Spam DIS Attack Against Routing Protocol in the Internet of Things

Cong Pu
Weisberg Division of Computer Science
Marshall University
Huntington, WV 25755, USA
puc@marshall.edu

***Abstract*—A rapidly growing number of various sensors, objects and smart devices that are capable of communicating with each other without human intervention are leading the emergence of Internet-of-Things (IoT) and its applications. As a major building block of IoT, Low Power and Lossy Network (LLN) that consists of a set of resource-constrained nodes in terms of communication, computation, memory, and energy plays an essential role in the realization of ubiquitous computing and communication paradigm. In order to provide both efficient and reliable communication and enable the integration of resource-constrained nodes into the Internet, a novel routing protocol for LLNs, also referred to as *RPL*, has been proposed. However, LLNs running with RPL are vulnerable to various Denial-of-Service (DoS) attacks because of inherent resource constraints, the lack of tamper resistance and security features of routing protocol. In this paper, we present and investigate a new type of DoS attack, called *spam DIS attack*, in swiftly burgeoning RPL-based LLNs. In spam DIS attack, the malicious node multicasts a large number of DODAG Information Solicitation (DIS) messages with different fictitious identities to cause the legitimate nodes to restart the Trickle algorithm and broadcast an excessive number of DODAG Information Object (DIO) messages, which drain down the energy resource of legitimate nodes, and finally make the legitimate nodes suffer from denial of service. We conduct extensive simulation experiments for performance evaluation of spam DIS attack and comparison with original RPL without adversary. The simulation results indicate that the spam DIS attack is an extremely severe DoS attack in RPL-based LLNs.**

***Index Terms*—Spam DIS Attack, Denial-of-Service, RPL, Low Power and Lossy Networks, Internet-of-Things**

I. Introduction

Smart devices or objects (later nodes) with the capability of communication and computation ranging from simple sensor nodes to sophisticated home appliances and smart phones are present everywhere around us, which is leading the emergence of pervasive and ubiquitous computing and Internet-of-Things (IoT). It has been predicated that the number of wireless connected devices for IoT applications will rise to 50 billion by the end of 2020 and global spending on the IoT will also rise to $1.7 trillion by 2020 [1]. As a major building block of IoT, Low Power and Lossy Network (LLN) comprised of thousands of embedded networking devices employs the open and standardized IPv6-based architecture to connect with the larger Internet, and paves the way to the realization of IoT applications. With the increasing demand of providing Internet (IPv6) connectivity to resource-constrained nodes and efficiently constructing reliable routes over lossy wireless links, the Internet Engineering Task Force (IETF) Working Group has proposed a novel routing protocol for low power and lossy networks, also referred to as *RPL* [2], to provide both efficient and reliable communication for IP smart object networks. For example, Cisco's Field Area Network (FAN) for smart grids (CG-Mesh) is designed based on the IPv6 architecture, which uses IEEE 802.15.4 at the PHY and MAC layer to form LLNs and employs RPL to provide end-to-end two-way communication to each smart metering endpoint [3].

Due to the harsh deployment environment and the lack of physical protection, however, nodes can be easily captured, tampered, or destroyed by an adversary. An open nature of shared wireless medium can also enable the adversary to overhear, duplicate, corrupt, or alter sensory data. In addition, RPL is not originally designed to consider the security requirements for malicious attacks, and security mechanism is optional to implement because it greatly affects the performance of resource-constrained devices [4], [5]. Thus, RPL-based LLNs are vulnerable to various Denial-of-Service (DoS) attacks that primarily target service availability [6].

