Mitigating Suppression Attack in Multicast Protocol for Low Power and Lossy Networks

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

Xitong Zhou
MS Graduate of Computer Science
Marshall University
Huntington, WV 25755, USA
Email: zhou34@marshall.edu

Sunho Lim
Department of Computer Science
Texas Tech University
Lubbock, TX 79409, USA
Email: sunho.lim@ttu.edu

***Abstract*—With increasingly prevalent wireless sensors and devices, low power and lossy networks (LLNs) play an essential role in the realization of ubiquitous computing and communication infrastructure, which in turn, leads to enhanced data accessibility and availability. A multicast protocol for LLNs, also referred to as MPL, has been standardized to provide both efficient and reliable communication. Due to the shared wireless medium, lack of tamper resistance, and inherent resource constraints, MPL-based LLNs are vulnerable to various Denial-of-Service attacks. In this paper, we propose a heuristic-based detection scheme, called *HED*, against the suppression attack in MPL-based 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. The simulation results show that the proposed scheme is a viable approach against suppression attack.**

***Index Terms*—Denial-of-Service attack, low power and lossy networks, multicast protocol, suppression attack**

I. Introduction

A rapidly growing number of wireless sensors and devices (later nodes), and hybrid networks are leading the emergence of Internet-of-Things (IoT) and its applications [1]. As a major part of IoT, low power and lossy networks (LLNs) play an essential role in the realization of ubiquitous computing and communication. The Internet Engineering Task Force (IETF) Working Group has proposed a multicast protocol for LLNs, also referred to as MPL [2], as the multicast communication standard. However, MPL-based LLNs are unquestionably vulnerable to various Denial-of-Service attacks [3] because of the inherent shared wireless medium and the lack of physical protection and security requirements of network protocol.

In this paper, we investigate a suppression attack and propose a heuristic-based detection scheme, called *HED*, to efficiently mitigate the suppression attack in MPL-based LLNs. In the HED, each node maintains an increment rate of the minimum sequence number in the Seed Set, and compares the recent increment of sequence numbers within a time period with the heuristically calculated increment threshold of sequence numbers to detect potential malicious node. We develop a customized discrete event-driven simulation framework by using OMNeT++ [4] and evaluate its performance through extensive simulation experiments. The simulation results indicate that the proposed countermeasure is a viable detection approach to suppression attack in MPL-based LLNs.

II. Related Work

Significant research efforts have been made to investigate a variety of attacks and countermeasures in resource-constrained wireless networks. In [5], a camouflage-based detection scheme, called CAM, is proposed to detect the forwarding misbehavior in energy harvesting motivated networks (EHNets). The EYES [6] is an extended version of the CAM. The AAA [7] is proposed to detect the stealthy collision attack in EHNets. In the SCAD [8], 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 (WSNs). In [9], a DSR-based bait detection scheme incorporated with a digital signature technique is proposed to detect routing misbehaviors in mobile ad hoc networks (MANETs).

Over the last few years, researchers have explicitly studied the numerous security issues associated with LLNs. The CMD [10] 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 [11], a dynamic threshold mechanism is proposed to mitigate the destination advertisement object (DAO) inconsistency attack 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.

III. Countermeasure to Suppression Attack

A low power and lossy network running with MPL is considered, where a set of resource-constrained nodes including single source node communicates among themselves directly or indirectly through lossy links. Each node is uniquely identified by an identifier, e.g., an IPv6 address. We assume that an adversary is able to capture and compromise a legitimate node, gain access to all stored information (e.g., public and private keys), and reprogram it to behave maliciously [13]. The primary goal of the adversary is to disrupt the MPL and interfere with any on-going communication. A malicious node will not intentionally drop all received multicast messages (i.e.,

