NETWORK LEVEL DEFENSES FOR INTERNET OF THINGS

Bilal Ishfaq

Supervisor: Dr. Fabian Gilson

Co-Supervisor: Dr. Dong Seong Kim

Co-Supervisor: Dr. Mengmeng Ge

Department of Computer Science and Software Engineering

University of Canterbury, New Zealand.

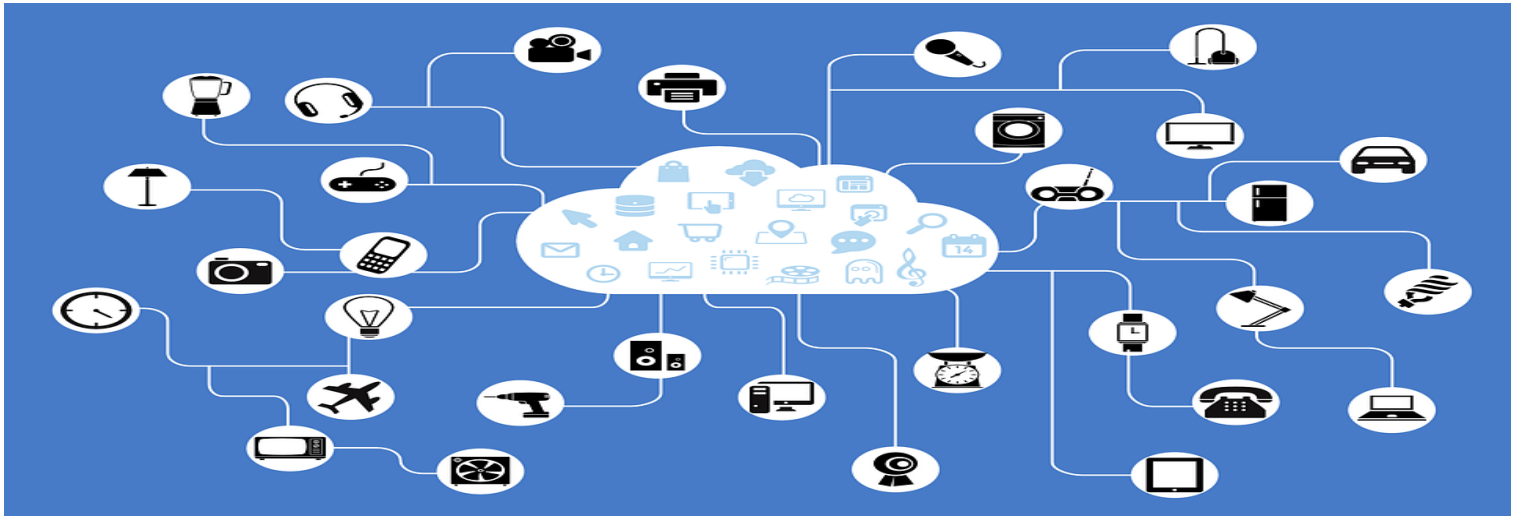
UC
UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha

