


Article

# Suppression Attack Against Multicast Protocol in Low Power and Lossy Networks: Analysis and Defenses

Cong Pu <sup>1,\*</sup>  and Xitong Zhou <sup>2</sup><sup>1</sup> Weisberg Division of Computer Science, Marshall University, Huntington, WV 25755, USA<sup>2</sup> MS Graduate of Computer Science, Marshall University, Huntington, WV 25755, USA; zhou34@marshall.edu

\* Correspondence: puc@marshall.edu; Tel.: +1-304-696-6204

Received: 14 August 2018; Accepted: 21 September 2018; Published: 26 September 2018



**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 (MPL), has been standardized to provide both efficient and reliable multicast communication. Due to the shared wireless medium, lack of tamper resistance, and inherent resource constraints, MPL-based LLNs are undoubtedly vulnerable to various Denial-of-Service (DoS) 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. In the HED, each node maintains an increment rate of the minimum sequence number in the Seed Set to detect the potential malicious node by comparing the recent increment of sequence numbers with the heuristically calculated increment threshold of sequence numbers. We evaluate the proposed scheme through extensive simulation experiments using OMNeT++ and compare its performance with original MPL with and without adversary, respectively. The simulation results show high detection rate and packet reception rate but low false detection rate, and indicate that the proposed scheme is a potentially viable approach against the suppression attack in MPL-based LLNs.

**Keywords:** Denial-of-Service attack; low power and lossy networks; multicast protocol; suppression attack

## 1. 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, where a myriad of multiscale nodes are seamlessly blended and communicate with each other [1]. It has been predicted that 11 billion wirelessly connected nodes will be available for IoT applications in 2018, a 33% increase from 2017, and will reach 20.4 billion by 2020 [2]. Economic growth of IoT-based services and applications is also said to be considerable for businesses. It is probable that the whole annual economic impact caused by IoT will be in the range of \$2.7–6.2 trillion by 2025 [3]. With the prevalence of WiFi and 4G LTE, cloud computing, social networking, and the recent technological advances in embedded devices and sensor networks, we envision a future in which wireless IP-enabled smart nodes under IoT will enhance data accessibility and availability, and lead to the further improvement of our lives.

As a major part of IoT, low power and lossy networks (LLNs) play an essential role in the realization of ubiquitous computing and communication, where a set of resource-constrained nodes in terms of communication, computation, memory, and energy communicates among themselves directly or indirectly via lossy links. With the increasing demand of sharing information and knowledge and

coordinating decisions, the Internet Engineering Task Force (IETF) Working Group has proposed a multicast protocol for LLNs, also referred to as MPL [4], as the multicast communication standard. However, MPL-based LLNs are unquestionably vulnerable to various Denial-of-Service attacks [5] because of the inherent shared wireless medium and the lack of physical protection and security requirements of network protocol. It has been noted that DoS attacks primarily target service availability to diminish the network capability by disrupting network protocol or interfering with any on-the-fly communication, rather than subverting the service itself. To address these issues, the MPL standard [4] makes the recommendation to employ the use of link-layer security mechanisms (e.g., IEEE 802.15.4 AES-128 [6] and Cisco's CG-Mesh [7]) to prevent an outside attacker who has no access to cryptographic materials from injecting spoof messages. However, the link-layer security mechanisms are incapable of countering an inside attacker who can capture and compromise a legitimate node, gain access to all stored information (e.g., public and private keys), and reprogram it to behave maliciously [8]. The current MPL implementations often do not deploy extra security operations that can significantly consume computing power and affect the performance of resource-constrained nodes [5,9,10]. In addition, a security threat analysis of LLNs presented in [11] is limited to discussing only well-known attacks with fundamental countermeasures. Thus, MPL-based LLNs are open to new attack wherein a malicious node can easily multicast a series of spoof data messages to disrupt routing protocol and interfere with on-going communications.

