Mitigating DAO Inconsistency Attack in RPL-based Low Power and Lossy Networks

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

***Abstract*—Due to the shared medium and the lack of physical protection, RPL-based low power and lossy networks (LLNs) are vulnerable to various attacks. Instinctive resources constraint also prevent devices from deploying expensive cryptography and enabling secure operation modes. In this paper, we propose a dynamic threshold mechanism, called *DTM*, to mitigate DAO inconsistency attack in RPL-based LLNs, 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. In the DTM, each parent node dynamically adjusts the threshold of accepting forwarding error packets within a time period based on the number of received forwarding error packets as well as the estimated normal forwarding error rate to counter DAO inconsistency attack. Simulation results indicate that the proposed scheme can provide higher packet delivery ratio but lower energy consumption compared to the fixed threshold scheme.**

***Index Terms*—Forwarding misbehavior, DAO inconsistency attack, RPL, low power and lossy networks.**

I. Introduction

The pervasive presence of a variety of things and objects being connected to the Internet are realizing the idea of the Internet of Things (IoT). To share information and coordinate decisions, the IoT enables a myriad of multi-scale sensors and devices (later nodes) to be seamlessly blended and communicate with each other [1]. As a major building block of rapidly emerging IoT, low power and lossy networks (LLNs) are playing an important role in achieving ubiquitous and pervasive computing. However, due to the shared wireless medium, resources constraint, and the lack of physical protection, LLNs are indeed vulnerable to various attacks [2]. As transmitted data become sensitive, the development of countermeasures to potential attacks are extremely critical and challenging for secure and reliable communication.

One potential attack is the DAO inconsistency attack [3], where a malicious node intentionally drops the received data packet and sets the *Forwarding-Error* flag in the packet option header to create the forwarding error packet, and then replies the forwarding error packet to cause the parent node to discard valid downward routes in the routing table. Since the downward route to destination node is removed from routing table, the parent node of malicious node has to reply the forwarding error packet to its parent node when it receives the data packet designated to the same destination node. As a result, all the ancestors of malicious node along the downward route will receive and reply a significant number of forwarding error packets, which significantly increases communication overhead and energy consumption, and finally leads to denial of service in RPL-based LLNs. The RPL standard [4] proposes to use a fixed threshold scheme to counter DAO inconsistency attack. Specifically, once a parent node receives a certain number of forwarding error packets from its child node within a time period (e.g., one hour), it will reject all further forwarding error packets from the child node. The RPL standard suggests a value of 20 for the threshold to limit the rate of accepting forwarding error packets and discarding downward routes in the routing table. However, the RPL standard does not provide any explanation why this value is recommended.

In this paper, we propose a dynamic threshold mechanism against DAO inconsistency attack in RPL-based LLNs, where each parent node dynamically adjusts the threshold of accepting forwarding error packets within a time period based on the number of received forwarding error packets as well as the estimated normal forwarding error rate. Our major contribution is briefly summarized in twofold:

- We analyze the DAO inconsistency attack in RPL-based LLNs to obtain a better understanding of the attack scenario and impact. To the best of our knowledge, this is the first in-depth attempt to investigate the performance impact of DAO inconsistency attack.
- We propose a dynamic threshold mechanism, called *DTM*, to efficiently mitigate the DAO inconsistency attack and finally purge the malicious node from the network.

We develop a customized discrete event-driven simulation framework by using OMNeT++ [5] to conduct the performance evaluation study in terms of packet delivery ratio, energy consumption, and the number of generated, received, and rejected error packets. The simulation results show a viable approach to mitigate DAO inconsistency attack in RPL-based LLNs.

The rest of paper is organized as follows. An overview of relevant work is presented in Section II. The basic RPL operations and its potential vulnerabilities are summarized and analyzed in Section III. The system and adversarial models, and the proposed scheme are presented in Section IV. Section V is devoted to extensive simulation experiments and analysis. Finally, concluding remarks are provided in Section VI.

978-1-5386-4649-6/18/$31.00 ©2018 IEEE

II. Related Work

While the security study of LLNs is burgeoning, a significant amount of research has been undertaken in the study of security issues in similar networks. In [6], each node maintains a reputation table with adaptive detection threshold to evaluate the forwarding behaviors of its adjacent nodes in wireless sensor networks (WSNs). Various countermeasures against potential forwarding misbehaviors in energy harvesting motivated networks have been investigated in [7], [8]. The [9] proposes an inducement-based detection scheme based on dynamic source routing to detect routing misbehaviors in mobile ad hoc networks. In the SCAD [10], a light-weight countermeasure to selective forwarding attack is proposed by deploying a single checkpoint node integrated with the timeout and hop-by-hop retransmission techniques.

