FIREWORK: Fog orchestration for secure IoT networks

Maryam Vahabi[1], Hossein Fotouhi[1], and Mats Björkman[1]

Mälardalen University; School of Innovation, Design, and Technology
{hossein.fotouhi, maryam.vahabi, mats.bjorkman}@mdh.se

Abstract. Recent advances in Internet of Things (IoT) connectivity have made IoT devices prone to Cyber attacks. Moreover, vendors are eager to provide autonomous and open source device, which in turn adds more security threat to the system. In this paper, we consider network traffic attack, and provide a Fog-assisted solution, dubbed as FIREWORK, that reduces risk of security attacks by periodically monitoring network traffic, and applying traffic isolation techniques to overcome network congestion and performance degradation.

1 Introduction

Internet of Things (IoT) considers billions of devices and objects connected to Internet in order to collect and exchange information to offer various application domains, such as health monitoring, industrial automation, home automation and environmental monitoring. IoT devices are equipped with sensor(s) and processing power, enabling them to be deployed in many environments [23]. The research and development in IoT devices in both academia and industry have failed to provide secure devices. Thus, security experts have warned for the potential risk of having large numbers of unsecured devices connected to the Internet [15].

In December 2013, a researcher at a security company (Proofpoint) found the first IoT botnet. According to Proofpoint, more than 25% of the botnet was generated by devices other than computers, including smart TVs, baby monitors, and other household appliances. Recently, New Hampshire-based provider of domain name services (Dyn) experienced service outages as a result of what appeared to be well coordinated attack [12]. On October 21, 2016, many websites including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud, and The New York Times were reported inaccessible by users caused by a distributed denial of service attack (DDoS) attack using a network of consumer devices from the IoT.

Many security issues and challenges have been identified in the literature that focus on various IoT standard protocols at the PHY, MAC, network and application layers [10]. Some of the security issues are known as authentication, access control, confidentiality, privacy, trust, secure middleware, mobile security and policy enforcement [18]. However, addressing each of these issues in traditional IoT architectures require high bandwidth utilization and high processing and memory capabilities.

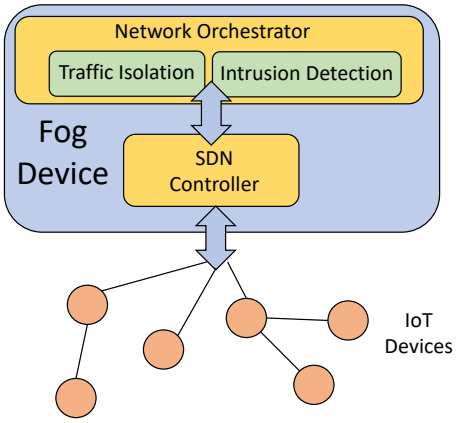

Fig. 1. Orchestration in Fog-based IoT networks.

Fog computing has been introduced to bring the provision of services closer to the end-users and IoT devices by pooling the available computing, storage and networking resources at the edge of the network [6, 22]. The decentralized computing architecture provides the opportunity of collaboration between IoT devices and the edge devices to reduce the processing burden on resource-constrained devices, reaching latency requirements of delay-sensitive applications and overcome the bandwidth limitations for centralized services [26].

To the best of our knowledge, the research on security considering the Fog computing architecture for IoT devices is still in its preliminary stages. In this paper, we consider the coexistence of IoT and Fog devices in the network. We tackle security issue as one of the main elements of different IoT applications. **We provide an idea to overcome security threat imposed by network traffic attacks by considering Fog-based IoT networks.**

Coordinating and orchestrating of future IoT networks with heterogeneous devices is of paramount importance. It is common to experience devices generating different types of traffic (low or high, periodic or sporadic). It is nontrivial to manage the traffic without a central management unit, while being capable of detecting suspicious traffic. There are some related works in the literature, where the main focus is on the design of a generic protocol stack [21], which is more suitable for traditional network architecture with the IoT-Cloud layers. Moreover, such solutions will add more cost to the system as each IoT device requires higher level of inteligence. This paper concentrates on a novel orchestration architecture based on using Software Defined Networking (SDN) controller as one of the major components of a Fog computing architecture for IoT networks. The proposed orchestration approach launches upon detecting a security threat in the network, where part of the suspicious traffic will be isolated. Figure 1 depicts the general architecture of a Fog-based IoT network, where the network orchestrator runs network management in terms of intrusion detection as well as traffic isolation.

