Energy Depletion Attack Against Routing Protocol in the Internet of Things

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

***Abstract*—Low power and lossy networks (LLNs) are undeniably vulnerable to various Denial-of-Service (DoS) attacks due to the shared wireless medium, the lack of physical protection, and instinctive resource constraints. In this paper, we propose a misbehavior-aware threshold detection scheme, called *MAD*, against energy depletion attack in RPL-based LLNs, where a malicious node intentionally generates and sends a large number of packets to legitimate nodes to excessively consume the energy resource of intermediate nodes located along the forwarding paths, and finally makes the resource-constrained network suffer from denial of service. In the *MAD*, each node maintains a count of the number of received packets from its child node within a specific time window, and then compares the count with a dynamically calculated threshold to detect potential malicious node. We conduct extensive simulation experiments for performance evaluation and comparison with the original RPL with and without adversary, respectively. The simulation results show that the proposed scheme is a viable approach against energy depletion attack in RPL-based LLNs.**

***Index Terms*—Energy depletion attack, Denial-of-Service, RPL, low power and lossy networks, Internet-of-Things**

I. Introduction

A rapidly growing pervasiveness and ubiquity of small and cheap computing devices (later nodes) endowed with sensing and communicating capabilities is paving the way to the realization of Internet-of-Things (IoT). As a major building block of emerging IoT, low power and lossy networks (LLNs) comprised of resource-constrained nodes with the limited communication, computation, memory and energy are playing an indispensable role in creating an ubiquitous computing and communication environment. However, due to the shared wireless medium, and the lack of resource, physical protection and security requirements of RPL routing protocol, RPL-based LLNs are vulnerable to various Denial-of-Service attacks [1].

In this paper, we investigate an energy depletion attack and propose its countermeasure in RPL-based LLNs, where a legitimate node compromised by an adversary intentionally generates and sends a large number of packets to legitimate nodes to excessively consume the energy resource of intermediate nodes located along the forwarding paths, and finally causes denial of service in resource-constrained networks. First, we present and analyze the energy depletion attack with a preliminary result. This is the first in-depth work to investigate the performance impact of energy depletion attack in RPL-based LLNs. Second, we propose a misbehavior-aware threshold detection scheme, called *MAD*, to efficiently detect and mitigate the energy depletion attack in RPL-based LLNs. Finally, we develop a customized discrete event-driven simulation framework by using OMNeT++ [2] and evaluate its performance through extensive simulation experiments. The simulation results indicate that the proposed countermeasure is a viable approach against energy depletion attack.

II. Related Work

In [3], a camouflage-based detection (CAM) scheme is proposed to detect the forwarding misbehavior in energy harvesting motivated networks (EHNets). The EYES [4] is an extended version of the CAM. [5] proposes an acknowledgment-based approach against stealthy collision attack in EHNets. In [6], a single checkpoint-assisted approach integrated with timeout and hop-by-hop retransmission techniques is proposed to detect the selective forwarding attack in wireless sensor networks. In [7], a DSR-based bait detection scheme incorporated with a digital signature technique is proposed to detect routing misbehaviors in mobile ad hoc networks. [8] examines security vulnerabilities and threats imposed by the inherent open nature of wireless communications, and presents a variety of efficient defense mechanisms for improving the wireless network security among different layers. In [9], DIO suppression attack is investigated in IPv6-based wireless sensor and actuator networks. In [10], a dynamic threshold mechanism is proposed to mitigate DAO inconsistency attack in RPL-based LLNs. In the CMD [11], each node monitors 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. In [12], a new type of Denial-of-Service attack, called hatchetman attack, is identified and investigated in RPL-based LLNs. The [13] and [14] propose a heuristic-based detection against the suppression attack in multicast protocol for LLNs. The history of research efforts in RPL-based LLNs and future research directions on which RPL should evolve have been reviewed and discussed in [15].

III. The RPL Routing Protocol and Energy Depletion Attack

A. The RPL Routing Protocol

RPL [16] is a novel distance vector and source routing protocol designed for low power and lossy networks operating

978-1-5386-5553-5/19/$31.00 ©2019 IEEE

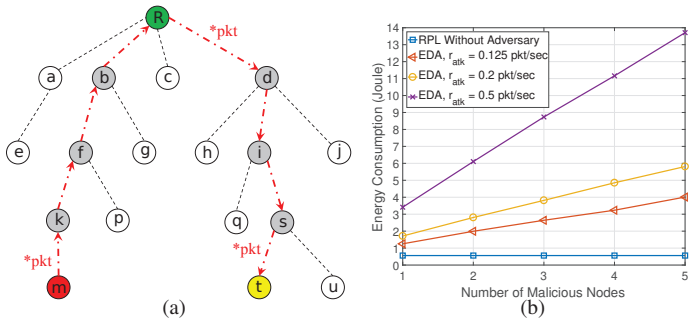


Fig. 1. An example of energy depletion attack and the performance impact of energy depletion attack: (a) A malicious node n_m intentionally generates and sends a large number of packets $*pkt$ to a destination node n_t. Here, green node is the DODAG root, and red dash-dotted lines represent forwarding path. (b) The energy consumption against number of malicious nodes and attack rate (r_{atk}). Here, a 200×200 (m^2) network area is considered, where normal packet injection rate is 0.1 pkt/sec.