In this paper, we present and investigate a new type of Denial-of-Service attack, called *spam DIS attack*, in RPL-based LLNs. In spam DIS attack, the malicious node multicasts a large number of DODAG Information Solicitation (DIS) messages with different fictitious identities to cause the legitimate nodes to restart the Trickle algorithm and broadcast an excessive number of DODAG Information Object (DIO) messages, which are the RPL messages necessary to build the routing topology. This drains down the energy resource of legitimate nodes, and finally causes the legitimate nodes to be unable to communicate and suffer from denial of service. The spam DIS attack primarily targets the vulnerability of DIO transmission mechanism in RPL by violating an implicit assumption, i.e., all legitimate nodes unhesitatingly and faithfully broadcast DIO message when they receive a DIS message without a Solicited Information option, or with a Solicited Information option and all matched predicates in the Solicited Information option. Our contribution is briefly summarized in the following:

- We present a new and severe DoS attack, called *spam DIS attack*, against RPL routing protocol in LLNs. This is the first in-depth work to investigate the performance impact of spam DIS attack in RPL-based LLNs.

978-1-5386-9223-3/19/$31.00 ©2019 IEEE

- We implement the original RPL without adversary for performance comparison. The original RPL without adversary is used as the lower bound of energy consumption and number of generated DIO messages, respectively.

We develop a customized discrete event-driven simulation framework by using OMNeT++ [7] and evaluate its performance impact through extensive simulation experiments in terms of energy consumption, node lifetime and number of generated DIO messages. The simulation results indicate that the spam DIS attack is an extremely severe DoS attack in RPL-based LLNs.

The rest of the paper is organized as follows. An overview of relevant work is provided in Section II. The basic RPL operations and its potential vulnerabilities are summarized and analyzed in Section III. The spam DIS attack and its performance impact evaluation with extensive simulation experiments are presented in Sections IV and V, respectively. Finally, concluding remarks is provided in Section VI.

II. Related Work

In this section, we categorize and analyze a variety of existing attacks and countermeasures in lower power and lossy networks and similar environments.

In the camouflage-based detection (CAM) [8], each node hides its current operational status and pretends not to monitor the forwarding operations of its adjacent nodes to detect the deep lurking malicious node in Energy Harvesting Motivated Networks (EHNets). A cooperative countermeasure (EYES) [9] is an extended version of the CAM, where each node periodically requests its adjacent nodes of a limited history of forwarding operations, and validates any prior uncertain forwarding operation to detect the forwarding misbehavior. In [10], an acknowledgment-based approach is proposed to detect stealthy collision attack in EHNets. A single checkpoint-assisted countermeasure (SCAD) [11] integrated with time-out and hop-by-hop retransmission techniques is proposed to detect the selective forwarding attack in Wireless Sensor Networks (WSNs), where single or multiple malicious nodes randomly or strategically drop any incoming packet. In [12], a DSR-based bait detection scheme incorporated with a digital signature technique is proposed to detect routing misbehaviors in Mobile Ad Hoc Networks (MANETs). [13] carries out a deep-dive into the main security mechanisms and their effects on the most popular protocols and standards used in WSN deployments, where potential security threats and existing countermeasures are discussed at each layer of WSN stack.

The security of lower power and lossy networks (LLNs) has been the subject of much research over the past few years along with the emergence of IoT. In [14], a rank attack that aims at the rank property in RPL and its performance impact are investigated in WSNs. In the Dodge-Jam [15], a light-weight anti-jamming technique suitable for LLN environments is proposed to address the stealthy jamming attacks with small overhead. The [16] investigates the DODAG Information Object suppression attack, which can severely degrade the routing service in RPL. In the CMD [17], each node monitors

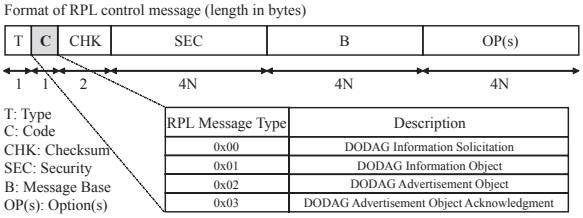

Fig. 1. The format of RPL control message. Here, the length is shown in byte.