In light of the above, 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 suppression attack, a malicious node multicasts a series of spoof data messages with continuous sequence numbers to prevent legitimate nodes from accepting valid data messages, and cause them to delete their cached data messages as well. Although the countering of jamming attacks and its variants have been extensively studied [12], the suppression attack and its countermeasure in MPL-based LLNs are under-explored and remain in their infancy. Our major contributions are summarized in the following:

- We significantly extend our previous work [13], and analyze the suppression attack with a preliminary result in MPL-based LLNs. This is the first in-depth work that investigates the performance impact of suppression attack in MPL-based LLNs.
- We 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 propose a simple analytical model of the HED and show its numerical result in terms of miss detection rate. We also revisit and implement the original MPL with and without adversary for performance comparison. In addition, the original MPL without adversary will be used as the upper bound of packet reception rate.

We develop a customized discrete event-driven simulation framework by using OMNeT++ [14] and evaluate its performance through extensive simulation experiments in terms of detection rate, packet reception rate, false detection rate, and changes of increment rate. The simulation results indicate that the proposed countermeasure is a viable detection approach to suppression attack in MPL-based LLNs.

The remainder of the paper is organized as follows. Prior approaches are presented and analyzed in Section 2. The basic MPL operations, analysis of suppression attack with a preliminary result, and the proposed countermeasure are presented in Section 3. An analytical model of the proposed countermeasure is presented in Section 4. Performance evaluation, including extensive simulation experiments and analysis, is provided in Section 5. In Section 6, we analyze and compare the suppression attack with well-known jamming attack in terms of attack method, stealthiness, attack

energy efficiency, and level of denial of service. Finally, Section 7 concludes the paper with possible future research directions.

## 2. Related Work

In this section, we categorize and analyze a variety of existing attacks and countermeasures in terms of wireless ad hoc networks, low power and lossy networks, and Internet of Things.

### 2.1. Wireless Ad Hoc Networks

In [15], a camouflage-based detection scheme, called CAM, is proposed to detect the forwarding misbehavior in energy harvesting motivated networks (EHNets). The basic idea is that each node hides its current operational status and pretends not to overhear or monitor any on-going forwarding operation of its adjacent nodes to detect a deep lurking malicious node. A cooperative countermeasure (EYES) [16] 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. The AAA [17] is proposed to detect the stealthy collision attack in EHNets, where each node forwards a data packet, and then monitors the subsequent packet transmission of its one-hop downstream node and waits for an explicit acknowledgment packet from its two-hop downstream node. In the SCAD [18], 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), where single or multiple malicious nodes randomly or selectively drop any incoming packet. In [19], a novel reactive routing scheme integrated with bypass technique is proposed to mitigate the selective forwarding attack in WSNs, where each node estimates and observes the parent node's reliability and link quality, and then decides whether to forward the packet.

In [20], a DSR-based bait detection scheme incorporated with a digital signature technique is proposed to detect routing misbehaviors in mobile ad hoc networks (MANETs), where a source node broadcasts a route request packet with a fictitious destination node to lure potential malicious nodes to reply a fake route reply packet. Yang et al. [21] proposed a polynomial-based compromise-resilient en-route filtering (PCREF) scheme against false data injection attack in cyber-physical networked systems. The PCREF is designed by adopting message authentication polynomials rather than message authentication codes and clusters to avoid utilizing node locations. Zou et al. [22] examined 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.

### 2.2. Low Power and Lossy Networks

Over the last few years, researchers have explicitly studied the numerous security issues associated with LLNs. In the VeRA [23], a version number and rank authentication security scheme based on one-way hash chains are proposed to secure the IPv6 routing protocol (RPL) [24] in LLN, where the misbehaving nodes illegitimately increase the version number of directed acyclic graph information object (DIO) message and compromise illegal rank values. To protect against the attackers that send DIO messages with higher version number values or that publish a high rank value, the version numbers are bound with authentication data and signature. In [25], 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. Four adversarial scenarios motivated by violating rank rule permanently and non-permanently and their potential performance impact are analyzed. In the Dodge-Jam [26], a lightweight anti-jamming technique suitable for LLN environments is proposed to address the stealthy jamming attacks with small overhead. Perazzo et al. [27] investigated the DODAG Information Object suppression attack, which can severely degrade the routing service in RPL. The CMD [28] 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 [29], a dynamic threshold mechanism is proposed to mitigate the destination advertisement object (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. The [30] identified and investigated 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.

