Designing a Micro-Moving Target IPv6 Defense for the Internet of Things

Kimberly Zeitz
Bradley Department of Electrical and Computer Engineering
Virginia Tech Information Technology Security Lab
Virginia Tech
Blacksburg, Virginia 24060
kazeitz@vt.edu

Michael Cantrell
Bradley Department of Electrical and Computer Engineering
Virginia Tech Information Technology Security Lab
Virginia Tech
Blacksburg, Virginia 24060
mcantrell@vt.edu

Randy Marchany
Virginia Tech Information Technology Security Lab
Virginia Tech
Blacksburg, Virginia 24060
marchany@vt.edu

Joseph Tront
Bradley Department of Electrical and Computer Engineering
Virginia Tech Information Technology Security Lab
Virginia Tech
Blacksburg, Virginia 24060
jgtront@vt.edu

ABSTRACT

As the use of low-power and low-resource embedded devices continues to increase dramatically with the introduction of new Internet of Things (IoT) devices, security techniques are necessary which are compatible with these devices. This research advances the knowledge in the area of cyber security for the IoT through the exploration of a moving target defense to apply for limiting the time attackers may conduct reconnaissance on embedded systems while considering the challenges presented from IoT devices such as resource and performance constraints. We introduce the design and optimizations for a Micro-Moving Target IPv6 Defense including a description of the modes of operation, needed protocols, and use of lightweight hash algorithms. We also detail the testing and validation possibilities including a Cooja simulation configuration, and describe the direction to further enhance and validate the security technique through large scale simulations and hardware testing followed by providing information on other future considerations.

CCS CONCEPTS

•Security and privacy →Security protocols; •Computer systems organization →Embedded and cyber-physical systems; •Networks →*Network protocols;*

KEYWORDS

IoT, Embedded Systems, Moving Target Defense

IoTDI 2017, Pittsburgh, PA USA

DOI: http://dx.doi.org/10.1145/3054977.3054997

ACM Reference format:
Kimberly Zeitz, Michael Cantrell, Randy Marchany, and Joseph Tront. 2017. Designing a Micro-Moving Target IPv6 Defense for the Internet of Things. In *Proceedings of The 2nd ACM/IEEE International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA USA, April 2017 (IoTDI 2017),* 6 pages.
DOI: http://dx.doi.org/10.1145/3054977.3054997

1 INTRODUCTION

There is a paradigm shift occurring in the way society interacts with technology. The Internet of Things (IoT) can be described as groups of wireless devices, often sensors and actuators, communicating and connected via the Internet. These are low power, low resource, and often unattended devices that exchange data and allow for a service. These services can vary from home automation such as motion lights and unlocking doors to manufacturing uses such as equipment controls. This is an integration of the physical world with the information world [20].

As the possibilities and services provided by the IoT grow, so does the risk of cyber-attacks which can now have more of a physical threat thanks to the connection of everyday and new physical devices to the Internet. Protecting the information and the sensors and remote-controlled objects themselves is a challenge that needs to be addressed. This paper outlines a Micro-Moving Target IPv6 Defense, μMT6D. The goal of this research is to experiment with, analyze, and assess the viability of the use of μMT6D to protect IoT low-powered embedded devices by limiting the time an attacker may conduct reconnaissance and therefore preventing them from being able to target a device. The design presented in this paper is only the first step towards realizing this goal.

This paper describes the design, optimizations, and testing and validation directions of a micro-moving target defense aimed to enhance the security of IoT devices by limiting the amount of time an attacker has to collect information and target a device for an attack making it highly unlikely for such an attack to succeed. This

defense, μMT6D, is currently being implemented and the testbeds set up. The experimentation and results will come in future publications. This paper shows the groundwork in the design, theory, background, and the direction of this research. The remaining sections of this paper describe the motivation behind this research in Section 2, further background information in Section 3, the design and optimizations in Section 5, a description of the testing and validation possibilities and a discussion on the base simulation configuration in Section 6, the future direction of this research in Section 7, and finally concluding remarks in Section 8.