the forwarding behaviors of the preferred parent node and observes the packet loss rate to detect the forwarding misbehavior of parent node in RPL-based LLNs. A dynamic threshold mechanism [18] is proposed to mitigate DAO inconsistency attack in LLNs running with RPL, where a malicious node intentionally drops the received data packet and replies the forwarding error packet to cause the parent node to discard valid downward routes in the routing table. The [19] identifies and investigates a new type of Denial-of-Service attack, called hatchetman attack, in LLNs, where a malicious node manipulates the source route header of the received packet, and then generates and sends the invalid packets with error route to legitimate nodes. The [20] proposes a heuristic-based detection against the suppression attack in multicast protocol for LLNs, where a malicious node multicasts a series of spoof data messages with continuous sequence numbers to prevent normal nodes from accepting valid data messages and cause them to delete cached data messages.

III. The RPL Routing Protocol

RPL [2] is a distance vector and source routing protocol that is designed to operate on IEEE 802.15.4 PHY and MAC layers, and represents a specific routing solution for low power and lossy networks with very limited resource in terms of energy, computation and bandwidth, turning them highly exposed to packet losses. To maintain the network state information, RPL organizes nodes as one or more Destination-Oriented Directed Acyclic Graphs (DODAGs), where DODAGs are differentiated by RPL Instance ID, DODAG ID, and DODAG Version Number. Each DODAG is associated with a set of normal nodes and one DODAG root, where the node providing a default route to the Internet acts as the DODAG root (i.e., gateway), and normal nodes are responsible for generating and forwarding data traffic to the DODAG root. In addition, RPL message is specified as a new type of ICMPv6 control message, and is composed of six fields: *Type*, *Code*, *Checksum*, *Security*, and a message body comprising a *Message Base* and a number of *Options*. Here, the structure of control message is depicted in Fig. 1, where the *Code* field identifies four types of control messages: DODAG Information Object (DIO), DODAG Information Solicitation (DIS), DODAG Destination Advertisement Object (DAO), and DODAG Destination Advertisement Object Ack (DAO-Ack).

The DODAG Information Object (DIO) message is issued by the DODAG root to construct a new DODAG and build upward routes directed from other nodes to the DODAG root. The DIO message carries the DODAG root's ID, the rank of

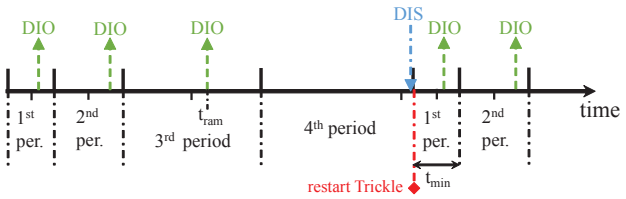

Fig. 2. Example of Trickle algorithm. Upward dashed arrows represent emitted DIO messages, and downward dash-dotted arrow represents received DIS message.

the DODAG root, and an Objective Function which describes the routing metrics and constraints. The piggybacked network information of DIO message allows a node to discover a RPL instance, learn its configuration parameters, build its parent list, and maintain the DODAG. Any node that receives the DIO message and is willing to join the DODAG should add the DIO message sender to its parent list, computes its own rank according to the piggybacked Objective Function, and passes on the DIO message with the updated rank information. Here, the rank is used to imply the node's position relative to other nodes with respect to the DODAG root. In the DODAG, nodes on top of the hierarchy receive smaller ranks than those in the bottom, and the smallest rank is assigned to the DODAG root. The node that has the smallest rank among all the nodes in the parent list is selected as the preferred parent node. After the DODAG is constructed, each node will be able to forward sensory data to the DODAG root by choosing its most preferred parent node as the next-hop forwarding node.