Outline

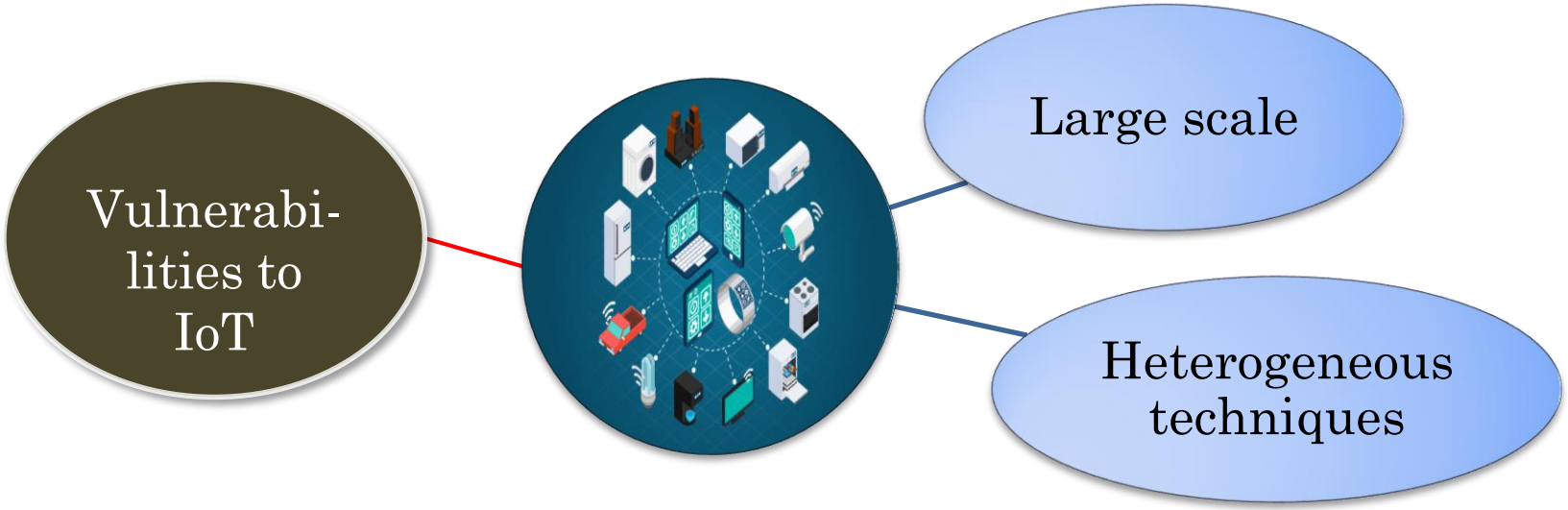
- Introduction
- Related Work
- Objectives
- Testbed Configuration
- Proposed Network-Level Defenses
  - Reactive Defense Mechanism
    - Network Topology Reconfiguration on Intrusion Detection
  - Proactive Defense Mechanism
    - Decoy system with MTD
    - Node-Level MTD
    - Distributed MTD Shuffling
- References

Introduction - IoT

- Refers to a world where everyday physical objects become locatable, addressable and reachable in the virtual world, and are able to communicate with each other and with other entities (e.g., human beings) [6].



INTRODUCTION – IOT (CONT..)



- Attackers can launch various attacks by exploiting the vulnerabilities [1].
- The typical advice for avoiding cyber attacks continues to be install the latest patch.
- However, the most obvious security challenge with IoT devices is the inability to easily upgrade or patch them (e.g. medical devices).

Outline

- Introduction
- Related Work
- Objectives
- Testbed Configuration
- Proposed Network-Level Defenses
  - Reactive Defense Mechanism
    - Network Topology Reconfiguration on Intrusion Detection
  - Proactive Defense Mechanism
    - Decoy system with MTD
    - Node-Level MTD
    - Distributed MTD Shuffling
- References

Related Work

- Related work: SD-IoT security issues:
  - Chakrabarty et al. [2]
  - Geng et al. [14]
  - Sandor et al. [3]
  - Bull et al. [16]
  - Grigoryan et al.[15]
  - Mengmeng et al. [22]

These researches are based on the simulation work and we consider the real testbed implementation.

- Related work: Deception with Moving Target Defense (MTD)
  - Pa et al. [17]
  - La et al. [18]
  - Anirudh et al. [8]
  - Casola et al. [19]
  - Sherburne et al. [20]
  - Mahmood et al. [21]

These researches propose the MTD mechanisms while we integrate the MTD with cyberdeception in order to make the complex attack surface..

Outline

- Introduction
- Related Work
- Objectives
- Testbed Configuration
- Proposed Network-Level Defenses
  - Reactive Defense Mechanism
    - Network Topology Reconfiguration on Intrusion Detection
  - Proactive Defense Mechanism
    - Decoy system with MTD
    - Node-Level MTD
    - Distributed MTD Shuffling
- References