2 MOTIVATION

There are several reasons why security is a major area of concern for the IoT. Since most of the communications are wireless, this can make them targets for eavesdropping. The devices may also be unattended for prolonged periods of time, leaving them vulnerable to physical attacks. Further, IoT devices limited in energy and computing power do not allow for the implementation and use of complex security schemes possible on other devices [1]. Using current encryption techniques often require more processing power and memory than is found on most embedded devices [22]. Methodologies for secure communications and data storage need to be adapted because they require more storage and power [3], and the distributed nature and large number of devices introduces authentication challenges [20]. Often, to perform authentication, IoT devices rely on a gateway such as a mobile device or wireless access point [33].

The data that is collected by these devices is an ever growing collection of what may be sensitive information, including private health, movement, environmental, or other types of metrics. Finally, the addition of these devices which traditionally are not networked, or are being utilized for new applications, may lead to the discovery of new vulnerabilities and security risks not previously considered. The large number of devices alone increases the potential of an attacker being able to find a weakness or vulnerability [1]. It is expected that 50 billion devices will be interconnected by 2020, and this number is further expected to reach a trillion [18]. In general, more devices mean more attack points and safeguarding these devices is therefore vital to the security of the data and applications for which the devices exist.

We need to look at advancing the state of the art of security techniques to include methodologies and defenses suited for these low-power and low-resource IoT devices. There are many security questions which have not been answered in relation to the use of embedded devices for these new applications and research findings and metrics may not yet even exist for comparison or reference. Just a few of the open questions which exist for IoT devices include:

How can IoT devices withstand attacks aiming to ...

- halt functionality?
- gain information?
- send false information?

These are very general and even more questions remain unexplored in this area of devices and although the use of small embedded systems is not a new area, the rate at which they are being utilized and their application for use in new areas such as smart homes and everyday physical objects has led to these devices being utilized at an even higher rate and present in many more places they were not previously.

Each of these open questions mentioned deals with an attack with a different goal. Battery exhaustion attacks and denial of service attacks attempt to stop the functionality and disrupt the service of a device. Eavesdropping is just one passive attack with the purpose of gathering information. Finally, man-in-the middle attacks, as well as physically tampering with sensors, exist for the purpose of sending false information to devices and systems. In the context of the IoT, imagine a smart thermostat being "tricked" into reading that an area is much hotter through the use of a heat lamp under the sensor. The thermostat may then run the air conditioning and rack up a high bill for the building owner. This may seem costly although relatively harmless, but many embedded devices are utilized for services which are considered to be much more high-risk. Health devices responsible for human lives, machinery equipment where malfunctions could lead to explosions or chemical leakages, and finally weapon or procedure sensors and actuators responsible for system notifications or deployments are just a few examples of devices for which security is a concern to prevent possibly devastating consequences from targeted attacks. These security vulnerabilities do not just apply to household IoT products. Research has been conducted to show how this shift toward IoT devices relates to defense strategies and systems. A "Military Internet of Things" (MIOT) [31] has been explained as an outcome of information based modern warfare. The battlefield/zone will become an information network filled with systems and devices all in communication to aid information sharing, decision making, and weapons control. The MIOT is a system allowing for the sharing of information with regard to military people, equipment, and operational systems [31]. The IoT is quickly becoming interwoven in many different aspects and operations of our society. These open questions and concerns all conclude in the need for more security strategies and defenses and an analysis of their use with IoT devices within different domains and applications.