With the emergence of IoT, intensive research efforts have been made to investigate secure communication in RPL-based LLNs. In [11], a rank attack that aims at the rank property in RPL and its performance impact are investigated in WSNs, where the adversary can compromise the rank rule to downgrade the RPL performance. The CMD [12] proposes a monitor-based approach to mitigate the forwarding misbehaviors in LLNs, where each node monitors the forwarding behaviors of the preferred parent node to observe the packet loss rate, compares the observation result with the collected packet loss rate from one-hop neighbor nodes, and detects the forwarding misbehaviors of the preferred parent node. In the VeRA [13], a version number and rank authentication security scheme based on one-way hash chains are proposed to secure communication in RPL-based LLNs. The [14] proposes two complementary and lightweight defense mechanisms to counter fragmentation attack in the adaptation layer of 6LoWPAN. The [15] analyzes the security capability of IEEE 802.15.4 MAC protocol as well as the limitations thereof in the context of IoT. The [16] designs and implements an intrusion detection system that can be modified to employ RPL routing protocol in neighborhood area network. A security threat analysis of RPL has been performed in [17], where potential security issues and fundamental countermeasures are presented.

III. The RPL Routing Protocol and DAO Inconsistency Attack

In this section, we first present the RPL routing protocol and then introduce the DAO inconsistency attack with a preliminary result.

A. The RPL Routing Protocol

RPL [4] is a novel distance vector and source routing protocol designed for low power and lossy networks operating on IEEE 802.15.4 PHY and MAC layers. The basic idea of RPL is to construct one or more Destination-Oriented Directed Acyclic Graphs (DODAGs) to maintain the network state information, where DODAGs are differentiated by RPL Instance ID, DODAG ID, and DODAG Version Number. Each DODAG is associated with a set of nodes and one DODAG root (i.e., base station or gateway node), where nodes can generate and forward data traffic and DODAG root is responsible for collecting the data measured by other nodes, controlling these nodes, and bridging the DODAG with IPv6 networks.

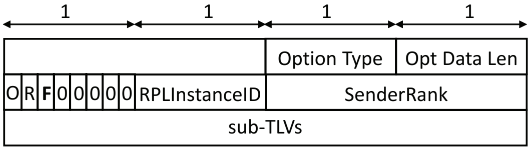


Fig. 1. The format of RPL packet option header, where **F** is the *Forwarding-Error* flag. Here, the length is shown in byte.

RPL relies on four types of control messages to establish and manage the network topology and routing information: DAG Information Object (DIO), DAG Information Solicitation (DIS), Destination Advertisement Object (DAO), and Destination Advertisement Object Ack (DAO-Ack). In order to construct a DODAG and build upward routes directed from other nodes to the DODAG root, the DODAG root will issue a DIO control message, which includes the DODAG root's ID, the rank of the DODAG root, and an Objective Function which describes the routing metrics and constraints. Any node that receives the DIO message and is willing to join the DODAG should add the DIO message sender to its parent list, compute its own rank according to the piggybacked Objective Function, and pass 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, and the rank of nodes along any upward route to the DODAG root should be monotonically decreasing to avoid any routing loop. If a new node wants to join the existing network, it can request topology information from the neighbor nodes in the adjacent DODAGs by broadcasting a DIS control message. To build downward routes from the DODAG root to other nodes, the destination node needs to issue a 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 destination node is established. Finally, the DODAG root replies a DAO-Ack message as a unicast packet to the source of DAO message.