In order to reduce the energy consumption through minimizing the redundant DIO messages and dynamically adjusting the transmission rate, the emission of DIO messages are regulated by the Trickle algorithm [21], which is a density-aware local communication primitive with an underlying consistency model to guide the message transmissions. More specifically, the emission rate of DIO messages is dynamically adjusted according to the stability of routing information. If the piggybacked information in the received DIO message from adjacent node is consistent with currently stored routing information, then the emission rate is reduced. Otherwise, the emission rate is increased when inconsistent DIO message is received. *Additionally, a DODAG Information Solicitation (DIS) message from a new node that wishes to join the network also will be considered as inconsistent routing information.* In Trickle algorithm, as shown in Fig. 2, time is divided into periods of variable length. The transmission of DIO message is scheduled at a random time t_{ram} in the second half of each period. Until t_{ram}, the node listens to wireless channel for inconsistent routing information, e.g., DIS message from new node. At time t_{ram}, if the node does not receive DIS message, it broadcasts the scheduled DIO message. And then, the length of the next period is doubled, until a maximum length is reached. Otherwise, the current period is interrupted and the transmission of the scheduled DIO message is terminated, e.g., as it happens within the 4^{th} period in Fig. 2, the Trickle algorithm starts again from t_{min}.

To build downward routes from the DODAG root to other nodes, the node needs to issue a DODAG Destination Advertisement Object (DAO) control message to propagate reverse route information and record the nodes visited along the upward routes. After passing the DAO message to the DODAG root, a complete downward route between the DODAG root and the node is established. Finally, the DODAG root replies a DODAG Destination Advertisement Object Acknowledgment (DAO-Ack) message as a unicast packet to the source of DAO message as a response.

If a new node wants to join the existing network, it can request topology information from the neighbor nodes in the adjacent DODAGs by multicasting a DODAG Information Solicitation (DIS) control message. When a node receives a DIS message without a Solicited Information option, or with a Solicited Information option and all predicates matched in the Solicited Information option, it terminates the scheduled transmission of DIO message, and restarts the Trickle algorithm again from a period of a minimum length t_{min}. Here, the Solicited Information option is used for a node to request DIO messages from neighboring nodes. The Solicited Information option may specify a number of predicate criteria to be matched by a receiving node, which is used by the requester to limit the number of replies. However, the DIS transmission mechanism can be exploited by an adversary to attack the network as well. For example, the malicious node multicasts a large number of DIS messages with different fictitious identities to disrupt network protocol and interfere with on-going communication.

IV. The Spam DIS Attack

The basic idea of spam DIS attack is that the malicious node multicasts a large number of DODAG Information Solicitation (DIS) messages with different fictitious identities to cause the legitimate nodes to restart the Trickle algorithm and broadcast an excessive number of DODAG Information Object (DIO) messages, which quickly drain down the energy resource of legitimate nodes, and finally cause the legitimate nodes to be unable to communicate and suffer from denial of service in LLNs. In this paper, we assume that an adversary is able to capture and compromise legitimate node, gain access to all stored information including public and private keys, and reprogram it to behave maliciously. In addition, the malicious node may create the fictitious identities derived either from its own media access control (MAC) address or a randomly generated fake MAC address. Due to the constant size of MAC address (e.g., 48 bits), it is not guaranteed that every randomly generated fictitious identity is different from all real MAC addresses used in the network. However, the probability of generating a fake MAC address which is same as the existing address in the network will be extremely low and close to zero, because the 24-bit address space contains 2^{24} possible MAC addresses. Thus, we implicitly assume that the randomly generated fictitious identity does not exist in the network, and will be considered as new identity by legitimate nodes.

First, a simple way to launch spam DIS attack is to randomly generate a fictitious identity, and multicast a DIS message piggybacked with fictitious identity to all adjacent

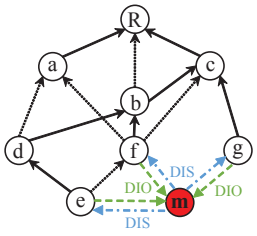

Fig. 3. A snapshot of the network, where a malicious node n_m multicasts the DIS message to probe for the DIO messages from adjacent nodes.