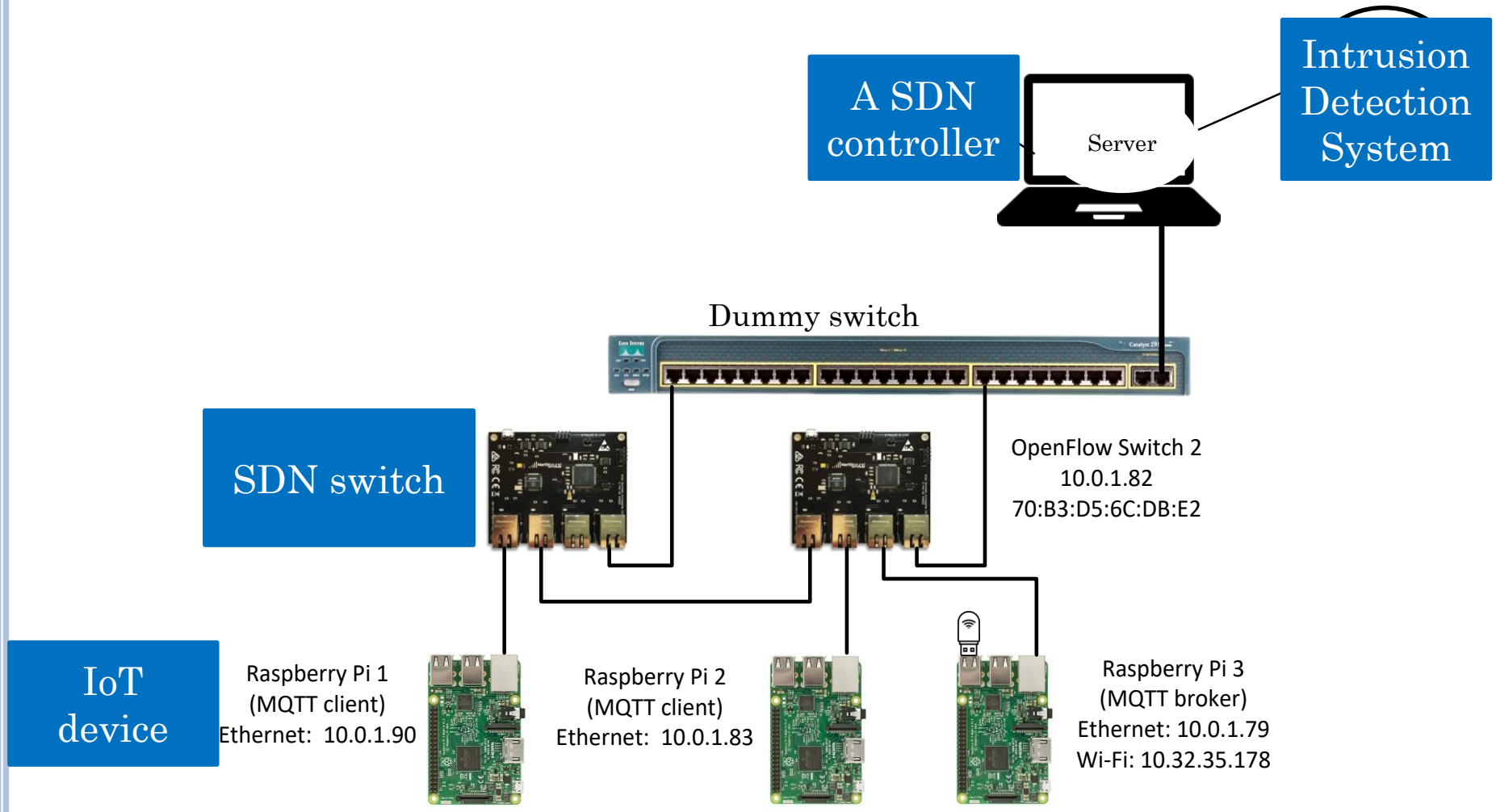
Objectives

- First, we design and implement an IoT testbed using SDN for the IoT network security with the following objectives:
  - To collect security related data from the testbed for large scale simulation of IoT networks.
  - Execute and validate the feasibility of network level defenses for IoT on IoT testbed.
- Second, we propose network level defenses:
  - Reactive defense mechanisms based on the reconfiguration of the IoT network topology.
  - Proactive defense mechanisms using both deception and moving target defense (MTD) techniques.