978-1-5386-4413-3/18/$31.00 ©2018 IEEE

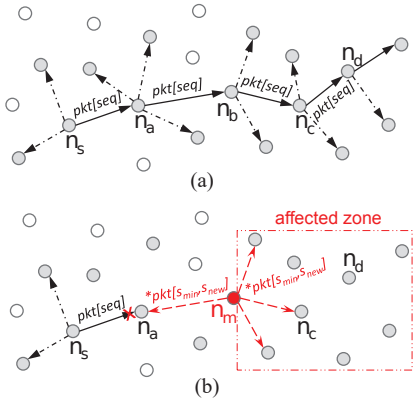

Fig. 1. An example of multicasting a data message: (a) no adversary, and (b) one adversary launching the suppression attack.

blackhole attack) because the legitimate nodes could still receive the messages from other multicasting nodes. In this paper, we primarily focus on the multicasting misbehavior and its corresponding adversarial scenario, where the malicious node multicasts a series of spoof data messages with continuous sequence numbers to suppress normal nodes to accept valid data messages and cause them to delete their cached data messages. We only deal with the scenario that the malicious node acts alone, and the problem of colluding malicious nodes is out of the scope of this paper. Note that we do not consider suppression attack combined with other general attacks, such as sybil, collision or jamming, wormhole, or vampire attacks.

The MPL uses a sequence number to normally maintain the order of data messages transmitted from a source node. However, the sequence number can be misused by an adversary to attack the network. Suppose that a source node (n_s) multicasts a data message ($pkt[seq]$) with a sequence number (*seq*) to a node (n_d) via intermediate nodes (e.g., n_a, n_b, and n_c) as shown in Subfig. 1(a), where other nodes that subscribe to the same MPL domain also could receive and multicast the data message. We implicitly assume that each node faithfully and collaboratively multicasts $pkt[seq]$ and thus, n_d can successfully receive the data message. A malicious node can intentionally multicast a series of spoof data messages with continuous sequence numbers within a short period of time to increase the minimum sequence number stored in the Seed Set. This can prevent the legitimate nodes from accepting valid data messages with a sequence number less than the minimum sequence number from the source node, and cause them to delete data messages with a sequence number less than the minimum sequence number from the Buffered Message Set. In Subfig. 1(b), for example, a malicious node (n_m) multicasts a series of spoof data messages with continuous sequence numbers ranging between s_{min} and s_{new} within a short period of time, denoted as ${}^*pkt[s_{min}, s_{new}]$, to its neighbor nodes. Here, s_{min} is the minimum sequence number stored in the Seed Set at neighbor nodes. Through frequently exchanged MPL control messages, it is not hard for a malicious node to find out the stored minimum sequence number at neighbor nodes. When a legitimate node, e.g., n_a, receives ${}^*pkt[s_{min}, s_{new}]$ from n_m, it updates the minimum sequence number stored in the Seed Set to (s_{new} + 1) and then deletes any data message that has sequence number less than (s_{new} + 1) from the Buffered Message Set. When the source node (n_s) generates and multicasts a new data message ($pkt[seq]$), where $seq <$ (s_{new} + 1), the legitimate node (n_a) will not accept $pkt[seq]$ based on the MPL protocol since $pkt[seq]$ has the sequence number less than the minimum sequence number stored in the Seed Set. As shown in Subfig. 1(b), due to the suppression attack, a great number of legitimate nodes that are located in the affected zone cannot accept valid data messages from the source node, suffering from denial of service.

