2015 IEEE 21st International Conference on Parallel and Distributed Systems

A Framework for Modeling and Assessing Security of the Internet of Things

Mengmeng Ge
Dept. of Computer Science and Software Engineering
University of Canterbury, Christchurch, New Zealand
Email: mge43@uclive.ac.nz

Dong Seong Kim
Dept. of Computer Science and Software Engineering
University of Canterbury, Christchurch, New Zealand
Email: dongseong.kim@canterbury.ac.nz

***Abstract*—Internet of Things (IoT) is enabling innovative applications in various domains. Due to its heterogeneous and wide scale structure, it introduces many new security issues. To address the security problem, we propose a framework for security modeling and assessment of the IoT. The framework helps to construct graphical security models for the IoT. Generally, the framework involves five steps to find attack scenarios, analyze the security of the IoT through well-defined security metrics, and assess the effectiveness of defense strategies. The benefits of the framework are presented via a study of two example IoT networks. Through the analysis results, we show the capabilities of the proposed framework on mitigating impacts of potential attacks and evaluating the security of large-scale networks.**

***Keywords*—Attack Graphs, Hierarchical Attack Representation Model, Internet of Things, Security Analysis**

1. Introduction

In the Internet of Things (IoT), every physical object becomes locatable, addressable and reachable in the virtual world [1], [2], [3]. The IoT is supposed to contain millions or billions of objects which will communicate with each other and with other entities (e.g., human beings). With the inherent complexity and heterogeneous feature, the IoT has faced numerous threats and attacks that will negatively affect its normal functionality. Thus protecting the security of the IoT becomes a complex and difficult task.

The motivation of our work lies within the field of security modeling for the IoT. Vulnerabilities of the IoT reside in different aspects, including devices (hardware, operating systems), communication protocols, service applications, service APIs, design of the IoT architecture, *etc*. By exploiting such vulnerabilities, an attacker can launch various attacks including eavesdropping, Denial of Service (DoS) attacks, node capture and node controlling [1]. With the presence of varied and complex attacks, the ability to discover potential attack scenarios (e.g., an attacker's paths to a target IoT device) and mitigate the impact of malicious attacks becomes a critical issue. Research on the IoT security modeling is also very limited due to the pioneering nature of the IoT.

In the paper, we propose a framework for security modeling and assessment of the IoT. The framework is used to construct a graphical security model to automate the security analysis of an IoT. The driving idea behind the framework is to mitigate the impact of potential attacks in the IoT and increase the IoT security level.

To the best of our knowledge, this work is the first approach to use a graphical security model (in particular, a scalable security model named Hierarchical Attack Representation Model (HARM) [4]) in modeling and assessing security for the IoT. The main contributions of this paper are summarized as follows:

- propose a framework for modeling and assessing security of the IoT;
- develop a graphical security model for the IoT in the framework; and
- show the benefits of the framework using example IoT networks based on a wireless body area network (WBAN) and a wireless sensor network (WSN).

The rest of the paper is organized as follows. Section 2 introduces related work on existing security modeling approaches for the IoT and discusses their constraints. The framework is presented in Section 3. The evaluation using two example IoT networks is presented in Section 4. Finally, Section 5 ends the paper with the conclusion.

2. Related Work

There are a few papers focusing on developing security modeling approaches for the IoT. Most papers only propose a high-level description or a theoretical framework of security modeling without any analytical and/or simulation work. Radomirovic [5] proposes a dense IoT model along with an adversary model based on Dolev-Yao adversary to address security and privacy issues of communication protocols in the IoT. The communication network is under control of the adversary with corruption and fingerprinting abilities. The paper points out the future work towards a formal model limiting the adversary's capabilities. Yang *et al.* [6] present a high-level security framework for the IoT. The framework is based on a 3C model encompassing three elements with linkages with each other, which are communication, control and computation, respectively. It is completed by putting security control between computation and control. Abie *et al.* [7] introduce a risk-based security framework for the

1521-9097/15 $31.00 © 2015 IEEE
DOI 10.1109/ICPADS.2015.102

IoT in the healthcare scenarios. Based on a continuous cycled process, the framework provides security solutions adaptively upon estimations of risk damage and benefits and evaluates solutions through security metrics. A patient monitoring case study is indicated to be used for validating the framework in the future simulation experiment. Stepanova *et al.* [8] propose a theoretical framework for modeling the IoT security based on the graph theory. By defining the IoT as the net of nets of things (NoTs), they design formalized network property indicators to assess the NoT sustainability and describe a sustainability maintaining method for the NoT entities. Future work includes the efficiency evaluation of the method with pre-defined indicators.