3 BACKGROUND

3.1 IoT Related Work

As mentioned in Section 2, security techniques must be adapted or developed to secure the communications and sensitive data of new IoT devices and applications [3, 18, 22]. Research and experiments for the IoT have varied from Secure Multi-Hop Routing Protocols [8] to testing large scale simulator applications [7]. Applications vary widely from healthcare [32], green architecture, environmental monitoring, to smart transportation [21] and security remains a major topic of concern. Since low-powered and low-resource devices cannot make use of some traditional authentication methods or intrusion detection systems, new models and techniques are needed [20, 33]. Many authentication methods, encryption forms, hardware approaches, and protocols have been explored for use [5, 6, 15, 30]. Much research has focused on the Transport Security Layer [14, 24, 27]. However, implementing encryption and authentication methodologies do not obscure the addresses of the devices, leaving an opening for adversaries to find and target these devices.

In terms of device addressing, the introduction of IPv6 has both positive and negative ramifications. Unfortunately, the StateLess Address AutoConfiguration, SLAAC, allowing devices to create their host portion of the IPv6 address, (the interface identifier (IID) often comprised of the MAC address), allows for malicious users to identify device location and monitor and/or track the communications of those devices [11]. Tracking and monitoring an address allows an adversary plenty of time to gather information in this reconnaissance stage, and ultimately plan out an attack strategy. This is the scenario moving target defenses aim to prevent.

3.2 Moving Target Defense Related Work

Attackers utilize reconnaissance to identify a target machine or device for conducting an attack. A defense to this involves limiting the time and possibility of selecting a target to directly impact the ability of an adversary to carry out an attack. This is the motivation and underlying concept behind a moving target defense security strategy.

Researchers at the Virginia Polytechnic Institute and State University have developed MT6D, a Moving Target IPv6 Defense, which has been shown successful in thwarting targeted attacks, host tracking, and eavesdropping by obscuring the network and transport layer addresses and avoiding static defenses which allow adversaries unlimited time to conduct attacks [13]. MT6D provides privacy and prevents targeted network attacks by obscuring the communication of two devices through address rotation [12]. This can be applied to the IoT. Optimizations were first done to this moving target defense by translating the implementation code from Python to C [16]. Next, a method has been developed for the dynamic address change on low-powered devices [23, 26]. This research takes previous research in this area further and presents a design and optimizations for fully implementing μMT6D and describes the base simulation setup and future hardware testing for further experimentation, assessment, and validation. By considering the challenges presented from IoT devices such as resource and performance constraints, this design, optimizations, and validation testing and experimentation will allow for the assessment of the use of μMT6D. As an overall goal and the leading direction for this work, we present the question:

> **Is a moving target defense methodology a viable defense for limiting reconnaissance time and thwarting attacks for IoT devices?**

The next sections describe the concept overview and the design and optimizations for μMT6D, the testing and validation configurations which should be considered for experimentation, the simulation base and hardware testbed needed along with a discussion of metrics and validation. Finally, we then outline a few other future works and directions for this research.

4 THREATS

IoT devices pose many new privacy risks based on the services they provide and their characteristics. Often, they are inaccessible for long periods of time depending on the application and location, for example a remote location where sunlight measurements are taken. They may also only be "online" for small bursts of time to save energy, especially if they have limited battery or solar power. This makes updates, such as for security, difficult. Further, these devices tend to function for applications requiring huge amounts of data collection, ranging from sensitive data for military operations to personal data for fitness trackers. The control and protection of this data should be a top concern and presents challenges for those producing IoT devices and implementing applications [28]. Given these characteristics, it is important to understand the threats IoT devices may face.

For example, IEEE 802.11 and the compressed 802.15.4 standards send header frames in plaintext, thus exposing the MAC addresses. This can be used to track the owner of a device and connect the MAC addresses to individuals. This could lead to companies tracking users' shopping habits or attackers learning personal information about a user. Sniffers could also be used to track a user and gather information such as routine travel locations and allow for the gathering of enough information to perform targeted attacks [2]. They could learn what hotel a user regularly stays at and try and learn password information with an email link and a fake website designed to mimic the hotel webpage and capture a password. Similarly, the collection of MAC addresses could be used to identify active IoT devices which are a part of a system, for instance a smart home. This allows for the discovery of what types of devices are present and their active cycles, such as automatic settings for thermostats in "away mode" when users are not home. Inventory of IoT devices and the flows of data can reveal these types of schedules and allow attackers to infer IoT device functions and system or user behavior [25]. This research aims to address similar threats.