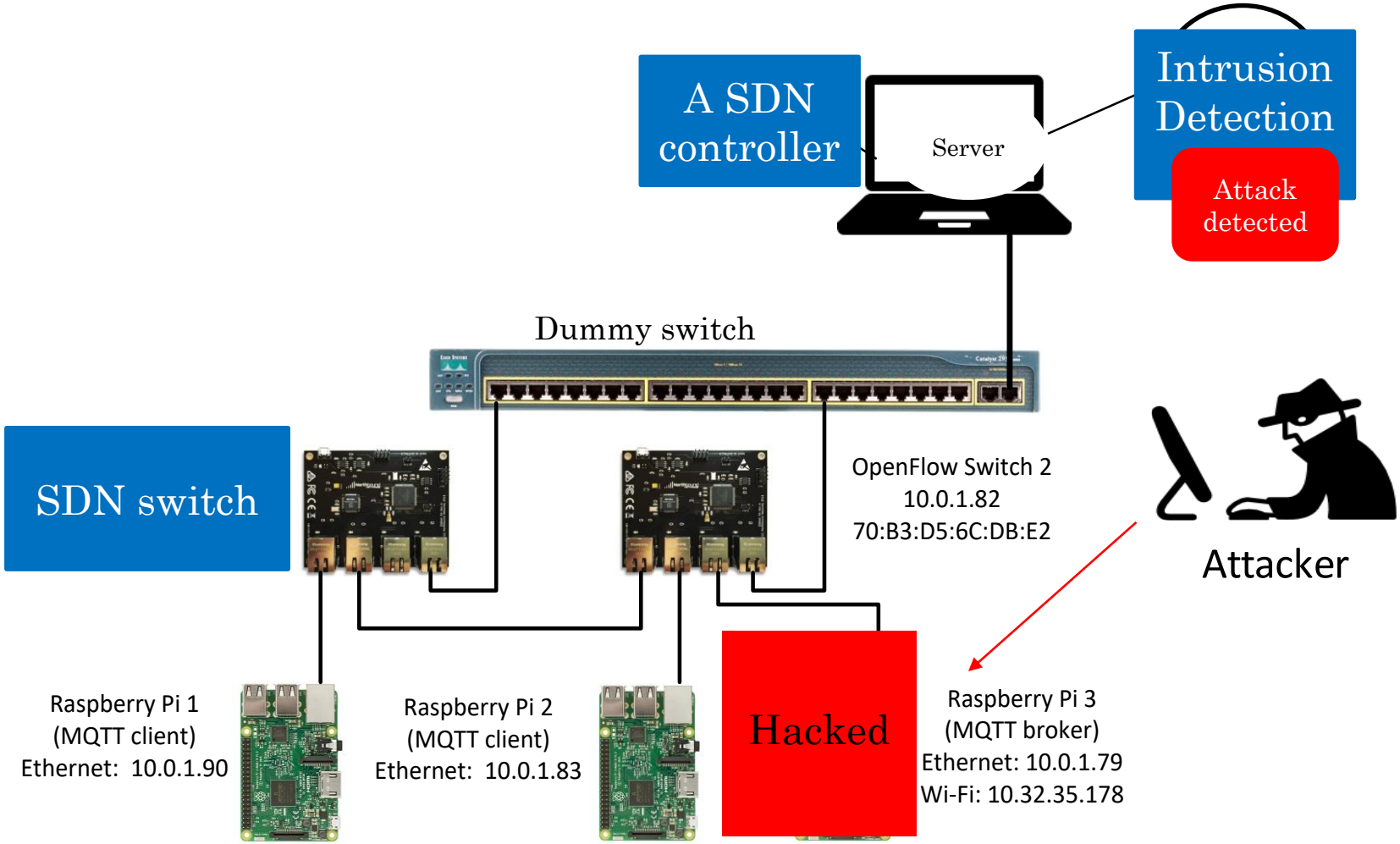
Outline

- Introduction
- Related Work
- Objectives
- Testbed Configuration
- Proposed Network-Level Defenses
  - Reactive Defense Mechanism
    - Network Topology Reconfiguration on Intrusion Detection
  - Proactive Defense Mechanism
    - Decoy system with MTD
    - Node-Level MTD
    - Distributed MTD Shuffling
- References

TESTBED CONFIGURATION
A SMALL IOT NETWORK IS WORKING!



Testbed Configuration
If an IoT device is being hacked?