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, 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 (i.e., base station), where normal nodes can generate and forward data traffic and DODAG root is responsible for collecting the data measured by normal nodes, controlling these nodes, and bridging the DODAG with Internet.

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 to the source of DAO message.

RPL provides point-to-point (P2P) routing mechanism for any two nodes to communicate in the DODAG [17]. If the destination node is the one-hop neighbor node of the packet sender, the latter directly sends the packet to destination node without going through its parent node. Otherwise, the operations of P2P routing mechanism depend on whether RPL is configured as storing or non-storing mode. In the non-storing mode, except for DODAG root, each node does not store any routing information about downward nodes. In this case, any packet must be first delivered through the upward route to the DODAG root, which will forward the packet to destination node. In the storing mode, each node locally caches the routing information about downward nodes. If the destination node is a descendant of packet sender, it forwards the packet to destination node via cached downward route. Otherwise, the packet is forwarded to parent node, at which the same aforementioned operations will be applied to send the packet to destination node. As such, the packet will be forwarded through upward routes until reaching the node that is the first ancestor of both packet sender and destination node.

B. Energy Depletion Attack

Normally, P2P routing mechanism is used to initiate data transfer, send end-to-end acknowledgments, or carry out infrequent network diagnostics. However, the vulnerability of P2P routing mechanism, e.g., all nodes unhesitatingly and faithfully route the received packets to destination node, can be exploited by adversary to attack the network as well. For example in Subfig. 1(a), a malicious node n_m generates and sends a large number of packets, denoted as $^*pkt$, to a destination node n_t. In the non-storing mode, all packets first have to be forwarded through upward route to the DODAG root n_R, which forwards the $^*pkt$ to destination node n_t according to cached downward route. In the storing mode, all packets will be forwarded through upward route until reaching the first common ancestor of n_m and n_t, which is the DODAG root n_R, and then delivered to destination node n_t. Thus, no matter which mode is configured, all intermediate nodes (i.e., n_k, n_f, n_b, n_d, n_i, and n_s) located along the forwarding path between packet sender n_m and destination node n_t have to receive and forward a large number of packets, which consume a significant amount of energy resource. In LLNs, since each node is equipped with a limited amount of energy, energy depletion attack can easily deplete the limited energy resource of legitimate nodes, and finally make the network suffer from denial of service. In Subfig. 1(b), we measure the energy consumption against number of malicious nodes and attack rate (r_{atk}) under energy depletion attack (EDA).

IV. The Proposed Approach

The basic idea of misbehavior-aware threshold detection (*MAD*) is that each node maintains a count of the number of received packets from its one-hop neighbor node within a specific time window, and then compares the count with a dynamically calculated threshold to detect malicious node.

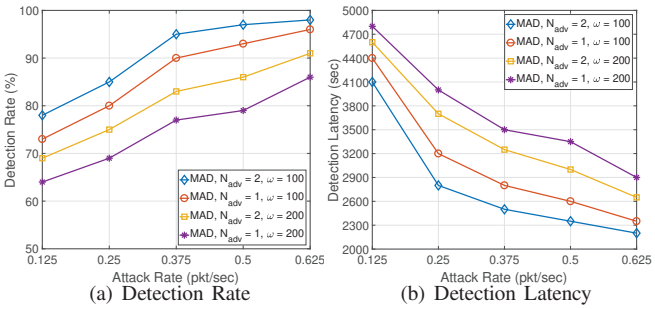
First, each node maintains an Observation Table (*OT*) to record the number of received packets from each neighbor node during an observation window (ω). In this paper, observation window ω is designed as a system parameter and can be configured depending on the urgency of removing malicious nodes from the network. For example, a communication

critical network in industrial control system or battlefield, ω is given a smaller value in order to frequently evaluate the forwarding operations of neighbor nodes, and quickly detect and isolate the potential adversary from the network. To balance the trade-off between detection accuracy and isolation latency, ω can have a relatively large value in non-critical situation. Here, the performance impacts of ω are observed in Section V. The *OT* consists of three components: neighbor node's id (nid), the number of received packets within observation window (rp), and the beginning timestamp of observation window (ts). At the beginning of each observation window, the number of received packets rp is reset to zero, and the timestamp ts is set to current time (t_{cur}).