The main contributions of this work for reducing network security attacks through network traffic are: (1) the need for exploiting a run-time intrusion detection algorithm, and (2) the need for running a traffic isolation algorithm upon detecting an intrusion in the network. These algorithms are currently rough ideas that are under implementation.

We have defined few research questions (RQ) that are necessary to answer while designing and implementing such intrusion detection algorithms:

RQ1. *How to identify an intrusion in an IoT network?* In order to prevent and confront a security threat, it is crucial to devise a mechanism to identify intrusion in the network. There are various ways that the system may have vulnerabilities and holes. **This work limits the intrusion attacks to additional traffic that leads to network congestion.**

RQ2. *What are the benefits of security approach in a three-tiered network architecture (Iot-Fog-Cloud) compared with a traditional two-tiered network architecture (IoT-Cloud)?* Conventional security mechanisms were considering IoT devices and the Cloud, while current mechanisms consider existence of Fog devices in the middle with the purpose of increasing security, while providing reliability and timeliness.

RQ3. *How to collect network traffic and apply new rules on traffic isolation while keeping low overhead?* It is naïve to devise complex algorithms for IoT networks as they have resource limitations. It is important to propose simple yet efficient security algorithms to monitor network traffic in real-time, and then react to changes in a timely manner, while adding low overhead to the system.

RQ4. *How to verify the feasibility of the proposed algorithm in a real environment?* It is important to conduct real-world tests by applying the algorithm to the network, while varying network condition.

2 Related research topics

In this section, we briefly address some of the most relevant topics to the research area.

Security in IoT networks. The Internet of Things integrates various sensors, objects and smart nodes, capable of communicating through Internet connection [3]. IoT devices are able to deliver lightweight of data, accessing and authorizing cloud-based resources for collecting and extracting data. IoT nodes are widely used in different application domains, ranging from healthcare to transportation [5]. Many business opportunities have been created with IoT devices since there will be more closer interaction between the end users and manufacturers and service providers. Security issues, such as privacy of data, access control, secure communication and secure storage are becoming important challenges in IoT applications [25]. Rapid growth of IoT devices and applications have led to the deployment of several vulnerable and insecure nodes and networks [9]. Moreover, traditional IoT architectures with user-driven security architectures are of little use in object-driven IoT networks [1]. Thus, new techniques and procedures are required to reside in IoT networks. FIREWORK focuses on the security challenge of IoT networks by considering a different perspective on how

efficiently and timely detecting intrusions in the network and how to confront the identified attack.

Fog computing architecture. Fog/Edge computing is an architecture organized by the networking edge devices and clients to provide computing services for customers or applications, locating between networking central servers and end-users [4, 24]. In Fog computing, massive data generated by IoT devices can be processed at the network edge instead of transmitting to the centralized Cloud infrastructure in order to conserve more bandwidth and energy [16, 17]. Since Fog computing is organized in a distributed manner, it is possible to get faster response and better quality in comparison to Cloud computing [16]. Fog computing is more suitable to be integrated within the IoT network, while providing more efficient and secure services for large number of end users [4]. This paper considers Fog computing architecture for IoT network, and defines security threats and solutions within this novel architecture.

SDN controller and orchestration. Following the recent innovations brought about by the Cloud computing, current advances in communication infrastructures show an unprecedent central role of software-based solutions [19, 14, 8]. The concept of SDN decouples software-based network control and management planes from the hardware-based forwarding plane, turning traditional vendor locked-in infrastructures into communication platforms that are fully programmable via a standardized interface [11]. This interface provides a unified management and orchestration of end-to-end services across multiple domains. It is possible to separate the data plane and control plane in IoT networks, allowing the IoT controller to program the network with the aim of guaranteeing specific quality of services.

SDN orchestration often involves coordinating software actions with an SDN Controller, which can be built using open source technologies such as OpenDaylight [7]. The controller can be programmed to make automated decisions in case of network congestion, faults and security threats. SDN-based orchestration can use network protocols including OpenFlow [13] and IP-based networking. The most important element of SDN orchestration is the ability to monitor network security threats. For this reason, it is considered as one of the most promising growth areas of SDN networks. FIREWORK provides network orchestration component for network management in terms of security. This is a novel approach that has been neglected in IoT networks.