Since 2014, several papers have been published to address game-based security modeling for the IoT. However, their scope focuses on mitigating impacts of certain attacks [9] or emphasizes model solutions for specific domains [10], [11]. Hamdi *et al.* [10] establish a Markov game-theoretic model to support decision making in the realm of IoT healthcare applications. Specifically, for smart things, the decision of whether or not authenticating a forwarding packet is based on the assessment of power life, channel bandwidth, memory capacity and compromised nodes through the game-based model. The performance of the model is evaluated through simulation which shows smart things extend their lifetime by adaptively adopting the security strategy. Chen *et al.* [9] propose a fusion-based defense mechanism to mitigate impacts of intentional attacks in the IoT architecture. They formulate a zero-sum game between the defense strategy and the attacker in the worst case scenario where the attacker knows the network topology and is capable of compromising all nodes simultaneously. The robustness of the IoT is greatly enhanced by the proposed mechanism through the results of performance evaluation. Rontidis *et al.* [11] develop a decision support method which minimizes security risks in the field of IoT prosumers selection. They formulate a non-cooperative and complete information game between the user and the attacker. The worst-case scenario is considered where the attacker knows all security controls of prosumers. Following this scenario, a mix strategy is proposed to randomize the prosumer selection in an optimal way and compared with two heuristic solutions through simulation which proves the effectiveness of the strategy in mitigating security risks.

From the aforementioned papers, there is no previous work on constructing a formal security model (e.g., Attack Graphs (AGs) [12], Attack Trees (ATs) [13]) for the IoT. In our work, we focus on constructing a graphical security model along with the security evaluation model and applying them to mitigating impacts of potential attacks for the IoT.

3. The Proposed Framework

The main goal of the framework is to depict all possible attack paths in the IoT, evaluate the security level of the IoT through security metrics, and assess the effectiveness of defense strategies. The proposed framework is shown in Figure 1. There are five steps in the framework: i) preprocessing, ii) security model generation, iii) visualization and storage, iv) security analysis, and v) changes and updates. We explain each step as follows:

In step 1, the security decision maker provides inputs needed to construct an IoT network. The inputs required are the total number of nodes, the network topology, and the vulnerability information for each node. The inputs are fed into the IoT Generator. The IoT Generator creates an IoT network with a specified network topology consisting of IoT nodes with their vulnerability information. The network topology is fixed after the generation. The security decision maker also selects the security metrics from a pre-defined metric pool which will be used as an input into the security analysis phase.

In step 2, the security model generation is performed. Our security model is developed based on a HARM [14] in which two layers are used to represent the network reachability information at the upper level and the vulnerability information at the lower level, respectively. Specifically, the Security Model Generator takes the constructed network with topology and vulnerability information as inputs and automatically computes all possible attack paths in the IoT network.

In step 3, the attack paths generated from the Security Model Generator are visualized in the form of an attack graph at the upper level and an attack tree at the lower level and stored for future use.

In step 4, the security analysis is carried out for the IoT network. The set of attack paths is taken as an input into the Security Evaluator along with the determined security metrics. Based on the metrics, the Security Evaluator can perform one of the two options. One is to output the analysis results directly and the other is to generate a text file and import the file into the analytic modeling and evaluation tool named Symbolic Hierarchical Automated Reliability and Performance Evaluator (SHARPE) [15] which computes the security analysis results. The security metric is selected from a pre-defined metric pool. Metrics for both the system level and the vulnerability level are defined in Table 1.

In step 5, any changes caused by the defense strategies are captured to update model inputs. Based on the security analysis results, the security decision maker knows which part of the IoT is the most vulnerable, thus being able to decide proper defense strategies. The deployment of the defense strategy changes either the vulnerability information (e.g., eliminates a specific vulnerability in an IoT node or mitigates the effect caused by the vulnerability) or the topology information, which should be updated and taken as the input to the Security Model Generator. When choosing the defense strategies, the security decision maker can also assess the effectiveness of different strategies via the framework by using security metrics, compare their effects and choose the best one among them.