B. DAO Inconsistency Attack

In storing mode, each node can quickly learn the routes of its descendants by aggressively caching the piggybacked downward route information of received DAO messages in its routing table. In this way, each intermediate node is able to record all of its descendants in its routing table with the next-hop node ID indicating the direction towards which the descendant node can be reached. In order to clean up stale downward routes from routing table, RPL employs the packet option header that contains a *Forwarding-Error* flag. The Forwarding-Error flag indicates that the node cannot forward the received data packet further towards the destination node based on the cached downward route in the routing table. If a parent node receives the forwarding error packet that has Forwarding-Error flag set from its child node corresponding to

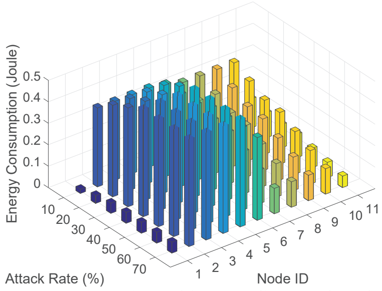


Fig. 2. The energy consumption of intermediate nodes along the downward route against attack rate. Here, node n_1 and n_6 is the DODAG root and malicious node, respectively.

previously forwarded data packet, the parent node removes the cached downward route designated to the destination node via this child node from routing table. Normally, the RPL packet option header is used to improve reliability of RPL. However, it can be used by a malicious node to attack the network as well. For example, a malicious node drops the received data packet and sets the Forwarding-Error flag in the packet option header to create the forwarding error packet, and then replies the forwarding error packet to cause the parent node to discard valid downward routes in the routing table. Here, the format of RPL packet option header is shown in Fig. 1.

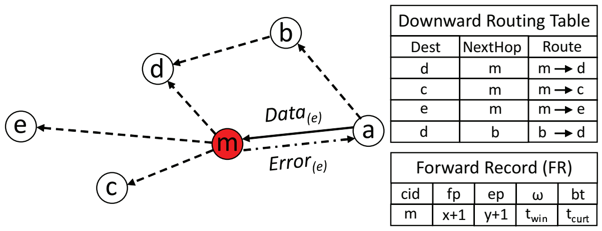
In Fig. 2, we measure the energy consumption of each node located along the downward route against attack rate, where node n_1 and n_6 is the DODAG root and malicious node, respectively. In this paper, attack rate is the probability that the malicious node intentionally sets Forwarding-Error flag and replies the forwarding error packet to parent node. As the attack rate increases in Fig. 2, the energy consumption of each node that is located prior to the malicious node along the downward route increases. This is because the malicious node frequently replies the forwarding error packets to cause the parent node to discard valid downward routes in the routing table. When the parent node of malicious node receives the data packet designated to the same destination node again, it has to reply the forwarding error packet to its parent node since the downward route to the destination node has been removed from routing table. As a result, all the ancestors of malicious node along the downward route (e.g., n_2, n_3, n_4, and n_5) will receive and reply a large number of forwarding error packets, which increase energy consumption significantly. When the attack rate reaches to 40%, the energy consumption is increasing slightly. This is because RPL uses the fixed threshold (e.g., 20 forwarding error packets per hour) to limit the rate of accepting forwarding error packets and discarding downward routes in the routing table.

IV. The Proposed Countermeasure

In this section, we first present the system and adversarial models, and then propose the dynamic threshold mechanism to mitigate DAO inconsistency attack in RPL-based LLNs.

A. System and Adversary Models

We consider a low power and lossy network running with RPL, where a set of resources-constrained nodes and one DODAG root communicate directly or indirectly through lossy links with high packet error rate and link outages. Each node is uniquely identified by a node ID, e.g., an Internet Protocol (IP) address. For simplicity, we assume that the RPL only maintains one DODAG structure rooted at the DODAG root in this paper. An adversary is able to capture and compromise a legitimate node, gain access to all stored information including public and private keys, and reprogram it to behave maliciously [18]. The primary goal of the adversary is to disrupt routing protocol and interfere with on-going communication. In this paper, we focus on the adversarial scenarios that cannot be detected by digital signature and cryptographic techniques. We do not consider cryptographic primitives.



Downward Routing Table		
Dest	NextHop	Route
d	m	m → d
c	m	m → c
e	m	m → e
d	b	b → d

Forward Record (FR)				
cid	fp	ep	ω	bt
m	x+1	y+1	t_{win}	t_{curt}

Fig. 3. A snapshot of the network, where a malicious node is marked as red.

B. DTM: Dynamic Threshold Mechanism

The basic idea of *DTM* is that each parent node dynamically adjusts the threshold of accepting forwarding error packets within a time period based on the number of received forwarding error packets as well as the estimated normal forwarding error rate to limit the rate of discarding valid downward routes in the routing table.