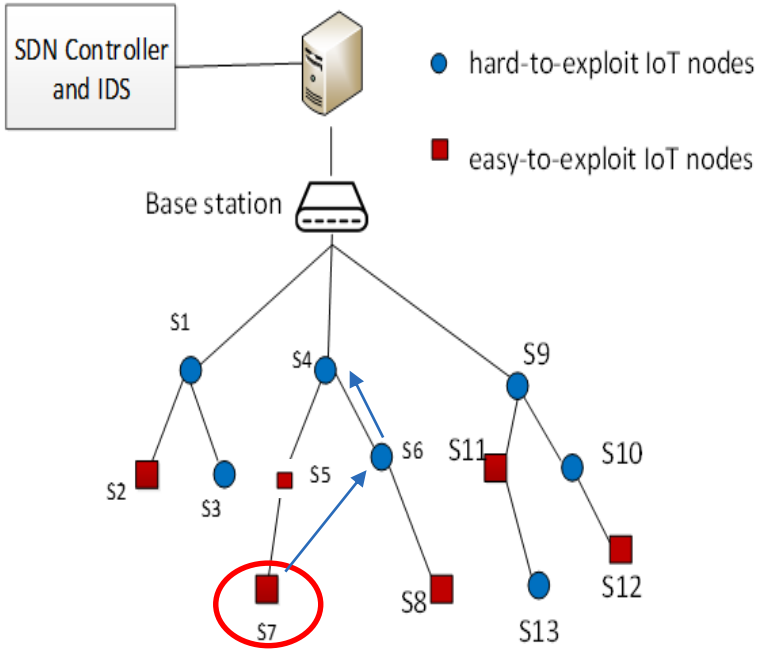
Outline

- Introduction
- Related Work
- Objectives
- Testbed Configuration
- Proposed Network-Level Defenses
  - Reactive Defense Mechanism
    - Network Topology Reconfiguration on Intrusion Detection
  - Proactive Defense Mechanism
    - Decoy system with MTD
    - Node-Level MTD
    - Distributed MTD Shuffling
- References

Reactive Defense Mechanism:
Network Topology Reconfiguration:
One Node Under Scanning Attack and applying MTD:

- The main objective is to maximize the number of hard to exploit IoT nodes and to minimize or the same number of hop count along the path to base station.

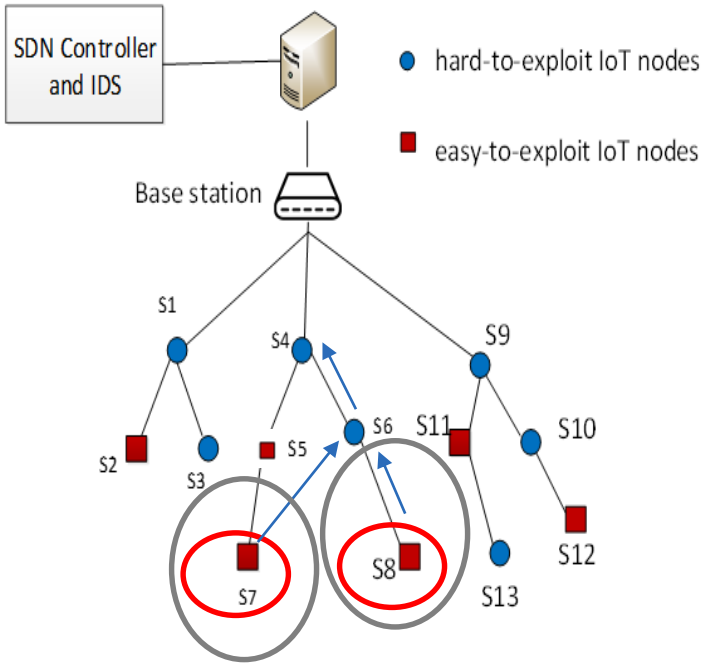
Example IoT Network:



- We consider one node is under scanning attack.
- The IoT network topology reconfiguration takes place on intrusion detection and follows the following step;
  - Compute the possible reconfigured set of topologies in the same communication range of IoT nodes before intrusion detection and apply the best suitable when intrusion is detected.
- The MTD technique of reconfiguring the IoT network topology takes place as follows;
  - If the node under the scanning attack is easy to exploit, it checks for the next neighbour nodes, whether it is easy to exploit or hard to exploit.
  - Establish the connection to the node which is hard to exploit and offering the minimum or same number of hop count along the path to the base station.

Reactive Defense Mechanism (Cont..)
Network Topology Reconfiguration (Cont..)
Two Nodes Under Scanning Attack and applying MTD
Step-by-Step

Example IoT Network:



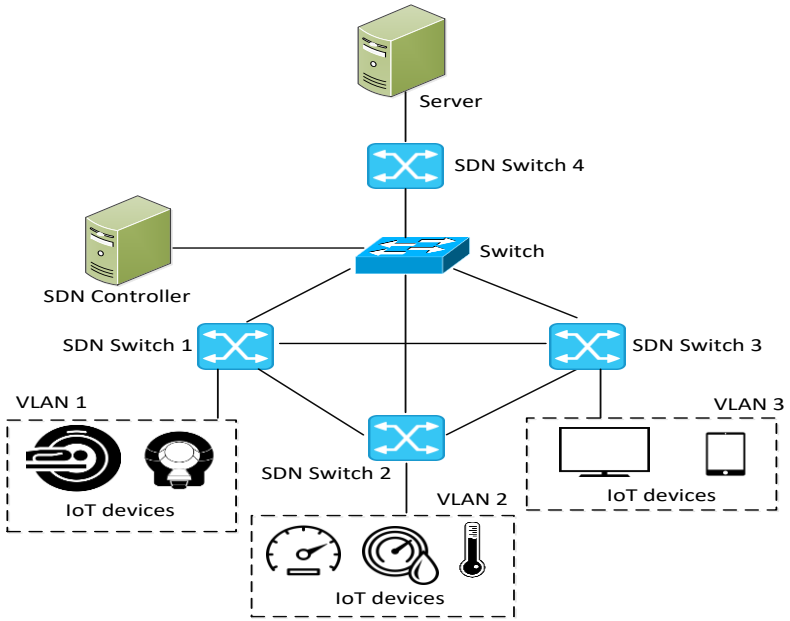
- We consider two IoT nodes under scanning attack.
- The IoT network topology reconfiguration takes place step by step as follows;
  - If the node under the scanning attack is easy to exploit, it establish the connection to the next hard to exploit IoT node, offering the minimum number of hop count.
  - By considering the recent shuffled topology and taking it as input, again apply MTD technique and establish the connection with the next hard to exploit IoT node.
  - If both of the next IoT nodes are hard to exploit then the connection establishes to the one which is again offering minimum number of hop counts.

Outline

- Introduction
- Related Work
- Objectives
- Testbed Configuration
- Proposed Network-Level Defenses
  - Reactive Defense Mechanism
    - Network Topology Reconfiguration on Intrusion Detection
  - Proactive Defense Mechanism
    - Decoy system with MTD
    - Node-Level MTD
    - Distributed MTD Shuffling
- References

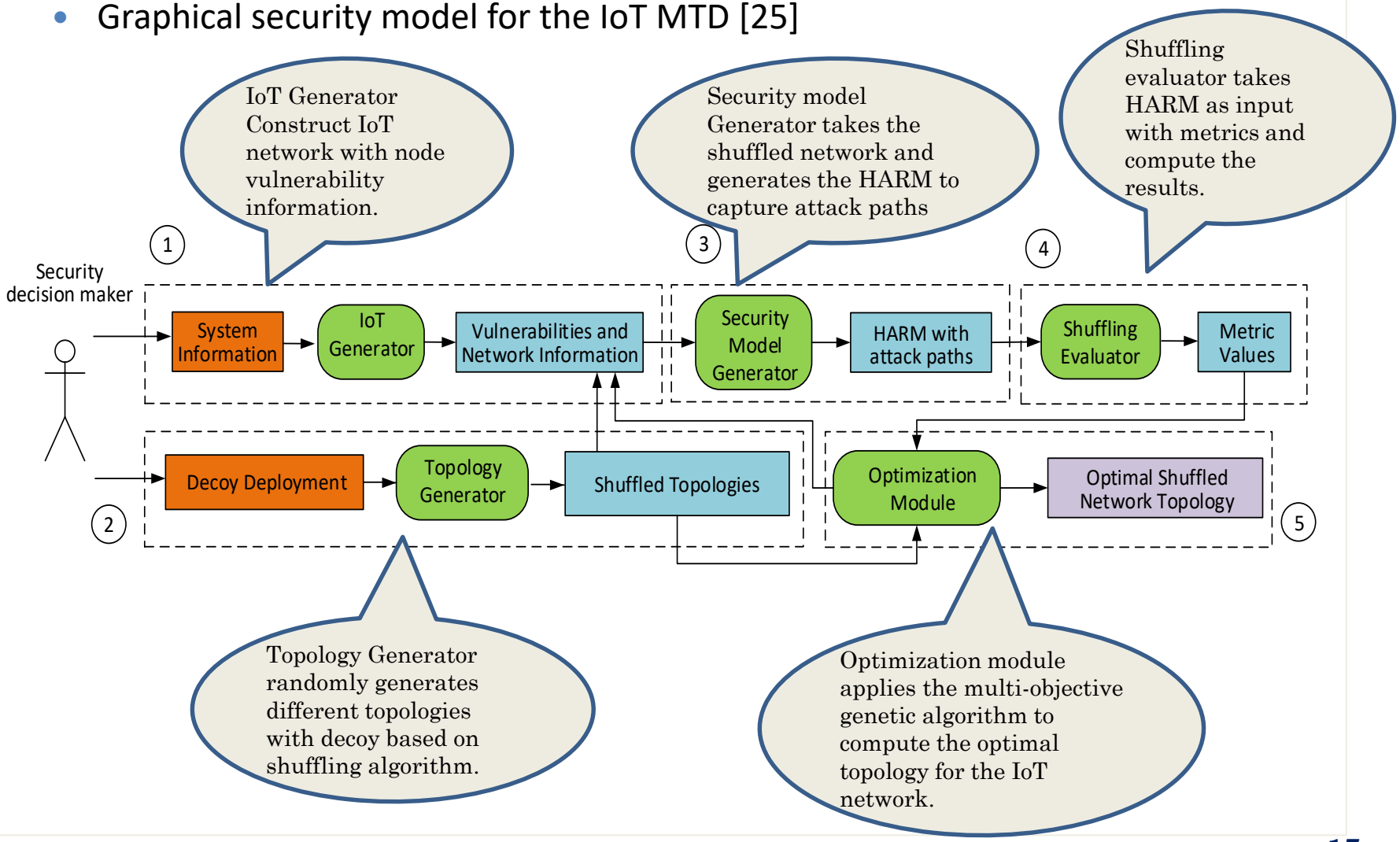
PROACTIVE DEFENSE MECHANISM:

- Decoy System with Moving Target Defense (MTD):
  - An integrated defense mechanism for SD-IoT network based on cyber-deception technology.
  - It is network topology shuffling-based MTD technique which is executed adaptively with system security vulnerability.
- **Example IoT Network:**



- Develop an integrated proactive defense system by proposing an adaptive MTD technique which maximize the hurdles for the attackers to launch their attacks.
- Use an algorithm for the random shuffling of IoT network topology which changes the connections between the IoT nodes and gives the optimal IoT network topology as a defense solution.

- Decoy System with MTD (cont..):
  - Graphical security model for the IoT MTD [25]



Outline

- Introduction
- Related Work
- Objectives
- Testbed Configuration
- Proposed Network-Level Defenses
  - Reactive Defense Mechanism
    - Network Topology Reconfiguration on Intrusion Detection
  - Proactive Defense Mechanism
    - Decoy system with MTD
    - Node-Level MTD
    - Distributed MTD Shuffling
- References

PROACTIVE DEFENSE MECHANISM (CONT..)

- Node Level MTD:
  - The overall concept is the implementation of MTD at node level in SD-IoT network.
  - The defense mechanism includes both the real and decoy IoT nodes.
  - It is based on IP address randomization.
  - A set of virtual IP addresses for each IoT node is defined by generating a list of random IP addresses, via algorithm.
  - Each IoT node also has one real IP address.
  - The IoT nodes change the virtual IP addresses at a defined time interval.
  - All the IoT nodes use virtual IP address to communicate with each other.

Outline

- Introduction
- Related Work
- Objectives
- Testbed Configuration
- Proposed Network-Level Defenses
  - Reactive Defense Mechanism
    - Network Topology Reconfiguration on Intrusion Detection
  - Proactive Defense Mechanism
    - Decoy system with MTD
    - Node-Level MTD
    - Distributed MTD Shuffling
- References

PROACTIVE DEFENSE MECHANISM (CONT..)

- Distributed MTD Shuffling for IoT:
  - We propose a distributed MTD defense mechanism for large scale IoT network.
  - It uses the concept of cluster head.
  - IoT nodes are distributed in an environment at different places, so one of the IoT node from specific area is considered as head IoT node.
  - We consider that all the IoT nodes in this specific area are controlled by the head IoT node.
  - The head IoT node communicates with the SDN controller on behalf of the IoT nodes under its control.
  - We assume that the head IoT node has capability to determine the MTD shuffling for the IoT nodes.
- Realistic for large scale IoT Network:
  - This defense mechanism is realistic for large scale IoT network as it uses multiple IoT nodes head for MTD shuffling instead of one centralized SDN controller.

THANK YOU!

Reference

[1] Mengmeng Ge, Jin B. Hong, Simon Enoch Yusuf, Dong Seong Kim, Proactive defense mechanisms for the Software-defined Internet of Things with non-patchable vulnerabilities, Future Generation Computer Systems, Volume 78, Part 2, 2018.

[2] S. Chakrabarty, D. W. Engels and S. Thathapudi, "Black SDN for the Internet of Things," 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Dallas, TX, 2015, pp. 190-198.

[3] H. Sándor, B. Genge and G. Sebestyén-Pál, "Resilience in the Internet of Things: The Software Defined Networking approach," 2015 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, 2015, pp. 545-552.

[4] T. Theodorou and L. Mamatas. Software Defined Topology Control Strategies for the Internet of Things. In Proceedings of the 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN '17), 2017.