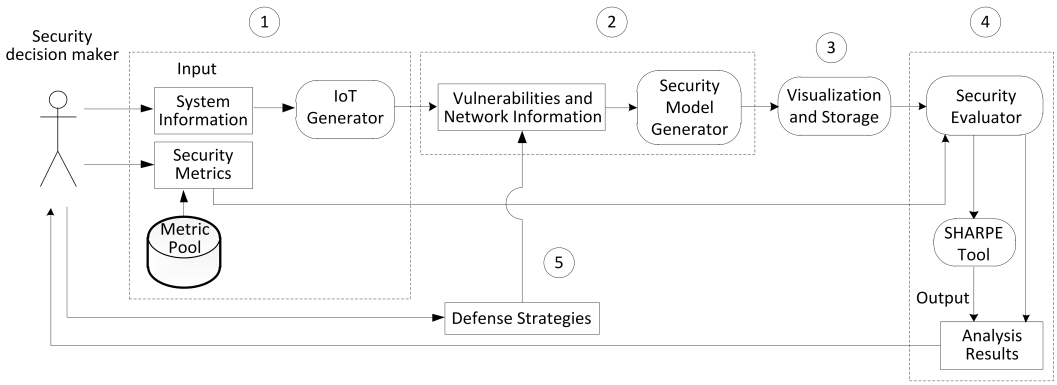

Figure 1. The proposed framework.

TABLE 1. DEFINITIONS OF SECURITY METRICS.

Levels	Metrics	Notations	Definitions
Vulnerability	Attack success probability	asp	Probability of an attacker to successfully exploit the vulnerability ([0,1])
	Attack cost	ac	Cost spent by an attacker to successfully exploit the vulnerability ([0,10])
	Risk	r	Potential harm caused by an attacker to successfully exploit the vulnerability ([0,10])
	Compromise rate	cr	Number of times of being compromised by an attacker in one unit time (hour)
System	Attack success probability	ASP	Probability of an attacker to successfully compromise the target ([0,1])
	Attack cost	AC	Minimum cost spent by an attacker to successfully compromise the target ([0,10])
	Risk	R	Maximum potential harm caused by an attacker to successfully compromise the target ([0,10])
	Mean-time-to-compromise	$MTTC$	Average time for the attacker to compromise the target (hour)

4. Evaluation

We present two example IoT networks; the WBAN in the domain of pervasive healthcare monitoring and the WSN in the domain of environment monitoring. The former example aims to demonstrate how the framework is used to identify possible attack paths, evaluate the system security and assess the effectiveness of the chosen defense strategy. The latter one shows the scalability of the framework.

4.1. An Example WBAN

4.1.1. Scenario Setup. In the WBAN, communications can be divided into two parts: the intra-body and the extra-body [16]. In the example network, we only consider the intra-body communication in the WBAN. Figure 2 shows an example network where 9 sensor nodes are placed on the human body along with one sink (e.g., PDA). Each node measures different health data (e.g., sn_1 measures the heart rate and the ECG (electrocardiogram) and sn_9 senses the blood oxygen respectively).

General assumptions are listed as follows:

- A tree based routing protocol is used for the intra-body communication [17]. Communications between sensor nodes and the sink are single hop or multi-hops.
- The network topology does not change in the body movement.
- A key management scheme is used to protect data confidentiality, data integrity and data authentication [18].

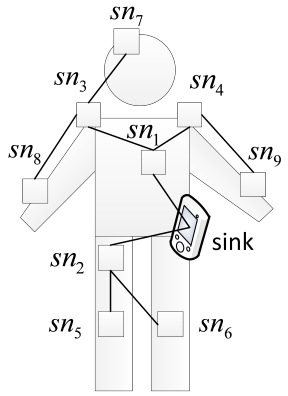

Figure 2. The intra-body communication network in the WBAN.

- Each sensor node runs identical operating system and has one vulnerability (e.g., the buffer overflow vulnerability in the operating system).
- Data packets are sent to the sink on pre-determined moments or immediately when an emergent problem occurs.
- The sink receives all information from sensors and provides an interface towards other networks (e.g., Internet).

The attacker model describes the attacker capabilities in the following:

1) In the WBAN, it is difficult for an attacker to physically access nodes without being detected.

Thus the attacker only has a remote access to the network. He can communicate with part of the network through wireless communication.

2) The attacker has a laptop-class device. He can exploit the buffer overflow vulnerability targeting the operating system to compromise a sensor node within an accepted time. Once a node is compromised, the attacker has full control (e.g., steal cryptographic keys, obtain routing table, inject and run arbitrary code). He can also reprogram the compromised node into a malicious node and exploit it to compromise other nodes.
3) The sink is assumed to be strongly protected such that the attacker cannot compromise the sink.