5 DESIGN & OPTIMIZATION

A Micro-Moving Target IPv6 Defense, or μMT6D, was designed to operate within IPv6 over Low-power Wireless Personal Area Networks, or 6LoWPAN. As discussed, [26] and [23] showed the viability of frequently rotating the IPv6 address of a single 6LoWPAN device. In order to implement and assess μMT6D, we have designed the modes of operation and optimizations which will be needed.

5.1 Concept Overview

The overall concept of operations for μMT6D is that by changing the address of the IoT device for which this security mechanism is deployed, this will limit the amount of time an attacker has to conduct reconnaissance and therefore also limit the viability of such an attacker carrying out an attack. As mentioned in Section 3, 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. Figure 1 shows an overview of this concept. At the top, is a depiction of three nodes, or resource constrained IoT devices, communicating and utilizing μMT6D. This represents an example true configuration. Below, is an attacker's view of the configuration in which seemingly many more devices are communicating and also look to appear and disappear on random addresses. The attacker does not have an idea of which nodes are actually communicating and believes there are many more nodes due to the many IPv6 addresses observed. After having

an understanding of the basic concept, it is important to detail the design for this concept. We present the design of two different modes of operation for μMT6D, Host-based and Border-based.

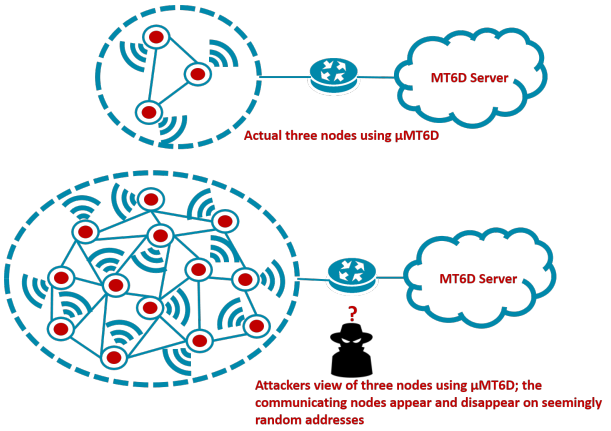

Figure 1: Concept Overview of *u*MT6D

5.1.1 Host-Based. For a host-based design of μMT6D, the implementation of the security technique would be present and carried out by the host devices themselves. These are our resource constrained IoT devices. In this mode of operation the implementation would be optimized for use on low-power and low-memory devices so as to not interfere with the task for which the devices are intended.

5.1.2 Border-Based. As mentioned in the introduction, the vast majority of IoT devices are low-powered and low-resource. Due to these limitations, these devices often have another device, or hub, which is more capable and less resource constrained with which to communicate [33]. The individual nodes may be engineered to only have the resources needed to perform their given role in the IoT. In this scenario, a border device, such as a router or other gateway device, could be utilized for the address rotation. One security implication of this which would need to be explored and noted is the fact that there would be a single point of failure for this moving target defense.

5.2 Protocol

In order to implement and test the different modes of operation and μMT6D itself, protocols need to be developed. This will include a protocol for multiple nodes in the WSN (Wireless Sensor Network) to communicate on the same network with each other and the border router for the host-based mode of operation. For the border-based mode of operation, a protocol will be developed for the communication of the border router, or other gateway device, to the nodes and the reverse. These protocols should be scalable. As mentioned in Section 2, the number of connected devices is increasing and more and more these devices are being utilized for new applications, many of which may involve communications between a large number of them. Finally, μMT6D needs to be able to allow for communications with stand alone MT6D host machines, as well as, MT6D servers.