[5] T. Xu, D. Gao, P. Dong, H. Zhang, C. H. Foh, and H. C. Chao. Defending Against New-Flow Attack in SDN-Based Internet of Things. IEEE Access, 5:3431–3443, 2017.

[6] Antonino Rullo, Daniele Midi, Edoardo Serra, and Elisa Bertino. 2017. Pareto Optimal Security Resource Allocation for Internet of Things. ACM Transactions on Privacy & Security 20, 4 (Oct. 2017), 15:1–15:30.

[7] A. Rullo, E. Serra, E. Bertino, and J. Lobo. 2017. Shortfall-Based Optimal Security Provisioning for Internet of Things. In Proceedings of 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS '17). IEEE, 2585–2586.

[8] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi. 2017. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP '17). IEEE, 1–4.

REFERENCE

[9] S. Dowling, M. Schukat, and H. Melvin. 2017. A ZigBee Honeypot to assess IoT Cyberattack Behaviour. In Proceedings of the 2017 28th Irish Signals and Systems Conference (ISSC ’17). IEEE, 1–6.

[10] J.-H. Cho and N. Ben-Asher, "Cyber defense in breadth: Modeling and analysis of integrated defense systems," *The Journal of Defense Modeling and Simulation,* vol. 15, no. 2, pp. 147-160, 2018.

[11] J.-H. Cho, Y. Wang, I. Chen, K. S. Chan, and A. Swami, "A Survey on Modeling and Optimizing Multi-Objective Systems," *IEEE Communications Surveys Tutorials,* vol. 19, no. 3, pp. 1867-1901, 2017.

[12] F. C. Gärtner, "Byzantine failures and security: Arbitrary is not (always) random," 2003.

[13] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications,* vol. 83, pp. 12-27, 2017.

[14] H. Geng, K. A. Kwiat, C. A. Kamhoua, and Y. Shi. On Random Dynamic Voltage Scaling for Internet-of-Things: A Game-Theoretic Approach. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(1):123{132, 2018.

[15] G. Grigoryan, Y. Liu, L. Njilla, C. Kamhoua, and K. Kwiat. Enabling Cooperative IoT Security via Software Defined Networks (SDN). *arXiv preprint arXiv:1806.01885*, 2018.

[16] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson. Flow Based Security for IoT Devices Using an SDN Gateway. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud ’16), pages 157–163. IEEE, 2016.

[17] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, and Christian Rossow. 2015. IoTPOT: Analysing the Rise of IoT Compromises. In Proceedings of the 9th USENIX Workshop on Offensive Technologies (WOOT ’15). USENIX Association.

[18] Q. D. La, T. Q. S. Quek, J. Lee, S. Jin, and H. Zhu. 2016. Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things. IEEE Internet of Things Journal 3, 6 (2016), 1025–1035.

REFERENCE

[19] V. Casola, A. De Benedictis, and M. Albanese, "A moving target defense approach for protecting resource-constrained distributed devices," in *Information Reuse and Integration (IRI), 2013 IEEE 14th International Conference on*, 2013, pp. 22-29: IEEE.

[20] 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*, 2014, pp. 37-40: ACM.

[21] K. Mahmood and D. M. Shila, "Moving target defense for Internet of Things using context aware code partitioning and code diversification," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 329-330: IEEE.

[22] Mengmeng Ge, Jin B. Hong, Simon Enoch Yusuf, Dong Seong Kim, Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities, Future Generation Computer Systems, Volume 78, Part 2, 2018

[23] Özçelik, Mert, Niaz Chalabianloo, and Gürkan Gür. "Software-defined edge defense against IoT-based DDoS." *2017 IEEE International Conference on Computer and Information Technology (CIT)*. IEEE, 2017.

[24] Albanese, M., De Benedictis, A., Jajodia, S., & Sun, K. (2013, October). A moving target defense mechanism for manets based on identity virtualization. In *2013 IEEE Conference on Communications and Network Security (CNS)* (pp. 278-286). IEEE.

[25] Ge, Mengmeng, and Dong Seong Kim. "A framework for automating security analysis of the internet of things." *Journal of Network and Computer Applications* 83 (2017): 12-27.

[26] M. Ge, **J.H. Cho**, B. Ishfaq, and D. S. Kim, "Modeling and Analysis of Integrated Proactive Defense Mechanisms for Internet-of-Things," Modeling and Design of Secure Internet of Things (Editors: Kamhoua et al.), 2019, IEEE Press (under press).