### 2.3. Internet of Things

The SVELTE [31] proposes a novel intrusion detection system to secure Low-Power Wireless Personal Area Network (6LoWPAN) from the network layer and routing attacks. Beigi-Mohammadi et al. [32] designed and implemented an intrusion detection system that can be modified to employ RPL routing protocol in neighborhood area network. Hummen et al. [33] proposed two complementary and lightweight defense mechanisms to counter fragmentation attack in the adaptation layer of 6LoWPAN. The security capability of IEEE 802.15.4 MAC protocol as well as the limitations thereof in the context of IoT are analyzed in [34]. A security threat analysis of RPL has been performed in [11], where potential security issues and fundamental countermeasures are presented. A more detailed survey of DoS attacks in IoT can be found in [35,36]. In [5], the history of research efforts in RPL-based LLNs and future research directions on which LLNs should evolve have been reviewed and discussed.

In summary, various attacks and their countermeasures have been well studied throughout various networks and environments. However, little attention has been shown to the suppression attack in the realm of MPL-based LLNs.

## 3. Countermeasure to Suppression Attack

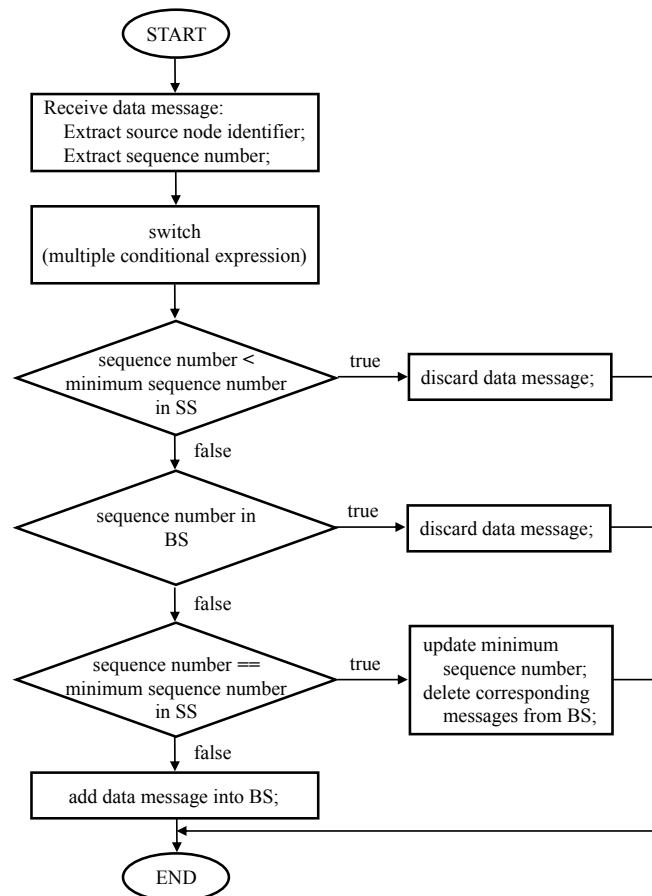
In this section, we begin with an overview of the multicast protocol for low power and lossy networks. Then, we analyze the suppression attack with a preliminary result. Finally, we present both system and adversary models and propose a heuristic-based detection scheme, also called HED, against the suppression attack in MPL-based LLNs.