First, each node maintains a forwarding record, *FR*, to store the historical statistics of forwarding operations to its child nodes, where the *FR* consists of five components: child node' id (*cid*), the number of forwarded data packets (*fp*), the number of received forwarding error packets (*ep*), record window (ω), and the beginning timestamp of record window (*bt*). For example in Fig. 3, suppose a node n_a forwards a data packet designated to destination node n_e via its child node n_m based on the cached downward route in the routing table, thus n_a increases $FR_a[m].fp$ by one. However, if the malicious node n_m drops the received data packet and replies a forwarding error packet to n_a, n_a increases $FR_a[m].ep$ by one, and then removes the cached downward route designated to destination node n_e via n_m from routing table. Here, suppose that x and y are previous value stored in *fp* and *ep*, respectively.

Second, we propose a dynamic threshold mechanism to determine the threshold and limit the rate of accepting forwarding error packets and discarding downward routes in the routing table. In this paper, λ_{error} is the dynamic threshold value and updated by the low-pass filter with a filter gain constant α.

$$\lambda_{error} = \alpha \cdot \lambda_{ferr}^{m} + (1 - \alpha) \cdot \lambda_{ferr}^{Avg} \tag{1}$$

Here, λ_{ferr}^{m} and λ_{ferr}^{Avg} is the threshold calculated based on the number of received forwarding error packets from n_m and the estimated forwarding error rate of all other child nodes, respectively. λ_{ferr}^{m} is expressed as

$$\lambda_{ferr}^{m} = \varphi + \frac{20 - \varphi}{e} \cdot e^{1-\gamma} \tag{2}$$

```
Notations:
• $pkt[seq, des, type]$: A packet with a sequence number, $seq$, destination node, $des$, and packet type, $type$. Here, $type$ is Data, Error or Isolate.
• $RT_s$, $RT_s[d]$ and $FE_{flag}$: Downward routing table of $n_s$, child node ID (or next-hop ID) towards the destination node $n_d$ in $RT_s$, and Forwarding-Error flag in packet option header.
• $FR$, $fp$, $ep$, $bt$, $\omega$, $\lambda_{error}$, $d_{mis}$, $\eta$: Defined before.
Algorithm:
◇ When a normal node $n_s$ receives a data packet, $pkt[seq, d, Data]$, designated to destination node $n_d$:
    Search the cached downward route to $n_d$ from $RT_s$;
    Forward $pkt[seq, d, Data]$ to $RT_s[d]$; $FR_s[RT_s[d]].fp$ += 1;
◇ When a malicious node $n_m$ receives a data packet, $pkt[seq, d, Data]$, designated to destination node $n_d$ from node $n_s$:
    Drop $pkt[seq, d, Data]$;
    Set $FE_{flag}$ in $pkt[seq, d, Error]$;
    Reply $pkt[seq, d, Error]$ back to $n_s$;
◇ When a normal node $n_s$ receives a forwarding error packet, $pkt[seq, d, Error]$, from its child node $n_m$:
    if $FR_s[m].ep > \lambda_{error}$;
        Reject $pkt[seq, d, Error]$;
    else
        Remove the cached downward route to $n_d$ via $n_m$ in $RT_s$;
        $FR_s[m].ep$ += 1;
        Calculate $\lambda_{error}$; /* Eq. 4 */
◇ When record window $\omega$ ends at node $n_s$:
    if $FR_s[m].ep > \lambda_{error}$;
        $d_{mis}$ += 1;
    if $d_{mis} > \eta$;
        Broadcast $pkt[seq, m, Isolate]$;
    Reset $ep$, $fp$, and $bt$;
```

Fig. 4. The pseudo code of the proposed DTM.

where $\gamma = \frac{ep}{fp}$, and φ is a system parameter. λ_{ferr}^{Avg} is expressed as

$$\lambda_{ferr}^{Avg} = \varphi + \frac{20 - \varphi}{e} \cdot e^{1-\delta} \tag{3}$$

where $\delta = \frac{\sum_{i=cid}^{N, m \notin N} \frac{ep_i}{fp_i}}{N}$, and N is the set of child nodes. Thus, the dynamic threshold is expressed as

$$\lambda_{error} = \varphi + \alpha \cdot \frac{20 - \varphi}{e} \cdot e^{1-\gamma} + (1 - \alpha) \cdot \frac{20 - \varphi}{e} \cdot e^{1-\delta} \tag{4}$$

Unlike the fixed threshold, λ_{error} is dynamically adjusted based on attack patterns and varying network conditions. If a malicious node frequently replies forwarding error packets to its parent node, the λ_{error} quickly drops and all further forwarding error packets from this child node that exceeds λ_{error} will be rejected. In the absence of attack, λ_{error} can also be maintained at a high level.