5.3 Lightweight Hash Algorithms

One optimization technique for μMT6D is the utilization of lightweight cryptographic hash algorithms. MT6D was first implemented with the use of the Secure Hash Algorithm, SHA-256. This is suited fine for use with the traditional computing devices, but the algorithm is not optimized for use with the resource constrained IoT devices. For this reason, this optimization of μMT6D will allow for the switching and selection of different lightweight hash algorithms.

Different hash algorithms have pros and cons concerning security, memory size, power, and throughput. In 2012, a comparison was done assessing various versions of hash functions such as PHOTON, QUARK, SPONGENT, and ARMADILLO [19]. Different algorithms were also implemented on an ATMEL AVR ATtiny45 8-bit microcontroller, and their performance was evaluated [4]. The area and throughput of the KECCAK, PHOTON, and SPONGENT hash functions have also been evaluated and implemented on Xilinx Spartan 6 FPGAs [17]. These and other works can be utilized to select different hash functions to include for use and evaluation with μMT6D. Many of the algorithms could also be further optimized depending on the target IoT device. Ultimately, comparisons and experimentation would help to find which were best suited for what applications or modes of operation of μMT6D.

6 TESTING & VALIDATION

6.1 Simulation

As mentioned, Micro-Moving Target IPv6 Defense, μMT6D, is a moving target defense designed to be lightweight and operate efficiently on small embedded devices. The open source Contiki operating system was selected for the implementation since it supports fully standard IPv6 along with IPv4 and has an option of utilizing different low-power wireless standards such as 6LoWPAN, RPL (Routing Protocol for Low-Power and Lossy Networks (LLNs)), and CoAP (Constrained Application Protocol) [9]. Our simulations run with the Cooja simulator included in the Contiki development environment which allows for the use of different simulated low-power and resource devices such as WiSmote and TMote Sky nodes. An RPL Border Router is utilized as the network edge device as this is the primary routing protocol for IPv6 LLNs [29].

Consistent with typical network architectures, [10], our configuration includes the RPL border router integrating 6LoWPAN over IEEE 802.15.4 with the IP network. This design configuration of the WSN of motes running μMT6D connected to a host machine running MT6D or an MT6D server can be seen in Figure 2. The RPL Border Router is the root of the directed acyclic graph (DAG) formed by the connected nodes running μMT6D. The border router hosts a webpage allowing for a visual of the IPv6 addresses of the neighboring nodes and routes in the simulation. The simulated RPL network was connected with a bridge to the local machine utilizing the Tunslip6 utility. Tunslip6 creates a virtual network interface (tun0) on the host and uses the Serial Line Internet Protocol (SLIP) to encapsulate and pass the IP traffic. This configuration will allow for future testing and experimentation with μMT6D. Another possible configuration which may be considered for utilization is simulating both the wireless sensor network and the host machine

or server and network it is connecting to. Such a configuration can be seen in Figure 3.

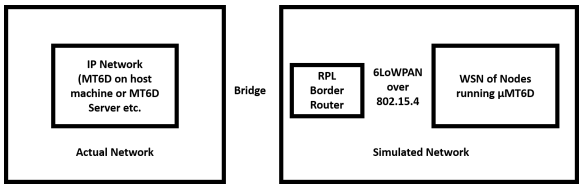

Figure 2: Simulation configuration of μMT6D

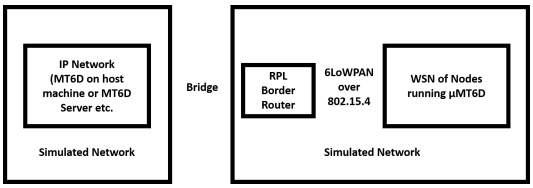

Figure 3: Simulation configuration of μMT6D plus network simulation

6.2 Hardware

Actual hardware experimentation and analysis will be done in addition to simulation and testing. This configuration will be similar to that of the simulation except a WSN composed of at least ten physical motes will be utilized. The utilization of both WiSMote and TMote Sky low-power wireless sensor devices will allow for the implementation and testing of μMT6D for analysis in real network conditions. A Raspberry Pi will be utilized as the border router. There is also the potential to combine simulation and real hardware for testing by the addition of having simulated network conditions being sent to the physical devices. Example configuration layouts can be seen in Figure 4 and Figure 5.