4.1.2. Security Modeling and Analysis. We come up with two scenarios for the example WBAN. In terms of the defense strategy for the buffer overflow, we can deploy the method of address space layout randomization (ASLR) for each node. The ASLR is based upon the low chance of an attacker guessing locations of randomly placed areas, thus enhancing the security by increasing the search space. We make assumptions on values of security metrics used for the node vulnerability in Table 2. Due to the limited space, explaining the meaning of specific values for each security metric is not considered (e.g., high or low).

TABLE 2. METRIC VALUES FOR THE NODE VULNERABILITY IN THE EXAMPLE WBAN.

Strategy \ Metric	asp	ac	r	cr
Without defense	0.7	3	5	0.4
With ASLR	0.2	8	1	0.25

Scenario 1: one access point and one target. We assume the attacker's goal is to compromise sn_1 and steal critical data stored on it. The attacker is supposed to take sn_9 as the access point by compromising it and exploit it to compromise other nodes. Figure 3 shows the visualized HARM in which A represents the attacker and v_1 denotes the buffer overflow vulnerability. The attack graph at the upper layer indicates the attack path in the network and the attack tree at the lower layer depicts the vulnerability information of the node. The formal definition of the two-layer HARM can be found in [14].

For the analysis results, without defense, ASP is 0.973; with ASLR, it drops to 0.488. AC changes from 9 to 24 while R is decreased to 3 compared with 15 originally. Figure 4 shows the analysis results of comparing system reliabilities under $MTTC$. $MTTC$ increases by approximately 0.49997 hour when considering the defense strategy.

Scenario 2: multiple access points and one target. We assume the attacker has the same target with scenario 1 but is able to take either sn_3 or sn_9 as the access point. Figure 5 shows the visualized HARM with two layers.

For the analysis results, without defense, ASP is 0.88543; with ASLR, it is reduced to 0.17568. AC increases from 6 to 16. With ASLR, R is decreased to 3 compared with 15 originally. Figure 6 shows analysis results of comparing system reliabilities under $MTTC$. $MTTC$ increases by approximately 0.95 hour when considering the defense strategy.

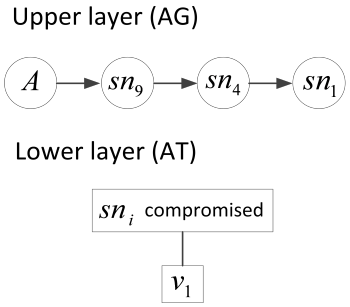

Figure 3. A two-layer HARM for scenario 1.

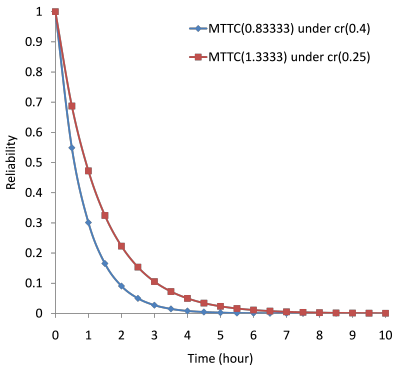

Figure 4. Results of comparing system reliabilities in scenario 1.

4.2. An Example WSN

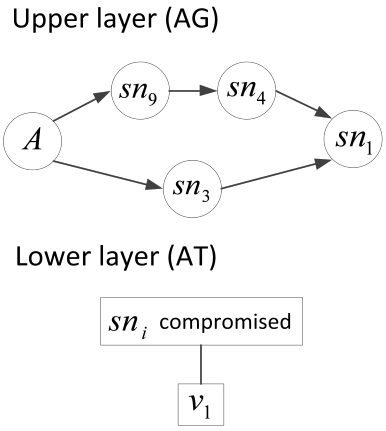

Figure 5. A two-layer HARM for scenario 2.

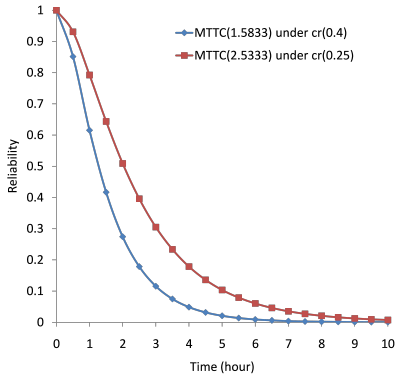

Figure 6. Results of comparing system reliabilities in scenario 2.