Second, we also suggest each node to maintain a Detection Table (*DT*) to record the number of detected forwarding misbehaviors of each neighbor node, an entry of *DT* consists of two components: neighbor node's id (nid) and the number of detected forwarding misbehaviors (c_{mis}). If the number of received packets rp from neighbor node is larger than the dynamically calculated threshold value, the corresponding forwarding operations of neighbor node within observation window is suspected as forwarding misbehavior, and c_{mis} is increased by one. In this paper, the number of detected forwarding misbehaviors c_{mis} is utilized to calculate the threshold value, and indicates how much weight a neighbor node's forwarding operations rp accounts for the calculation of threshold value. If a neighbor node has a larger c_{mis}, the number of received packets from this node within observation window will have less weight in the calculation of threshold value, and vice versa. Note that the rationale behind this design is to consider an implicit penalty of forwarding misbehaviors. If a malicious neighbor node shows more forwarding misbehaviors which can be detected, a larger c_{mis} will be observed. However, the larger c_{mis} makes the rp of malicious neighbor node have less weight in the calculation of threshold, thus, the threshold will be scaled to the rp of normal neighbor nodes, and the forwarding misbehavior can be easily detected.

Third, at the end of each observation window, each node examines Observation Table *OT* and Detection Table *DT*, and calculates a threshold value as the reasonable number of received packets from neighbor node within observation window. In this paper, the threshold value (T_{pkt}) is calculated based on the historical detection result and most recent forwarding record, and it is expressed as, $T_{pkt} = \frac{\sum_{i=nid}^{G} wt_i \cdot rp_i}{|G|}$. Here, G is the one-hop neighbor list. wt_i is the weight that the forwarding record of node n_i accounts for the calculation of T_{pkt}, and it is expressed as, $wt_i = 1 - \frac{c^i_{mis}}{\sum_{j=nid}^{G} c^j_{mis}}$. Thus, the threshold value T_{pkt} can be expressed as $T_{pkt} = \frac{\sum_{i=nid}^{G} \left(1 - \frac{c^i_{mis}}{\sum_{j=nid}^{G} c^j_{mis}}\right) \cdot rp_i}{|G|}$.

Fourth, when the observation window ends, if the number of received packets from neighbor node within observation window is larger than T_{pkt}, the corresponding forwarding operations are suspected as forwarding misbehavior, and the number of detected forwarding misbehaviors, c_{mis}, is increased by one. In addition, when the number of detected forwarding misbehaviors of suspected node reaches a threshold (φ), the node broadcasts an *Isolate* packet to its one-hop neighbor nodes to prevent them from receiving or accepting any packet from the suspected malicious node. This way, the malicious node cannot be involved in any routing operations, and it is isolated from the network.



(a) Detection Rate (b) Detection Latency

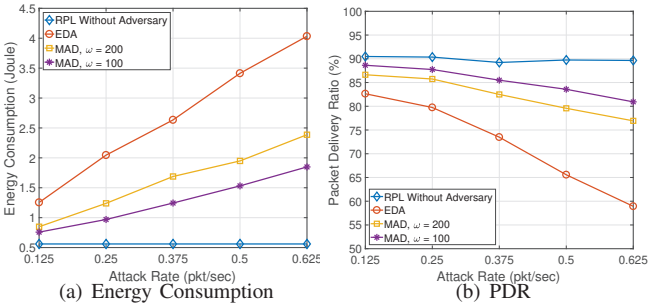
Fig. 2. The detection rate and detection latency against attack rate.

V. Performance Evaluation

We conduct extensive simulation experiments using OMNeT++ [2] to evaluate the performance of the proposed scheme. 100 nodes including one DODAG root are uniformly distributed within a 200×200 m^2 square network area. The communication range of each node is 30 (m). An exponential packet rate with mean 0.1 is adopted to emulate low network traffic scenarios in LLNs. The size of each packet is 40 bytes. 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 [18]. The channel error rate is set to 10%. We assume that the DODAG root is always trusted, and a couple of legitimate nodes are compromised and reprogrammed by adversary to behave maliciously. The attack rate varies between 0.125 and 0.625 pkt/sec. The total simulation time is 5000 seconds.