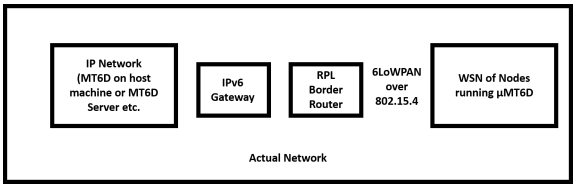

Figure 4: Physical hardware configuration of μMT6D testbed

6.3 Metrics & Validation

Whether through simulation or physical hardware testing, when we conduct experiments to analyze μMT6D, we want to set up the experiments to be able to gain insights into the viability of both modes of operation, host- and border-based, as well as, the viability of μMT6D in general for resource constrained devices. This involves analyzing the security technique from different angles. For simulation, we will consider scaling and seek to find the limitations in the number of nodes that can be a part of a WSN

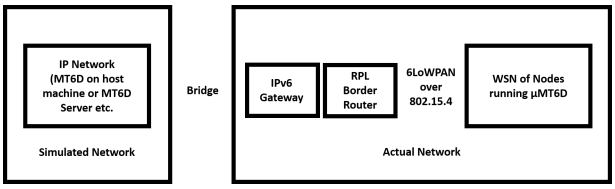

Figure 5: Physical hardware plus network simulation configuration of μMT6D testbed

running μMT6D for both modes of operation. This will demonstrate if our moving target defense is a workable solution for a network containing some n nodes or devices for each and can also lead to looking at further optimizations and/or factors that could alter the performance. Further, performance should be explored on both simulated motes, as well as, physical motes. A security technique is of little use if the device cannot perform its intended functionality within the necessary time frame. A device with a non-time critical application will have different requirements than one which is time critical. For example a temperature sensor sending data to a thermostat in a smart home will have little impact if slightly delayed in comparison to a sensor sending data to an emergency alarm to warn of equipment overheating that could lead to an explosion. Focusing on gathering data on the data delivery speed, throughput, and latency of the devices running μMT6D will be necessary.

In addition to those already discussed, there are more considerations for resource constrained devices. The percentage of overall resources utilized by a device running μMT6D in comparison to those running the same application without μMT6D should be assessed. The additional storage space needed, as well as, the additional power consumption needed by μMT6D should be as low as possible to enable the most resources to be available for the device application while still providing an appropriate level of security.

7 FUTURE WORK

There is much future work needed to carry this research closer to answering the question of "Is a moving target defense methodology a viable defense for limiting reconnaissance time and thwarting attacks for IoT devices?" As touched on in Section 6, scaling is one factor which needs to be further considered. The developed protocols and the operation of μMT6D for both host-based and border-based modes of operation need to be further analyzed with regard to scalability. Another area to explore includes the security implications of utilizing different lightweight hashing algorithms. The ability to switch and select the algorithm needs to be paired with research into any resulting factors and/or security issues which may be linked to this change. In addition, research can be done to test both modes of operation of μMT6D and compare their use in communication with the traditional MT6D running on a host device and also with an MT6D server. Finally, risk analysis and research into the benefits and limitations of this design and the protocols it utilizes is necessary as this work moves forward. This could include assessing any potential attack methodologies which could be utilized against μMT6D.