Security in Fog computing. Fog computing technology bridges the gap between the Cloud and IoT devices, while enabling enhanced security, decreased bandwidth, and reduced latency [4]. Fog is considered as a nontrivial extension of the Cloud, and thus it is inevitable that some security challenges will continue to persist [2]. Fog computing can introduce new security challenges due to its distinct characteristics such as mobility support. These challenges might impact the adaptation of Fog computing into the IoT network. On the other hand, Fog computing offers an ideal platform to address many security issues in the IoT. Fog nodes are represented as proxy nodes that provide enhanced security support that IoT nodes are unable to provide [20]. The research on security in Fog computing for IoT networks is still in its early stage, and thus, we are aiming to enhance this line of research by initiating novel ideas.

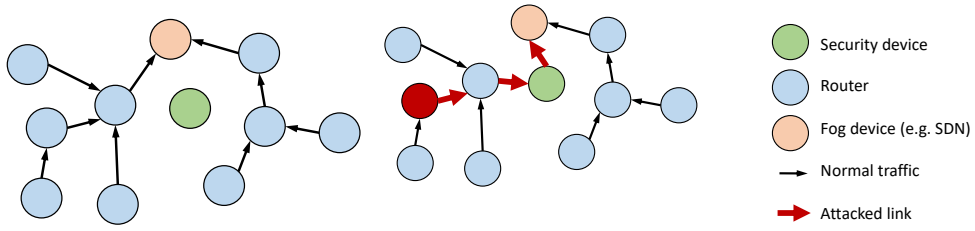

Fig. 2. Network monitoring in a Fog-based IoT network, (a) without security attach and (b) with security attack.

3 Fog-based security solution

The proposed Fog-based security solution, also known as FIREWORK, has two steps, where the first step stands for detecting attacks, and the second step focuses on recovering the network.

Network monitoring. It is crucial to devise and develop algorithms in the SDN controller in order to (i) detect attacks in the networks, and (ii) re-route traffic through security devices to confirm that devices (hosts and routers) are secure. There are various techniques for detecting attacks in the network. Security threats may involve increasing network traffic and degrading network performance. Keeping a history of network performance is a need to identify sudden increase or drop in network traffic. Upon detecting suspicious data packets, SDN controller is supposed to route network traffic through security devices. It is important to note that placement of security devices in the network will affect our approach in terms of timeliness.

Figure 2(a) depicts the case, where Fog devices detect normal traffic in all links. Apparently, the traffic from each device may vary from a low threshold (T_l) to a high threshold (T_h). However, there are some cases that there is a sudden change in one link, meaning that either there is an alarm message or a security threat. It is not trivial to distinguish between these situations, unless re-routing part of the traffic through a security device, which has been shown in Figure 2(b).

Traffic isolation. One of the main advantages of Fog nodes is the ability to maintain network traffic shunt system, where it is possible to isolate part of the network that has security threat. It is also possible to separate a special traffic from a part of the network, which is more suspicious. SDN controller provides the opportunity to allocate network slicing and dynamically moving traffic or eliminating traffic. Figure 3 shows two examples, where in the left figure all routers can communicate with each other, either directly or through the Fog device. However, upon detecting a security threat, Fog device abandons part of the network, eliminating network traffic spreading the network. This is the first step in network security before resolving the problem.

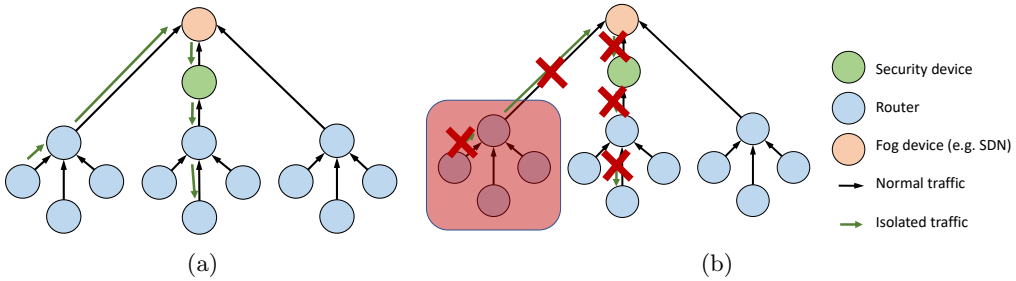

Fig. 3. Traffic isolation after detecting a security attack; (a) a network without traffic isolation, and (b) a network with traffic isolation.