### 3.1. Overview of Multicast Protocol

Multicast protocol for low power and lossy networks, also referred to as MPL [4], is a IPv6 multicast forwarding protocol in resource-constrained networks. The MPL disseminates messages to all the nodes within the same MPL domain without the need of constructing or maintaining any multicast forwarding topology. To exchange control-plane and data-plane messages in a highly robust, energy efficient, and scalable manner, the MPL relies on the Trickle Algorithm [37]. The basic idea of Trickle Algorithm is to optimize the message transmission frequency based on network conditions. Specifically, the frequency is increased whenever an inconsistent network information is received, and decreased in the opposite case.

When a source node has a data message to send within an MPL domain, it generates a message that includes the MPL domain address as a destination address. Here, the MPL domain is a scope zone in which nodes subscribe to the same MPL domain address and also participate in the dissemination of MPL data and control messages. The source node also piggybacks its identifier, a newly generated sequence number, and the payload in the data message. It then schedules a multicast of data message using the Trickle Algorithm, which is completed without any prior indication that the neighboring nodes have received the data message. After transmitting the data message a limited number of times, the source node terminates the transmission process of data message.

When the node that subscribes to the same MPL domain address has received the data message, it extracts the source node identifier and sequence number to determine whether or not the data message has been received. If the sequence number is less than the minimum sequence number maintained in the Seed Set, or equal to the sequence number stored in the Buffered Message Set, the receiving node discards the data message because it believes that it has received the data message before. In the MPL, a Seed Set records a sliding window that is used to determine the sequence number of data message that the node is willing to receive. The Seed Set consists of three components: the identifier of source node, the minimum sequence number that the node is willing to receive, and the lifetime of the Seed Set entry. Additionally, a Buffered Message Set records recently received data messages that have a sequence number greater than the minimum sequence number in the Seed Set. The Buffered Message Set is composed of three components: the identifier of source node, the sequence number of data message, and the payload of data message. If the sequence number is equal to the minimum sequence number in the Seed Set, the receiving node updates the minimum sequence number to one greater than the received data message's sequence number. At this point, it deletes any data message that has a sequence number less than the updated minimum sequence number from the Buffered Message Set. If the sequence number is greater than the minimum sequence number in the Seed Set, but not stored in the Buffered Message Set, the receiving node adds the received data message into the Buffered Message Set. Then, the receiving node multicasts the received data message using the Trickle Algorithm to all neighbor nodes that subscribe to the same MPL domain. Here, an overall information flow of normal node that receives a data message is shown in Figure 1.



**Figure 1.** An information flow of a normal node that receives a data message. Here, *SS* and *BS* denote Seed Set and Buffered Message Set, respectively.

Nodes that subscribe to the same MPL domain also periodically exchange a MPL control message using the Trickle Algorithm to discover new data messages that have not been received, where MPL

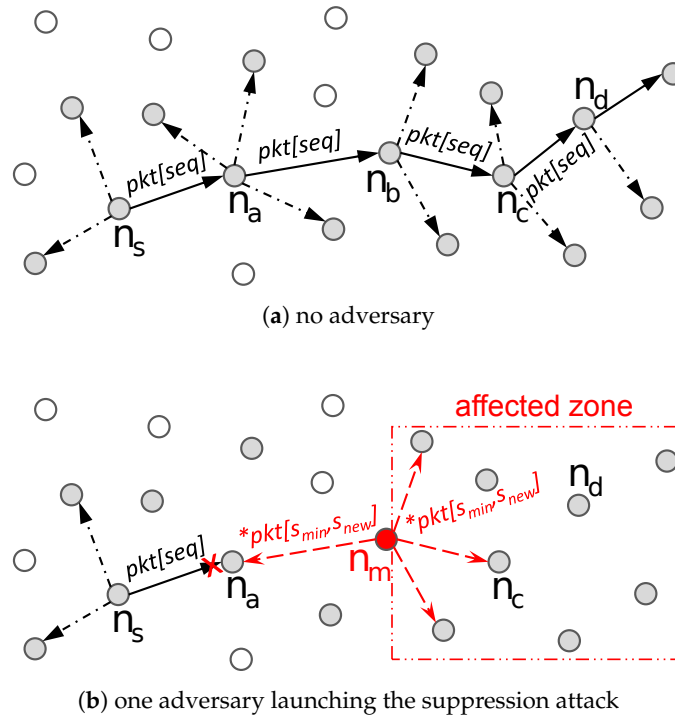
control message contains the information of Seed Set and Buffered Message Set. If a node discovers a neighbor node that has not received certain data messages, it multicasts those data messages using the Trickle Algorithm.