8 CONCLUSION

We have outlined the design and optimizations for a Micro-Moving Target IPv6 defense, μMT6D. The flexibility to utilize different lightweight hash algorithms will greatly enhance the potential for the use of μMT6D with different applications based on the varying performance and size constraints, but still within the realm of resource constrained embedded systems. Protocols for μMT6D will be developed to allow for the communication between many devices as well as communications with gateway devices and host machines running MT6D or an MT6D server. In addition, implementing the described host-based and also border-based modes of operation will be utilized for comparison and evaluation to provide insight into the use of this security technique with the ultimate goal of finding the strengths and weaknesses of each mode of operation and the suitability of μMT6D for different applications.

Further, the Cooja simulation base and hardware testbed for μMT6D are described and possible different combinations of configurations for experimentation are given. The use of simulations plus hardware will allow for large scale experimentation and also the gathering of a variety of metrics to analyze and validate of the use of μMT6D with low-power and low-resource devices. Ultimately, this design and future work will explore the use of a moving target defense to limit the time an attacker has to conduct reconnaissance and therefore prevent targeted attacks.

ACKNOWLEDGMENTS

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

REFERENCES

[1] Habtamu Abie and Ilangko Balasingham. 2012. Risk-based adaptive security for smart IoT in eHealth. In *Proceedings of the 7th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 269–275.

[2] Ali-Amir Aldan, Omer Cerrahoglu, Erjona Topalli, and Xavier Soriano. 2016. Marauderfis Map: Sniffing MAC addresses in the MIT wireless network. (2016). https://courses.csail.mit.edu/6.857/2016/files/34.pdf

[3] Ibrahim Ethem Bagci, Shahid Raza, Taeyoung Chung, Utz Roedig, and Thiemo Voigt. 2013. Combined secure storage and communication for the internet of things. In *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on*. IEEE, 523–531.

[4] Josep Balasch, Barış Ege, Thomas Eisenbarth, Benoit Gérard, Zheng Gong, Tim Güneysu, Stefan Heyse, Stéphanie Kerckhof, François Koeune, Thomas Plos, and others. 2012. *Compact implementation and performance evaluation of hash functions in attiny devices*. Springer.

[5] Nabil Benamar, Antonio Jara, Latif Ladid, and Driss El Ouadghiri. 2014. Challenges of the internet of things: IPv6 and network management. In *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*. IEEE, 328–333.

[6] Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi. 2012. Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*. IEEE, 1–7.

[7] Giacomo Brambilla, Marco Picone, Simone Cirani, Michele Amoretti, and Francesco Zanichelli. 2014. A simulation platform for large-scale internet of things scenarios in urban environments. In *Proceedings of the First International Conference on IoT in Urban Space*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 50–55.

[8] Paul Loh Ruen Chze and Kan Siew Leong. 2014. A secure multi-hop routing for IoT communication. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. IEEE, 428–432.

[9] OS Contiki. 2012. The Open Source OS for the Internet of Things. (2012).

[10] Laurent Deru, Sébastien Dawans, Mathieu Ocaña, Bruno Quoitin, and Olivier Bonaventure. 2014. Redundant border routers for mission-critical 6lowpan networks. In *Real-world wireless sensor networks*. Springer, 195–203.

[11] Matthew Dunlop, Stephen Groat, Randy Marchany, and Joseph Tront. 2011. The good, the bad, the IPv6. In *Communication Networks and Services Research Conference (CNSR), 2011 Ninth Annual*. IEEE, 77–84.

[12] Matthew Dunlop, Stephen Groat, William Urbanski, Randy Marchany, and Joseph Tront. 2011. Mt6d: A moving target ipv6 defense. In *Military Communications Conference, 2011-Milcom 2011*. IEEE, 1321–1326.

[13] Matthew Dunlop, Stephen Groat, William Urbanski, Randy Marchany, and Joseph Tront. 2012. The Blind Man's Bluff Approach to Security Using IPv6. *Security & Privacy, IEEE* 10, 4 (2012), 35–43.