ACKNOWLEDGMENT

The work presented in this paper is supported by the Swedish Foundation for Strategic Research via the project Future Factories in the Cloud (FiC), and by the Swedish Research Council (Vetenskapsrådet), through starting grant no. 2018-04582 via the project MobiFog: mobility management in Fog-assisted IoT networks, and from the Swedish Knowledge Foundation (KKS) throughout research profile Embedded Sensor System for Health (ESS-H), and the distributed environments E-care@home.

References

[1] Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F.: Internet of things security: A survey. Journal of Network and Computer Applications 88, 10–28 (2017)
[2] Alrawais, A., Alhothaily, A., Hu, C., Cheng, X.: Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing 21(2), 34–42 (2017)
[3] Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S.R., Rahmani, A.M., Liljeberg, P.: On the feasibility of attribute-based encryption on internet of things devices. IEEE Micro 36(6), 25–35 (2016)
[4] Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on Mobile cloud computing. pp. 13–16. ACM (2012)
[5] Chifor, B.C., Bica, I., Patriciu, V.V., Pop, F.: A security authorization scheme for smart home internet of things devices. Future Generation Computer Systems 86, 740–749 (2018)
[6] Computing, F.: the internet of things: Extend the cloud to where the things are. Cisco White Paper (2015)
[7] Consortium, O., et al.: Opendaylight (2013)
[8] Fotouhi, H., Vahabi, M., Ray, A., Björkman, M.: Sdn-tap: an sdn-based traffic aware protocol for wireless sensor networks. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom). pp. 1–6. IEEE (2016)
[9] Giaretta, A., Balasubramaniam, S., Conti, M.: Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks. IEEE Transactions on Information Forensics and Security 11(4), 665–676 (2016)

[10] Granjal, J., Monteiro, E., Silva, J.S.: A secure interconnection model for ipv6 enabled wireless sensor networks. In: Wireless Days (WD), 2010 IFIP. pp. 1–6. IEEE (2010)
[11] Hu, F., Hao, Q., Bao, K.: A survey on software-defined network and openflow: From concept to implementation. IEEE Communications Surveys & Tutorials 16(4), 2181–2206 (2014)
[12] Lam, B., Larose, C.: How did the internet of things allow the latest attack on the internet? (2016)
[13] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner, J.: Openflow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review 38(2), 69–74 (2008)
[14] Peterson, L., Al-Shabibi, A., Anshutz, T., Baker, S., Bavier, A., Das, S., Hart, J., Palukar, G., Snow, W.: Central office re-architected as a data center. IEEE Communications Magazine 54(10), 96–101 (2016)
[15] Poslad, S., Hamdi, M., Abie, H.: 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. pp. 373–378. ACM (2013)
[16] Pu, Q., Ananthanarayanan, G., Bodik, P., Kandula, S., Akella, A., Bahl, P., Stoica, I.: Low latency geo-distributed data analytics. In: ACM SIGCOMM Computer Communication Review. vol. 45, pp. 421–434. ACM (2015)
[17] Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: Vision and challenges. IEEE Internet of Things Journal 3(5), 637–646 (2016)
[18] Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in internet of things: The road ahead. Computer networks 76, 146–164 (2015)
[19] Soares, J., Gonçalves, C., Parreira, B., Tavares, P., Carapinha, J., Barraca, J.P., Aguiar, R.L., Sargento, S.: Toward a telco cloud environment for service functions. IEEE Communications Magazine 53(2), 98–106 (2015)
[20] Stojmenovic, I., Wen, S., Huang, X., Luan, H.: An overview of fog computing and its security issues. Concurrency and Computation: Practice and Experience 28(10), 2991–3005 (2016)
[21] Vahabi, M., Fotouhi, H., Björkman, M.: Network management in heterogeneous wireless sensor network applications. In: 2016 3rd Smart Cloud Networks & Systems (SCNS). pp. 1–6. IEEE (2016)
[22] Vaquero, L.M., Rodero-Merino, L.: Finding your way in the fog: Towards a comprehensive definition of fog computing. ACM SIGCOMM Computer Communication Review 44(5), 27–32 (2014)
[23] Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal 4(5), 1250–1258 (2017)
[24] Yi, S., Li, C., Li, Q.: A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 workshop on mobile big data. pp. 37–42. ACM (2015)
[25] Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C.: A survey of intrusion detection in internet of things. Journal of Network and Computer Applications 84, 25–37 (2017)
[26] Zhang, T.: Fog boosts capabilities to add more things securely to the internet. Cisco Blogs (2016)