In light of these, we propose a heuristic-based detection scheme, called HED, to efficiently mitigate the suppression attack. The basic idea of HED is that each node maintains an increment rate of the minimum sequence number in the Seed Set, and compares the recent increment of sequence numbers within a time period with the heuristically calculated increment threshold of sequence numbers to detect the potential malicious node in MPL-based LLNs. First, each node records a trace of multicast operations of neighbor nodes executed during an observation window (ω), and maintains a multicast trace table (*MT*) to monitor their multicast operations. We deploy an observation window (ω) to detect anomalous increment of sequence numbers within a time period, and ω is adaptively adjusted based on the number of detected multicasting misbehaviors of suspected malicious node. Here, ω is a system parameter. The multicast trace table consists of five components: neighbor node's id (*nid*), sequence number of the first received data message within observation window (*fs*), timestamp of the first received data message within observation window (t_{fp}), sequence number of the last received data message within observation window (*ls*), and timestamp of the last received data message within observation window (t_{lp}). For example, as shown in Subfig. 1(b), suppose a malicious node (n_m) multicasts a series of spoof data messages with continuous sequence numbers in range of s_{min} to s_{new} within a time period between t_{begin} and t_{end}, denoted by ${}^*pkt[s_{min}, s_{new}]$, to its neighbor nodes. When a legitimate node (e.g., n_a) receives ${}^*pkt[s_{min}, s_{new}]$, it updates the corresponding entry in the *MT*, $MT_a[m].fs = s_{min}$, $MT_a[m].t_{fp} = t_{begin}$, $MT_a[m].ls = s_{new}$, and $MT_a[m].t_{lp} = t_{end}$. In this example, we implicitly assume that the time period of multicast operations, (t_{end} - t_{begin}), is within the observation window ω. However, our approach is not dependent on this assumption and (t_{end} - t_{begin}) is not required to be within ω.

Second, we modify the Seed Set (*SS*) and introduce an additional component: increment rate of the minimum sequence number within observation window. Thus, the Seed Set *SS* consists of four components: identifier of source node (*nid*), minimum sequence number that the node is willing to receive (s_{min}), lifetime of the Seed Set entry (t_{life}), and increment rate of the minimum sequence number within observation window (R_{inc}). R_{inc} indicates how much the minimum sequence number has increased per second, and it is updated by the low pass filter with a filter gain constant α, $R_{inc} = \alpha \cdot R_{inc}$

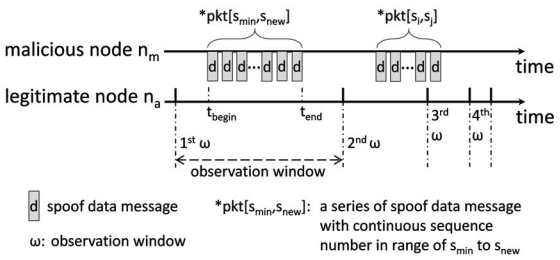

Fig. 2. Example of adaptively adjusted observation window ω based on the detected multicasting misbehavior.

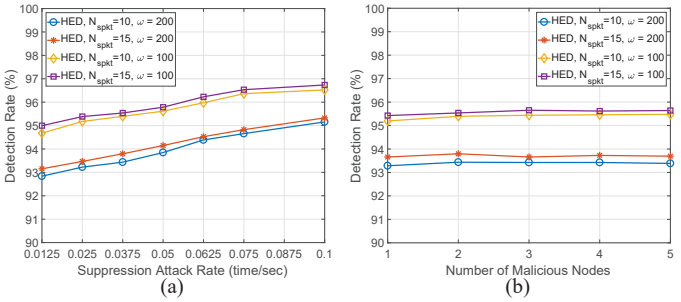

Fig. 3. The detection rate against suppression attack rate and number of malicious nodes.

$+ (1 - \alpha) \cdot R^k_{rec}$. Here, R^k_{rec} is the most recently calculated increment rate of minimum sequence number, and it can be expressed as $R^k_{rec} = \frac{ls^k - fs^k}{t^k_{lp} - t^k_{fp}}$. Thus, the increment rate of the minimum sequence number R_{inc} can be expressed as $R_{inc} = \alpha \cdot R_{inc} + (1 - \alpha) \cdot \frac{ls^k - fs^k}{t^k_{lp} - t^k_{fp}}$. Here, α is a system parameter.