### 3.2. Analysis of Suppression Attack

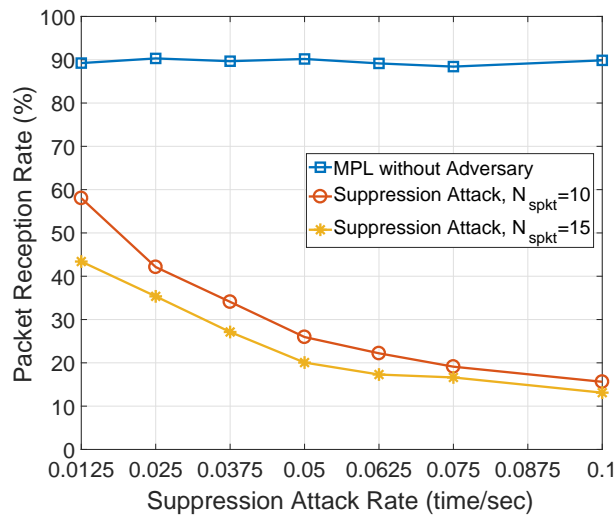
The MPL uses a sequence number to normally maintain the order of data messages transmitted from a source node. However, the sequence number can be misused by an adversary to attack the network. For example, a malicious node can intentionally multicast a series of spoof data messages with continuous sequence 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.

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 Figure 2a, 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. However, a malicious node can easily launch the suppression attack by multicasting a series of spoof data messages with continuous sequence numbers to increase the minimum sequence number stored in the Seed Set at legitimate nodes. In Figure 2b, 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. The malicious node could increase the time of multicasting a series of spoof data messages with continuous sequence numbers, however, the malicious node does not benefit from doing so because the minimum sequence number maintained in the Seed Set will not be increased greatly. 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 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 Figure 2b, 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 Figure 3, we measure the packet reception rate against the suppression attack rate and number of spoof data messages ( $N_{spkt}$ ). In this paper, the suppression attack rate indicates how frequently a malicious node multicasts a series of spoof data messages with continuous sequence numbers to increase the minimum sequence number stored in the Seed Set. As shown in Figure 3, when the suppression attack rate increases, the packet reception rate of legitimate node decreases quickly. This is because the series of spoof data messages with continuous sequence numbers makes the minimum sequence number increase, and data messages with smaller sequence number from source node will not be accepted. As the number of spoof data messages  $N_{spkt}$  increases in each attack, a lower packet reception rate is observed compared to that of  $N_{spkt} = 10$ . In effect, additional spoof data messages can make the minimum sequence number increase greatly and quickly, and more data messages from source node will be rejected, which leads to lower packet reception rate. In summary, the suppression attack can be easily launched to prevent a great number of legitimate nodes that subscribe to the same MPL domain from receiving valid data messages, and finally leads to denial of service in MPL-based LLNs.



**Figure 2.** An example of multicasting a data message: (a) no adversary; and (b) one adversary launching the suppression attack.



**Figure 3.** The packet reception rate against suppression attack rate and number of spoof data messages ( $N_{spkt}$ ). Here, we consider a network area ( $150 \times 150$  (m<sup>2</sup>)), where 51 nodes including one source node and five malicious nodes are uniformly distributed.