In Subfig. 2(a), we measure the detection rate by changing attack rate r_{atk}, number of malicious nodes N_{adv}, and observation window ω. As the attack rate increases linearly, the detection rate of the proposed scheme increases quickly. This is because the malicious node generates and sends a larger number of attack packets with larger r_{atk}, which is much higher than normal packet rate, the packet receiver can easily detect the forwarding misbehavior by comparing forwarding record with the calculated threshold with a significant difference. When the attack rate reaches 0.625 pkt/sec, the overall detection rate is above 85%. When the number of malicious nodes N_{adv} increases to 2, a higher detection rate is observed. This is because more malicious nodes show forwarding misbehaviors by generating and sending attack packets, more forwarding misbehaviors can be detected, and finally a higher detection rate can be observed. When a smaller observation window ω is configured in the approach, a higher detection rate can be achieved.

In Subfig. 2(b), we measure the detection latency by changing r_{atk}, N_{adv}, and ω. As the attack rate increases, the detection latency significantly decreases. This is because



(a) Energy Consumption (b) PDR

Fig. 3. The energy consumption and packet delivery ratio against attack rate.

the malicious node generates and sends more attack packets with larger attack rate, more forwarding misbehaviors can be detected, and the malicious node can be isolated and removed from network more quickly. With a shorter observation window ω, a lower detection latency is observed. This is because the malicious node will be evaluated more often with smaller ω, more forwarding misbehaviors can be detected, and a lower detection latency is achieved. When more malicious nodes exist in the network, a lower detection latency can be achieved.

In Subfig. 3(a), the energy consumption is measured based on the number of forwarded and overheard packets by changing r_{atk} and ω. Without adversary, the energy consumption of RPL is maintained around 0.5 Joule. This is because a low packet rate is employed by legitimate nodes, which generate and send a limited number of packets to destination nodes, the lowest energy consumption is observed. As the attack rate increases, the energy consumption of energy depletion attack (EDA) significantly increases. This is because the malicious node generates and sends more attack packets to destination nodes, all the intermediate nodes located along the forwarding path have to receive and forward a large number of packets, which consume a large amount of energy resource. However, as shown in Subfig. 3(a), the *MAD* can significantly reduce the energy consumption. Since each node counts the number of received packets from its one-hop neighbor nodes, calculates the threshold of the number of received packets within an observation window, and then detects the forwarding misbehaviors of malicious node. Thus, the malicious node can be isolated from the network quickly when the number of detected forwarding misbehaviors reaches a threshold value, and the network traffic is significantly reduced.

In Subfig. 3(b), we measure the packet delivery ratio (PDR) by changing r_{atk} and ω. The RPL without adversary achieves the highest PDR (about 90%), this is because the legitimate node generates and sends a limited number of packets, and every node cooperatively and faithfully forwards the received packets to destination node. However, due to bad channel quality, a few number of packets (approximate 10%) could get lost. As the attack rate increases, the PDR of energy depletion attack (EDA) significantly decreases. The *MAD* achieves a higher PDR than that of energy depletion attack (EDA). This is because the malicious node can be isolated from the network quickly, the legitimate nodes will be able to involve in the packet forwarding and receiving operations. As the observation window extends, a higher PDR can be observed.

VI. Conclusion

In this paper, we presented and analyzed the energy depletion attack with a preliminary result in RPL-based LLNs, where a malicious node intentionally generates and sends a large number of packets to destination nodes to excessively consume the energy resource of intermediate nodes located along the forwarding path. In light of this, we proposed a misbehavior-aware threshold detection scheme to efficiently detect the energy depletion attack, and extensive simulation results indicate that the proposed scheme is a viable approach against energy depletion attack in RPL-based LLNs.

Acknowledgment

This research was supported and made possible by NASA West Virginia Space Grant Consortium, Training Grant #NNX15AI01H, 2018 John Marshall University Summer Scholars Awards, and Startup grant in the Weisberg Division of Computer Science at Marshall University.

References

[1] A. Nia and N. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, September 2017, https://10.1109/TETC.2016.2606384.
[2] A. Varga, *OMNeT++*, 2014, http://www.omnetpp.org/.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.
[9] 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.
[10] C. Pu, "Mitigating DAO Inconsistency Attack in RPL-based Low Power and Lossy Networks," in *Proc. IEEE CCWC*, 2018, pp. 570–574.
[11] C. Pu and S. Hajjar, "Mitigating Forwarding Misbehaviors in RPL-based Low Power and Lossy Networks," in *Proc. IEEE CCNC*, 2018, pp. 1–6.
[12] 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.
[13] 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.
[14] C. Pu and X. Zhou, "Suppression Attack Against Multicast Protocol in Low Power and Lossy Networks: Analysis and Defenses," *Sensors*, vol. 18, no. 10, p. 3236, 2018.
[15] 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.
[16] T. Winter and P. Thubert, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *RFC Standard 6550*, March 2012.
[17] O. Gaddour and A. Koubâa, "RPL in a nutshell: A survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, 2012.
[18] A. Boulis, *Castalia*, 2014, http://castalia.forge.nicta.com.au.