Third, at the end of each observation window, each node examines its multicast trace table with an increment rate of the minimum sequence number in the Seed Set to detect any anomalous increment of sequence numbers that was caused by potential multicasting misbehaviors. If the recent increment of sequence numbers within observation window is larger than the heuristically calculated increment threshold of sequence numbers, the corresponding multicast operations are suspected as a multicasting misbehavior and the number of detected multicasting misbehaviors (c_{mis}) of suspected node is increased by one. Additionally, the observation window of the suspected node is reduced by half, $\frac{\omega}{2}$. When the c_{mis} reaches a threshold value φ, the node broadcasts an *Isolate* packet to its all one-hop neighbor nodes to prevent neighbor nodes from accepting any message from the suspected node.

In Fig. 2, for example, a malicious node (n_m) multicasts a series of spoof data messages with continuous sequence numbers $^*pkt[s_{min}, s_{new}]$ within a time period between t_{begin} and t_{end} to a legitimate node (n_a). At the end of first ω, n_a observes the actual increment of sequence numbers based on its multicast trace table, inc_{seq} = ($MT_a[m].ls$ - $MT_a[m].fs$), calculates the most recent increment rate of sequence numbers based on R^k_{rec}, updates increment rate of the minimum sequence number based on R_{inc}, and then heuristically calculates the increment threshold of sequence numbers, th_{seq} = ($MT_a[m].t_{lp}$ - $MT_a[m].t_{fp}$) $\times$ R_{inc}. If $inc_{seq} > th_{seq}$, the multicast operations of n_m are suspected as the multicasting misbehavior, the number of detected multicasting misbehaviors of n_m, c^m_{mis}, is increased by one, and the observation window of n_m, ω^m, is reduced by half, $\frac{\omega^m}{2}$. Additionally, the observation window of suspected node becomes shorter, and the multicast operations of a malicious node can be observed more often, and can result in more detections of multicasting misbehaviors. Thus, the smaller the observation window is, the more often the multicasting misbehaviors can be detected.

IV. Performance Evaluation

We conduct simulation experiments using OMNeT++ [4] to evaluate the performance of the proposed approach. A 150×150 m^2 square network area is considered, where 51 nodes including single source node are uniformly distributed. The communication range of each node is 30 (m). To emulate low packet rate scenarios, an exponential packet injection rate with mean 0.1 packet/sec is adopted and 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 [14]. The channel error rate is set to 10%. We assume that the source node is always trusted, and 2% to 10% of nodes can be compromised and reprogrammed by an adversary to behave maliciously. The suppression attack rate varies between 0.0125 and 0.1 time/sec, and the number of spoof data messages in each attack is 10 or 15. The total simulation time is 10,000 seconds.

First, we measure the detection rate against suppression attack rate, number of malicious nodes and N_{spkt} in Fig. 3. Overall, the detection rate of HED can be maintained above 90%. In Subfig. 3(a), the detection rate of HED increases as the suppression attack rate increases. This is because the malicious node shows more multicasting misbehaviors with increasing suppression attack rate, however, these multicasting misbehaviors can be easily detected within adaptively adjusted observation window. The HED with larger N_{spkt} achieves higher detection rate than that of the HED with smaller N_{spkt}. Since additional spoof data messages can cause the minimum sequence number to increase, the HED can easily compare the significant increment of a sequence number within a time period with the heuristically calculated increment threshold of the sequence number to detect multicasting misbehaviors. As the observation window reduces, a higher detection rate is achieved in comparison to a larger observation window. This is because each node can frequently compare the observed increment of a sequence number with the heuristically calculated increment threshold of sequence numbers to detect any multicasting misbehavior.