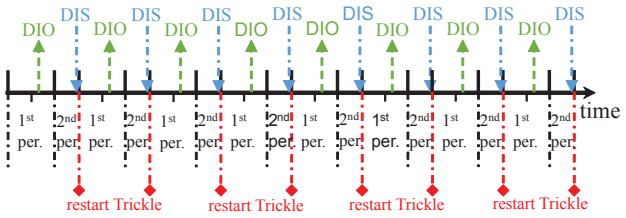

Fig. 4. The legitimate node n_f repeatedly restarts its Trickle algorithm after receiving multiple DIS messages from malicious node n_m.

nodes. When the legitimate node receives the DIS message piggybacked with new identity, it assumes that a new node wishes to join the network and probes for network configuration and other parameters through DIS message, which will be considered as inconsistent routing information. Thus, the legitimate node restarts the Trickle algorithm from the minimum period t_{min}, and then broadcasts a DIO message piggybacked with current network information at a random time in the second half of t_{min}. Let us illustrate the spam DIS attack by means of an example as shown in Fig. 3, where supposing that n_m is a malicious node. n_m multicasts a DIS message piggybacked with a randomly generated fictitious identity to all its neighbor nodes n_e, n_f, and n_g. When the neighbor node (e.g., n_f) receives the DIS message from n_m, it believes that a new node wishes to join the network and requests for current network information. Thus, n_f restarts the Trickle algorithm from t_{min}, and then broadcasts the DIO message piggybacked with current network information to n_m at a random time in the second half of t_{min}.

Second, if the malicious node generates multiple DIS messages piggybacked with different fictitious identities at a consistent rate, and then multicasts them to adjacent nodes, all receiving nodes will restart the Trickle algorithm from the beginning repeatedly and broadcast a large number of DIO messages. For example in Fig. 4, the malicious node n_m generates and multicasts multiple DIS messages with different identities to node n_f. Then, node n_f has to restart its Trickle algorithm from t_{min} repeatedly, and then broadcasts the DIO messages, which cause n_f to shorten the time interval of consecutive DIO messages. As a result, an excessive number of received DIS and broadcasted DIO messages significantly exhaust energy resource and communication bandwidth, and finally cause the legitimate node n_f to run out of its energy and suffer from denial of service.

V. Performance Evaluation

We conduct extensive simulation experiments using the OMNeT++ [7] to evaluate the performance impact of spam

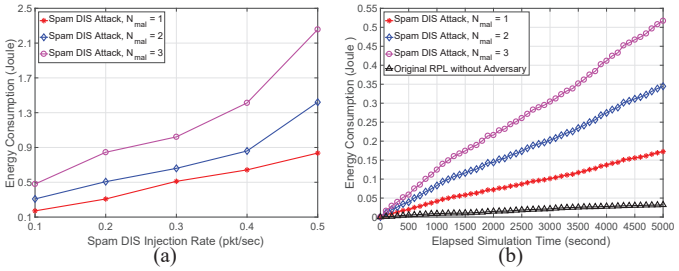

Fig. 5. The performance of energy consumption against spam DIS message injection rate and elapsed simulation time.

DIS attack. 30 nodes including a single DODAG root are uniformly distributed in a 100×100 m^2 square network area. The communication range of each node is 30 (m). The radio model simulates CC2420 with a normal data rate of 250 Kbps, and 802.15.4 MAC/PHY operates with a default configuration in the 2.4 GHz band [22]. Packet injection rate is set to 0.1 pkt/sec to emulate low data rate scenario. A set of malicious nodes are randomly located in the network. And the total simulation time is 5000 seconds, and each simulation scenario is repeated 5 times to obtain steady state performance metrics. In this paper, we measure the performance in terms of energy consumption, node lifetime, and number of generated DIO messages by changing key simulation parameters, including spam DIS message injection rate (r_{dis}) and number of malicious node (N_{mal}). We compare the performance impact of spam DIS attack with the original RPL without adversary.