[14] Oscar Garcia-Morchon, Sye Loong Keoh, Sandeep Kumar, Pedro Moreno-Sanchez, Francisco Vidal-Meca, and Jan Henrik Ziegeldorf. 2013. Securing the IP-based internet of things with HIP and DTLS. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, 119–124.

[15] Jorge Granjal, Edmundo Monteiro, and Jorge Sa Silva. 2013. End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication. In *IFIP Networking Conference, 2013*. IEEE, 1–9.

[16] Owen Russell Hardman. 2016. *Optimizing a network layer moving target defense by translating software from python to c*. Ph.D. Dissertation. Virginia Tech.

[17] Bernhard Jungk, Leandro Rodrigues Lima, and Matthias Hiller. 2014. A systematic study of lightweight hash functions on FPGAs. In *ReConFigurable Computing and FPGAs (ReConFig), 2014 International Conference on*. IEEE, 1–6.

[18] Arun Kanuparthi, Ramesh Karri, and Sateesh Addepalli. 2013. Hardware and embedded security in the context of internet of things. In *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*. ACM, 61–64.

[19] Adarsh Kumar and Alok Aggarwal. 2012. Lightweight cryptographic primitives for mobile ad hoc networks. In *Recent Trends in Computer Networks and Distributed Systems Security*. Springer, 240–251.

[20] Parikshit N Mahalle, Neeli Rashmi Prasad, and Ranga Prasad. 2014. Threshold Cryptography-based Group Authentication (TCGA) scheme for the Internet of Things (IoT). In *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference on*. IEEE, 1–5.

[21] Gurpreet Singh Matharu, Priyanka Upadhyay, and Lalita Chaudhary. 2014. The Internet of Things: Challenges & security issues. In *Emerging Technologies (ICET), 2014 International Conference on*. IEEE, 54–59.

[22] Stefan Poslad, Mohamed Hamdi, and Habtamu Abie. 2013. Adaptive security and privacy management for the internet of things (ASPI 2013). In *Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication*. ACM, 373–378.

[23] Tanner Preiss, Matthew Sherburne, Randy Marchany, and Joseph Tront. 2014. Implementing dynamic address changes in contikios. In *Information Society (i-Society), 2014 International Conference on*. IEEE, 222–227.

[24] Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, and Thiemo Voigt. 2013. Lithe: Lightweight secure CoAP for the internet of things. *Sensors Journal, IEEE* 13, 10 (2013), 3711–3720.

[25] Ignacio Sanchez, Riccardo Satta, Igor Nai Fovino, Gianmarco Baldini, Gary Steri, David Shaw, and Andrea Ciardulli. 2014. Privacy leakages in Smart Home wireless technologies. In *Security Technology (ICCST), 2014 International Carnahan Conference on*. IEEE, 1–6.

[26] Matthew Sherburne, Randy Marchany, and Joseph Tront. 2014. 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, 37–40.

[27] Marco Tiloca. 2014. Efficient Protection of Response Messages in DTLS-Based Secure Multicast Communication. In *Proceedings of the 7th International Conference on Security of Information and Networks*. ACM, 466.

[28] Johanna Ullrich, Artemios G Voyiatzis, and Edgar R Weippl. 2016. The Quest for Privacy in the Consumer IoT. (2016).

[29] Tim Winter. 2012. RPL: IPv6 routing protocol for low-power and lossy networks. (2012).

[30] Teng Xu, James B Wendt, and Miodrag Potkonjak. 2014. Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press, 417–423.

[31] Lan Yushi, Jiang Fei, and Yu Hui. 2012. Study on application modes of military internet of things (miot). In *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on*, Vol. 3. IEEE, 630–634.

[32] Xiao Ming Zhang and Ning Zhang. 2011. An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine. In *Computer and Management (CAMAN), 2011 International Conference on*. IEEE, 1–4.

[33] Zhi-Kai Zhang, Michael Cheng Yi Cho, and Shiuhpyng Shieh. 2015. Emerging security threats and countermeasures in IoT. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 1–6.