As shown in Subfig. 3(b), the detection rate of HED is not sensitive to the number of malicious nodes. The HED is a stand-alone approach [8] where the same detection scheme is running on each node but no information is exchanged for detection. Thus, each neighbor node of malicious node can record the multicast operations of malicious node and detect the potential multicasting misbehaviors. However, the detection rate is responsive to the length of the observation

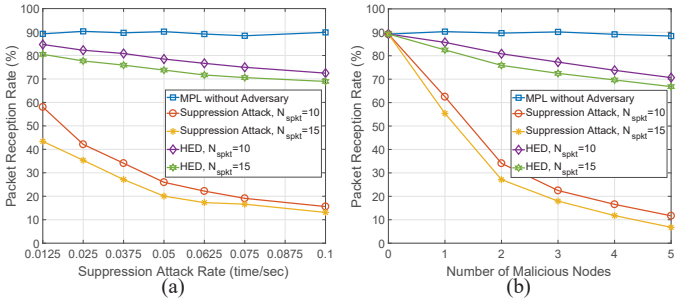

Fig. 4. The packet reception rate (PRR) against suppression attack rate and number of malicious nodes.

window, and a higher detection rate is observed with short observation window. In this instance, the multicast operations of a malicious node can be continuously evaluated, and more multicasting misbehaviors can be detected.

Second, the packet reception rate (PRR) is measured against suppression attack rate and number of malicious nodes in Fig. 4, in which the MPL without adversary provides the highest PRR, around 90%, and it is used as the upper bound of PRR. In Subfig. 4(a), as the suppression attack rate varies between 0.0125 and 0.1 time/sec, the PRR of MPL under the suppression attack with different number of spoof data messages (N_{spkt}) significantly decreases from 60% and 43% to approximate 15%. This is due to the fact that the malicious node multicasts spoof data messages more frequently as the suppression attack rate increases, the minimum sequence number stored in the Seed Set increases more often, and less number of valid data messages from the source node will be accepted. Lower PRR is observed with larger $N_{spkt} = 15$ under suppression attack. Since more spoof data messages make the minimum sequence number increase greatly and quickly, more valid data messages from the source node will be rejected. The HED provides lower and higher PRR than that of the MPL with and without the suppression attack, because each node records the multicast operations of neighbor nodes within an adaptively adjusted observation window to detect any anomalous increment of the sequence number. Thus, the multicasting misbehaviors of a malicious node can be easily detected, and quickly isolated from the network. The result is that more data message can be received. As the N_{spkt} increases, a lower PRR is observed. This is because more valid data messages will be rejected due to the changes in the increment of the minimum sequence number.

As shown in Subfig. 4(b), when the number of malicious nodes increases, the PRR of MPL under suppression attack decreases. This is because more number of malicious nodes can launch more multicasting misbehaviors, and more valid data messages from source node will be rejected. However, the HED provides much higher PRR than that of MPL under the suppression attack. This is because the HED can detect the anomalous increment of sequence number due to multicasting misbehaviors of malicious node, the malicious node can be isolated and removed from the network more quickly, and more data messages can be received.

V. Concluding Remarks

In this paper, we presented and analyzed the suppression attack in MPL-based LLNs, where a malicious node multicasts a series of spoof data messages with continuous sequence numbers to prevent the normal nodes from accepting valid data messages and cause them to delete the cached data messages. To resolve this issue, we proposed a heuristic-based detection scheme to efficiently detect the suppression attack in MPL-based LLNs, where each node maintains an increment rate of minimum sequence number in the Seed Set, and compares the recent increment of sequence numbers within a time period with the heuristically calculated increment threshold of sequence numbers to detect potential multicasting misbehaviors. Extensive simulation results show high detection rate and packet reception rate. Thus, the proposed scheme can be a viable approach against the suppression attack in MPL-based LLNs. Since radio propagation and its channel dynamics cannot easily be captured by simulation models, we plan to develop a small-scale testbed and deploy a real network to see the full potential of the proposed countermeasure.

Acknowledgment

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

References

[1] M. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, 2016.

[2] J. Hui and R. Kelsey, "Multicast Protocol for Low-Power and Lossy Networks (MPL)," *RFC Standard 7731*, February 2016.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

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

[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] S. Challa, M. Wazid, A. Das, N. Kumar, A. Reddy, E. Yoon, and K. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

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