Third, when the record window ω ends, each parent node compares the number of received forwarding error packets *ep* from its child node with the calculated threshold λ_{error}. If *ep* is larger than λ_{error}, the child node is suspected as malicious node and the number of detected forwarding misbehavior (d_{mis}) is increased by one. When the number of detected forwarding misbehaviors of the suspected node reaches a threshold (η), the parent node broadcasts an *Isolate* packet to its one-hop neighbor nodes to prevent the suspected node from involving any forwarding operation. Major operations of the *DTM* are summarized in Fig. 4.

V. Performance Evaluation

We conduct extensive simulation experiments using OMNeT++ [5] to evaluate the performance of proposed scheme in RPL-based LLNs. 50 nodes are uniformly distributed in a 150×150 m^2 square network area, where a single DODAG root is deployed. 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 [19]. The channel error rate (r_{cer}) is 10%. To emulate low packet rate scenario, packet injection rate is set to 0.1 pkt/sec. A set of malicious nodes are randomly located in the network. And the total simulation time is 50000 seconds. In this paper, we measure the performance in terms of packet delivery ratio, energy consumption, and the number of generated, received, and rejected error packets by changing key simulation parameter, attack rate (r_{akt}). For performance comparison, we compare the proposed scheme with the RPL without adversary and RPL under DAO inconsistency attack.

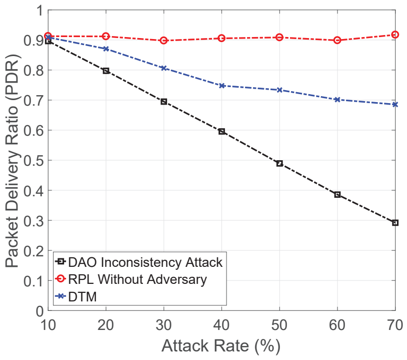


Fig. 5. The performance of packet delivery ratio against attack rate.

First, we measure the packet delivery ratio by varying attack rate (r_{akt}) in Fig. 5, where no adversary case is considered as the performance upper bound of packet delivery ratio. As shown in Fig. 5, the RPL without adversary achieves the highest PDR (about 90%), this is because every node cooperatively and faithfully forwards the received data packets to the destination nodes. However, due to bad channel quality (r_{cer} = 10%), a few number of data packets (approximate 10%) could get lost. The PDR under DAO inconsistency attack quickly decreases as the attack rate increases, because the malicious nodes can frequently drop the received data packets and reply the forwarding error packets to its parent node, which cause the parent node to discard the valid downward routes in the routing table. The DTM shows higher and lower PDR than that of DAO inconsistency attack and RPL without adversary, respectively. This is because the DTM can not only dynamically adjust the threshold to limit the rate of accepting forwarding error packets and discarding valid downward routes in the routing table, but also can detect the forwarding misbehaviors of malicious nodes and purge them from network. Thus, more number of data packets can be delivered to the destination nodes.

Second, we measure the energy consumption based on the number of forwarded and received packet [20] by varying attack rate (r_{akt}) in Fig. 6. The RPL without adversary provides the lowest energy consumption, because each node cooperatively and faithfully forwards the received data packets

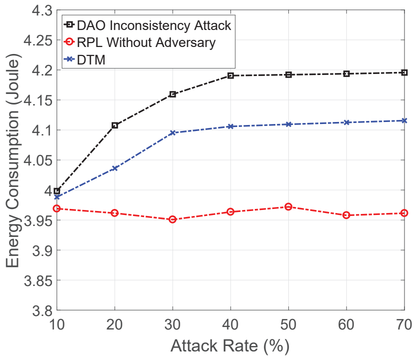
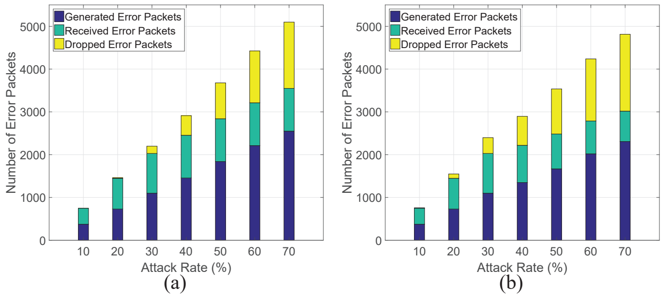


Fig. 6. The performance of energy consumption against attack rate.