4.2.1. Scenario Setup. We consider a WSN with 1000 sensor nodes and one base station deployed in an open and unattended field. General assumptions are listed as follows:

- Sensor nodes and the base station are static after deployment.
- Sensor nodes self-organize and form a routing tree which is rooted at the base station [19].
- Each sensor has a transmission range of r meters and uses bidirectional wireless communication. Communications between the base station and sensor nodes are single-hop or multi-hops.
- Data packets are encrypted by employing a pair-wise key scheme [20].
- The base station is connected to the Internet and becomes the gateway between the sensor network and the Internet.
- Sensor nodes periodically send packets to the base station (e.g., in every 10 minutes).

The attacker model is based on [21] which describes the attacker capabilities as follows:

1) In the wireless communication, radio links are insecure. We assume an attacker can eavesdrop on radio transmissions by distributing a wireless monitoring device in the area of interest. The transmission range of the monitoring device is larger than the transmission range of a sensor node (e.g., $3r$) but does not cover the entire network.
2) The attacker can physically move from one location to another location in the network but cannot monitor the entire network.
3) Each node routes packets in a fixed path to the base station under wireless communication. Thus the attacker can launch a rate monitoring attack to deduce the location of the base station by monitoring packet sending rate of nodes and moving to nodes with the higher rate.
4) As the base station is in an open environment, the attacker can physically damage it once he discovers its location.

In terms of the defense strategy, we can deploy the multi-parent routing scheme proposed in [21]. When forwarding a packet, the node randomly selects one of its parent nodes to forward the packet. We use estimated values for input security metrics used for the node vulnerability in Table 3.

TABLE 3. METRIC VALUES FOR THE NODE VULNERABILITY IN THE EXAMPLE WSN.

Node/Strategy \ Metric		asp	ac	r	cr
Sensor node	Without defense	0.6	7	8	2.0
	With defense	0.3	9	5	0.25
Base station		0.2	8	9	0.05

4.2.2. Security Modeling and Analysis. We assume that the attacker's goal is to destroy the base station physically. The attacker is assumed to access one sensor node (e.g., a node deployed in the edge of the network). Due to the limited space, we only present the analysis results.

With the defense strategy, ASP changes from 0.99979 to 0.52696; AC increases from 71 to 89; R decreases from 81 to 54. Figure 7 shows the analysis results of comparing system reliabilities under $MTTC$. $MTTC$ increases by approximately 1.467998 hour when considering the defense strategy.

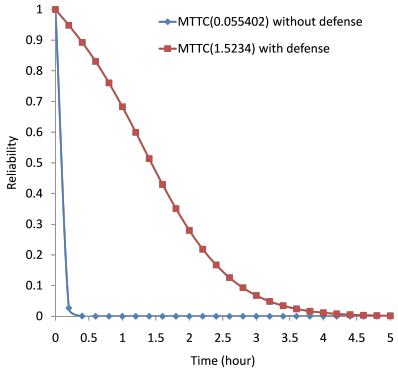

Figure 7. Results of comparing system reliabilities under $MTTC$.

4.3. Discussions and Limitations

More security analysis can be made in the following aspects:

Introducing multiple targets: we use one target in each example. One can introduce multiple targets, compute attack paths for each target separately and do analysis through security metrics. If there is a limit for the security budget, decisions about deploying defense strategies can be made based on comparing various metric values.

Considering different defense strategies: we only utilize one strategy for the vulnerability. One can consider multiple strategies and compare their effects via the models.

There are several limitations of the framework we aim to resolve in the future research.

Addressing the heterogeneity: we only consider the sensor networks consisting of identical nodes. As the nature of the IoT is heterogeneous, the security model should be able to tackle this problem. An idea is to develop a three layer hierarchical attack model in which the upper layer represents the cluster reachability information (e.g., nodes of the same type form a cluster), the middle layer captures the network topology information, and the lower layer depicts the vulnerability information of nodes. The three layer hierarchical structure will also make the model more practical to deal with the scalability issue.

Tackling the mobility: when analyzing the example networks, we assume the topology is static. However, one of the key features of the IoT is the mobility. Thus the model needs to be extended to deal with the mobility problem. An idea is to construct a model to capture changes in the network (e.g., nodes join in or move out) and update other models in the framework.

5. Conclusion

Modeling security of the IoT is a complex task as the IoT is characterized by a large number of heterogeneous and mobile nodes. In the paper, we have presented a framework of modeling and assessing security for the IoT which encompasses five steps: i) preprocessing, ii) security model generation, iii) visualization and storage, iv) security analysis, and v) changes and updates. In the framework, we have developed an IoT Generator, a Security Model Generator and a Security Evaluator. Two example IoT networks were provided to demonstrate the capabilities of the framework on mitigating impacts of potential attacks and addressing the scalability problem.