First, the energy consumption is measured in terms of the number of received and broadcasted packets by changing spam DIS message injection rate and number of malicious nodes in Subfig. 5(a). Overall, the energy consumption of spam DIS attack increases as the spam DIS message injection rate increases. This is because the malicious node can generate and multicast more DIS packets to legitimate nodes with larger spam DIS message injection rate, the legitimate nodes will reply a large number of DIO messages accordingly. In other words, the legitimate nodes have to receive and broadcast an excessive number of control packets, thus, the larger energy consumption is observed. As the number of malicious nodes increases, the energy consumption increases significantly. Since more malicious nodes exist in the network and broadcast spam DIS messages, the legitimate nodes have to receive and broadcast more DIS and DIO messages respectively, and finally result in larger energy consumption.

Second, we measure the energy consumption against the elapsed simulation time by varying the number of malicious nodes in Subfig. 5(b). The RPL without adversary shows the lowest energy consumption than that of spam DIS attack, because the emission rate of DIO messages is dynamically adjusted and regulated by the Trickle algorithm to reduce the energy consumption through minimizing the redundant DIO messages, and less number of control packets are received and broadcasted. Thus, the lowest energy consumption is achieved by the RPL without adversary. As the number of malicious nodes N_{mal} increases, the energy consumption of spam DIS attack quickly increases along with the elapsed simulation time. Since more DIS messages are generated and broadcasted

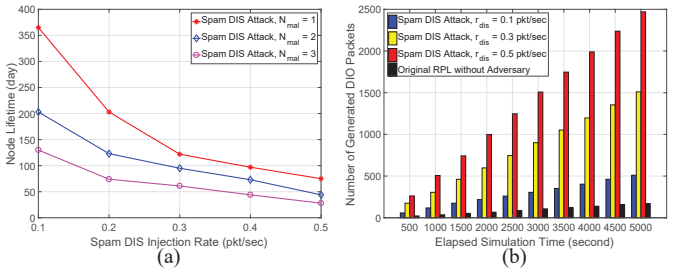

Fig. 6. The performance of node lifetime and number of generated DIO packets against spam DIS message injection rate and elapsed simulation time.

by more malicious nodes to probe for DIO messages from neighbor nodes, the legitimate nodes receive a larger number of DIS messages, and then broadcast excessive DIO messages, which consumes more energy.

Third, we measure the node lifetime with varying number of malicious nodes N_{mal} and spam DIS message injection rate in Subfig. 6(a). Here, we assume that each legitimate node is equipped with one standard AA battery (400 mAh and 1.5 V), and the legitimate node will die and be unable to communicate further when it runs out of the half of battery energy (e.g., 1080 Joule). And the malicious node has no energy constraints. As the spam DIS message injection rate increases, the overall node lifetime quickly decreases. This is because the legitimate node receives and broadcasts a large number of control packets, consumes a significant amount energy resource, and quickly runs out of the stored energy resource. With the number of malicious node $N_{mal} = 3$, the node lifetime is reduced from approximate 130 to 28 days as the spam DIS message injection rate increases. Due to the larger number of DIS messages generated by malicious nodes, the legitimate nodes have to respond by broadcasting more DIO messages, which consumes the limited energy quickly.

Fourth, the number of generated DIO messages are measured by changing spam DIS message injection rate r_{dis} in Subfig. 6(b). Under spam DIS attack, a larger number of DIO messages are generated compared to that of RPL without adversary. This is because the malicious nodes frequently broadcast DIS messages to probe for DIO messages from legitimate nodes. As the spam DIS message injection rate increases, the number of generated DIO messages significantly increases. On the other side, the least number of DIO messages is observed by the original RPL without adversary because Trickle algorithm is employed to minimize the redundant DIO messages in order to reduce the energy consumption.