(a)

(b)

Fig. 7. The performance of the number of generated, received, and rejected error packets against attack rate.

and the number of received and forwarded control packets will not change greatly. The DAO inconsistency attack shows the higher energy consumption than that of DTM, this is because the DTM can dynamically adjust the threshold to limit the rate of accepting forwarding error packets. Thus, less number of valid downward routes will be discarded in the routing table, and less number of DAO control packets are issued by destination nodes to build new downward routes. As the attack rate increases from 10% to 40%, the energy consumption of DAO inconsistency attack and DTM reach to 4.19 and 4.11 Joule, respectively. This is because the number of forwarding error packets has not reached the threshold, more forwarding error packets are accepted and more valid downward routes will be discarded in the routing table. As the attack rate continues to increase from 40%, the energy consumption of DAO inconsistency attack and DTM increase slightly because extra forwarding error packets are rejected.

Third, we measure the number of generated, received, and rejected error packets by varying attack rate (r_{akt}) in Fig. 7. More number of error packets are rejected by the DTM compared to that of DAO inconsistency attack, this is because the DTM can dynamically adjust the threshold to limit the rate of accepting forwarding error packets under different attack rates and varying network conditions. In addition, less number of forwarding error packets are accepted by the DTM as the attack rate increases.

VI. Conclusion

In this paper, we propose a countermeasure against DAO inconsistency attack in RPL-based LLNs. First, the DAO inconsistency attack and its performance impact are investigated with a preliminary result. Then, a dynamic threshold mechanism, called *DTM*, is proposed to efficiently mitigate DAO inconsistency attack. Extensive simulation results indicate that the proposed approach achieves better performance, not only improving packet delivery ratio, but also reducing energy consumption and communication overhead compared to the fixed threshold approach.

Acknowledgment

This research was supported by Startup grant in the Weisberg Division of Computer Science at Marshall University.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] 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.*, Sep 2017.

[3] J. Hui, “The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams,” *RFC Standard 6553*, March 2012.

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

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

[6] J. Ren, Y. Zhang, K. Zhang, and X. Shen, “Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks,” *IEEE Trans. on Wireless Commun.*, vol. 15, no. 5, pp. 3718–3731, 2016.

[7] 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.

[8] 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.

[9] C. Pu, S. Lim, C. Jinseok, and J. Byungkwan, “Active Detection in Mitigating Routing Misbehavior for MANETs,” *Wireless Networks, Springer*, Accepted, Nov 2017.

[10] C. Pu and S. Lim, “A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation,” *IEEE Systems Journal*, pp. 1–9, 2016.

[11] 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.

[12] C. Pu and S. Hajjar, “Mitigating Forwarding Misbehaviors in RPL-based Low Power and Lossy Networks,” in *Proc. IEEE CCNC*, Jan 2018.

[13] A. Dvir, T. Holczer, and L. Buttyan, “VeRA-Version Number and Rank Authentication in RPL,” in *Proc. IEEE MASS*, 2011, pp. 709–714.

[14] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, “6LoWPAN Fragmentation Attacks and Mitigation Mechanisms,” in *Proc. ACM WiSec*, 2013, pp. 55–66.

[15] S. M. Sajjad and M. Yousaf, “Security analysis of IEEE 802.15. 4 MAC in the context of Internet of Things (IoT),” in *Proc. IEEE CIACS*, 2014, pp. 9–14.

[16] N. Beigi-Mohammadi, J. Misic, H. Khazaei, and V. B. Misic, “An Intrusion Detection System for Smart Grid Neighborhood Area Network,” in *Proc. IEEE ICC*, 2014, pp. 4125–4130.

[17] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, “A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs),” *RFC Standard 7416*, January 2015.

[18] J. Kim and G. Tsudik, “SRDP: Secure route discovery for dynamic source routing in MANETs,” *Ad Hoc Networks*, vol. 7, no. 6, pp. 1097–1109, 2009.

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

[20] X. Tang and J. Xu, “Extending Network Lifetime for Precision-Constrained Data Aggregation in Wireless Sensor Networks,” in *Proc. IEEE INFOCOM*, 2006, pp. 1–12.