References

[1] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613000054

[2] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, pp. 51–58, Sept 2011.

[3] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971

[4] J. Hong and D. Kim, "HARMs: Hierarchical Attack Representation Models for Network Security Analysis," in *Proceedings of the 10th Australian Information Security Management Conference in SECAU Security Congress (SECAU 2012)*, Dec 2012.

[5] S. Radomirovic, "Towards a Model for Security and Privacy in the Internet of Things," in *Proceedings of 1st International Workshop Security of the Internet of Things (SecIoT 2010).*, 2010.

[6] J.-C. Yang and B.-X. Fang, "Security model and key technologies for the Internet of things," *The Journal of China Universities of Posts and Telecommunications*, vol. 18, Supplement 2, pp. 109–112, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1005888510601598

[7] H. Abie and I. Balasingham, "Risk-based Adaptive Security for Smart IoT in eHealth," in *Proceedings of the 7th International Conference on Body Area Networks*, ser. BodyNets '12. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 269–275. [Online]. Available: http://dl.acm.org/citation.cfm?id=2442691.2442752

[8] T. Stepanova and D. Zegzhda, "Applying Large-scale Adaptive Graphs to Modeling Internet of Things Security," in *Proceedings of the 7th International Conference on Security of Information and Networks*, ser. SIN '14. New York, NY, USA: ACM, 2014, pp. 479–482. [Online]. Available: http://doi.acm.org/10.1145/2659651.2659696

[9] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Information Fusion to Defend Intentional Attack in Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 337–348, Aug 2014.

[10] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in *2014 IEEE International Conference on Communications (ICC)*, June 2014, pp. 920–925.

[11] G. Rontidis, E. Panaousisy, A. Laszkaz, T. Dagiuklas, P. Malacariax, and T. Alpcan, "A Game-Theoretic Approach for Minimizing Security Risks in the Internet-of-Things," in *IEEE Workshop on Security and Privacy for Internet of Things and Cyber-Physical Systems (IEEE ICC 2015 - IoT/CPS Security 2015)*, 2015.

[12] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. Wing, "Automated Generation and Analysis of Attack Graphs," CMU, Tech. Rep., 2002.

[13] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*. John Wiley and Sons Inc., 2000.

[14] J. Hong and D. Kim, "Assessing the Effectiveness of Moving Target Defenses using Security Models," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–1, 2015.

[15] R. A. Sahner, K. Trivedi, and A. Puliafito, *Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software Package*. Springer Publishing Company, Incorporated, 2012.

[16] B. Latre, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A Survey on Wireless Body Area Networks," *Wirel. Netw.*, vol. 17, no. 1, pp. 1–18, Jan. 2011. [Online]. Available: http://dx.doi.org/10.1007/s11276-010-0252-4

[17] B. Latre, B. Braem, I. Moerman, C. Blondia, E. Reusens, W. Joseph, and P. Demeester, "A Low-delay Protocol for Multihop Wireless Body Area Networks," in *4th Annual International Conference on Mobile and Ubiquitous Systems: Networking Services, 2007. (MobiQuitous 2007)*, Aug 2007, pp. 1–8.

[18] D. Singelee, B. Latre, B. Braem, M. Peeters, M. De Soete, P. De Cleyn, B. Preneel, I. Moerman, and C. Blondia, "A Secure Cross-Layer Protocol for Multi-hop Wireless Body Area Networks," in *Ad-hoc, Mobile and Wireless Networks*, ser. Lecture Notes in Computer Science, D. Coudert, D. Simplot-Ryl, and I. Stojmenovic, Eds. Springer Berlin Heidelberg, 2008, vol. 5198, pp. 94–107. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-85209-4-8

[19] A. Woo, T. Tong, and D. Culler, "Taming the Underlying Challenges of Reliable Multihop Routing in Sensor Networks," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, ser. SenSys '03. New York, NY, USA: ACM, 2003, pp. 14–27. [Online]. Available: http://doi.acm.org/10.1145/958491.958494

[20] L. Eschenauer and V. D. Gligor, "A Key-management Scheme for Distributed Sensor Networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 41–47. [Online]. Available: http://doi.acm.org/10.1145/586110.586117

[21] J. Deng, R. Han, and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005. (SecureComm 2005)*, Sept 2005, pp. 113–126.