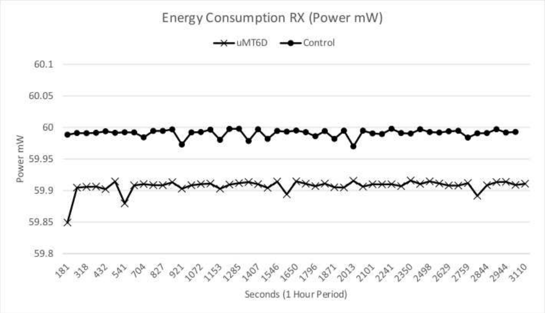

Fig. 4. RX Power Consumption One Hour Sample

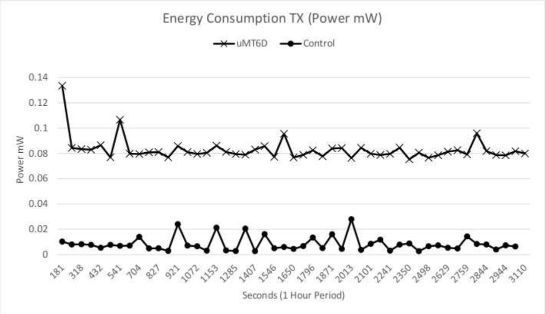

Fig. 5. TX Power Consumption One Hour Sample

future work includes the addition of a lightweight encryption scheme for packet encryption. To decrease power consumption overhead, the time interval for each address change can be altered to be more or less frequent. This trade-off will be explored further since affects the window of time that a device address remains static. Also, a hash library of lightweight hash algorithms has been incorporated for use with μMT6D and an assessment of the use of these different algorithms. This hash library allows for μMT6D to be updated based on new lightweight hashing algorithms as they are released. Lightweight hash functions such as PHOTON, Quark, and SPONGENT are designed to have smaller internal state sizes and be less intense on power consumption [21], this is expected to decrease power consumption further. Other additions will include the connection with a server running the full scale MT6D and a border-based implementation. Finally, large scale simulation will be used to explore the scalability of μMT6D.

VII. Conclusion

We have presented initial power consumption results of the use of μMT6D. This security mechanism was based on the established algorithms and fundamentals of the full scale MT6D, but has been designed and implemented to suit the power and resource constraints of IoT devices and applications that are becoming prevalent in our society. Due to the need for privacy and resilience to targeted attacks, μMT6D is a viable security mechanism for future use.

References

[1] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, *Moving target defense: creating asymmetric uncertainty for cyber threats*. Springer Science & Business Media, 2011, vol. 54.

[2] M. Green, D. C. MacFarland, D. R. Smestad, and C. A. Shue, "Characterizing network-based moving target defenses," in *Proceedings of the Second ACM Workshop on Moving Target Defense*. ACM, 2015, pp. 31–35.

[3] K. Zeitz, M. Cantrell, R. Marchany, and J. Tront, "Designing a micro-moving target ipv6 defense for the internet of things," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, ser. IoTDI '17. New York, NY, USA: ACM, 2017, pp. 179–184. [Online]. Available: http://doi.acm.org/10.1145/3054977.3054997

[4] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *Communications Surveys & Tutorials, IEEE*, vol. 17, no. 3, pp. 1294–1312, 2015.

[5] M. Dunlop, S. Groat, R. Marchany, and J. Tront, "The good, the bad, the ipv6," in *Communication Networks and Services Research Conference (CNSR), 2011 Ninth Annual*. IEEE, 2011, pp. 77–84.

[6] ——, "Ipv6: now you see me, now you donâĂŹtâĂŹ," in *International Conference on Networks (ICN)*, 2011, pp. 18–23.

[7] H. Okhravi, M. Rabe, T. Mayberry, W. Leonard, T. Hobson, D. Bigelow, and W. Streilein, "Survey of cyber moving target techniques," DTIC Document, Tech. Rep., 2013.

[8] K. Zaffarano, J. Taylor, and S. Hamilton, "A quantitative framework for moving target defense effectiveness evaluation," in *Proceedings of the Second ACM Workshop on Moving Target Defense*. ACM, 2015, pp. 3–10.

[9] R. Zhuang, S. A. DeLoach, and X. Ou, "A model for analyzing the effect of moving target defenses on enterprise networks," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*. ACM, 2014, pp. 73–76.

[10] R. Zhuang, S. Zhang, A. Bardas, S. A. DeLoach, X. Ou, and A. Singhal, "Investigating the application of moving target defenses to network security," in *Resilient Control Systems (ISRCS), 2013 6th International Symposium on*. IEEE, 2013, pp. 162–169.

[11] D. Kewley, R. Fink, J. Lowry, and M. Dean, "Dynamic approaches to thwart adversary intelligence gathering," in *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings*, vol. 1. IEEE, 2001, pp. 176–185.

[12] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: transparent moving target defense using software defined networking," in *Proceedings of the first workshop on Hot topics in software defined networks*. ACM, 2012, pp. 127–132.

[13] M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront, "The blind man's bluff approach to security using ipv6," *Security & Privacy, IEEE*, vol. 10, no. 4, pp. 35–43, 2012.

[14] ——, "Mt6d: A moving target ipv6 defense," in *Military Communications Conference, 2011-Milcom 2011*. IEEE, 2011, pp. 1321–1326.

[15] C. Morrell, J. S. Ransbottom, R. Marchany, and J. G. Tront, "Scaling ipv6 address bindings in support of a moving target defense," in *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for*. IEEE, 2014, pp. 440–445.

[16] C. Morrell, R. Moore, R. Marchany, and J. G. Tront, "Dht blind rendezvous for session establishment in network layer moving target defenses," in *Proceedings of the Second ACM Workshop on Moving Target Defense*. ACM, 2015, pp. 77–84.

[17] R. Moore, C. Morrell, R. Marchany, and J. G. Tront, "Utilizing the bittorrent dht for blind rendezvous and information exchange," in *Military Communications Conference, MILCOM 2015-2015 IEEE*. IEEE, 2015, pp. 1560–1565.

[18] T. Preiss, M. Sherburne, R. Marchany, and J. Tront, "Implementing dynamic address changes in contikios," in *Information Society (i-Society), 2014 International Conference on*. IEEE, 2014, pp. 222–227.

[19] M. Sherburne, R. Marchany, and J. Tront, "Implementing moving target ipv6 defense to secure 6lowpan in the internet of things and smart grid," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*. ACM, 2014, pp. 37–40.

[20] A. Dunkels, J. Eriksson, N. Finne, F. Österlind, N. Tsiftes, J. Abeillé, and M. Durvy, "Low-power ipv6 for the internet of things," in *Networked Sensing Systems (INSS), 2012 Ninth International Conference on*. IEEE, 2012, pp. 1–6.

[21] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Report on lightweight cryptography," *NISTIR*, vol. 8114, 2017.