VI. Concluding Remarks

In this paper, we investigate the spam DIS attack, which is a new and severe denial-of-service attack in RPL-based LLNs. We analyze the spam DIS attack and compare it with the original RPL without adversary. Extensive simulation results show that the spam DIS attack can significantly increase the energy consumption and decrease the node lifetime, which leads to denial of service. As a future work, we plan to propose a light-weight countermeasure to mitigate the spam DIS attack in RPL-based LLNs. For example, each intermediate node along the forwarding path can maintain a threshold to limit the rate of receiving messages from the same node within a time period. If the number of received messages exceeds the threshold, all further messages will be rejected. To see the full potential of the proposed countermeasure, we plan to develop a small-scale testbed for experimental study.

Acknowledgment

This research was supported by Startup grant in the Weisberg Division of Computer Science and 2018 John Marshall University Summer Scholars Awards at Marshall University.

References

[1] I. Yaqoob, E. Ahmed, I. Hashem, A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 10–16, 2017.

[2] T. Winter and P. Thubert, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *RFC Standard 6550*, March 2012.

[3] Cisco, *Connected Grid Networks for Smart Grid - Field Area Network*, http://www.cisco.com/web/strategy/energy/field area network.html.

[4] H. Kim, J. Ko, D. Culler, and J. Paek, "Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2502–2525, 2017.

[5] A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Schnwlder, "Addressing DODAG Inconsistency Attacks in RPL Networks," in *Proc. IEEE GIIS*, 2014, pp. 1–8.

[6] A. Nia and N. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, 2017.

[7] A. Varga, *OMNeT++*, 2014, http://www.omnetpp.org/.

[8] C. Pu and S. Lim, "Spy vs. Spy: Camouflage-based Active Detection in Energy Harvesting Motivated Networks," in *Proc. IEEE MILCOM*, 2015, pp. 903–908.

[9] C. Pu, S. Lim, B. Jung, and J. Chae, "EYES: Mitigating Forwarding Misbehavior in Energy Harvesting Motivated Networks," *Elsevier Computer Communications*, vol. 124, pp. 17–30, 2018.

[10] C. Pu, S. Lim, J. Byungkwan, and M. Manki, "Mitigating Stealthy Collision Attack in Energy Harvesting Motivated Networks," in *Proc. IEEE MILCOM*, 2017, pp. 575–580.

[11] C. Pu and S. Lim, "A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation," *IEEE Systems Journal*, vol. 12, pp. 834–842, 2016.

[12] C. Pu, S. Lim, C. Jinseok, and J. Byungkwan, "Active Detection in Mitigating Routing Misbehavior for MANETs," *Wireless Network (2017)*, https://doi.org/10.1007/s11276-017-1621-z.

[13] I. Tomić and J. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, 2017.

[14] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks," *IEEE Sensors J.*, vol. 11, no. 10, pp. 3685–3692, 2013.

[15] J. Heo, J. Kim, S. Bahk, and J. Paek, "Dodge-Jam: Anti-Jamming Technique for Low-Power and Lossy Wireless Networks," in *Proc. IEEE SECON*, 2017, pp. 1–9.

[16] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, "DIO Suppression Attack Against Routing in the Internet of Things," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2524 – 2527, 2017.

[17] C. Pu and S. Hajjar, "Mitigating Forwarding Misbehaviors in RPL-based Low Power and Lossy Networks," in *Proc. IEEE CCNC*, 2018, pp. 1–6.

[18] C. Pu, "Mitigating DAO Inconsistency Attack in RPL-based Low Power and Lossy Networks," in *Proc. IEEE CCWC*, 2018, pp. 570–574.

[19] C. Pu and T. Song, "Hatchetman Attack: A Denial of Service Attack Against Routing in Low Power and Lossy Networks," in *Proc. IEEE CSCloud*, 2018, pp. 12–17.

[20] C. Pu, X. Zhou, and S. Lim, "Mitigating Suppression Attack in Multicast Protocol for Low Power and Lossy Networks," in *Proc. IEEE LCN*, October 2018.

[21] P. Levis and T. Clausen, "The Trickle Algorithm," *RFC Standard 6206*, March 2011.

[22] A. Boulis, *Castalia*, 2014, http://castalia.forge.nicta.com.au.