### 3.3. HED: Heuristic-Based Detection Scheme

**System and Adversary Models:** 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. Due to the shared wireless medium, lack of tamper resistance, and inherent resource constraints, 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 [8]. However, we do not consider node capture attack [38], where an adversary can capture a legitimate node from the network as the first step to further conduct different types of

attacks. 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., blackhole attack) because the legitimate nodes could still receive the messages from other multicasting nodes. The malicious node may inject bogus messages into the network to consume the scarce network resource (i.e., bogus data injection attack), but this attack can be easily prevented by using the technique proposed in [39]. 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.

**Major Operations:** 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. The HED has three major operations. First, each node records a trace of multicast operations of neighbor nodes executed during an observation window ( $\omega$ ), and maintains a multicast trace table ( $MT$ ) to monitor their multicast operations. We deploy an observation window ( $\omega$ ) to detect anomalous increment of sequence numbers within a time period, and  $\omega$  is adaptively adjusted based on the number of detected multicasting misbehaviors of suspected malicious node. Here,  $\omega$  is a system parameter and its impacts on the performance are observed in Section 5. 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 ( $t_{lp}$ ). Here, each entry in multicast trace table brings only an extra 12 bytes of overhead in the memory, where 4 bytes are for node's id and 2 bytes are for every other four components. For example, as shown in Figure 2b, 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  $\omega$ . However, our approach is not dependent on this assumption and  $(t_{end} - t_{begin})$  is not required to be within  $\omega$ .

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 ( $R_{inc}$ ). Here, the  $R_{inc}$  in Seed Set brings only an extra 2 bytes of overhead in the memory.  $R_{inc}$  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  $\alpha$ ,

$$R_{inc} = \alpha \cdot R_{inc} + (1 - \alpha) \cdot R_{rec}^k. \quad (1)$$

The basic idea of Equation (1) is that  $R_{inc}$  is calculated with the currently observed increment rate of the minimum sequence number within observation window and historical statistics of increment rate of the minimum sequence number. Here, a historical statistics of increment rate of the minimum



sequence number is represented by  $R_{rec}^k$ , which is the most recently calculated increment rate of minimum sequence number, and it can be expressed as,

$$R_{rec}^k = \frac{ls^k - fs^k}{t_{lp}^k - t_{fp}^k} \tag{2}$$

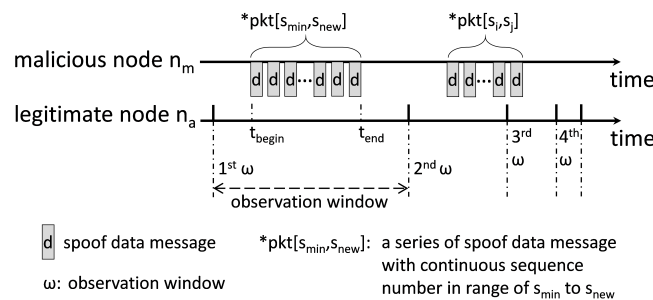
The basic idea of Equation (2) is to divide the increment of sequence number ( $ls^k - fs^k$ ) by the elapsed time period ( $t_{lp}^k - t_{fp}^k$ ) within  $k^{th}$  observation window. Thus, the increment rate of the minimum sequence number  $R_{inc}$  can be expressed as,

$$R_{inc} = \alpha \cdot R_{inc} + (1 - \alpha) \cdot \frac{ls^k - fs^k}{t_{lp}^k - t_{fp}^k} \tag{3}$$

Here,  $\alpha$  is a system parameter and its changes ( $\alpha \in [0.2, 0.8]$ ) and impacts on the increment rate  $R_{inc}$  are also observed in Section 5.

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  $\varphi$ , 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 Figure 4, 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  $\omega$ ,  $n_a$  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 Equation (2), updates increment rate of the minimum sequence number based on Equation (3), 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  $n_m$ ,  $c_{mis}^m$ , is increased by one, and the observation window of  $n_m$ ,  $\omega^m$ , 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 of malicious node can be detected. Both major operations of MPL protocol and HED scheme are summarized in Figure 5.



**Figure 4.** Example of adaptively adjusted observation window  $\omega$  based on the detected multicasting misbehavior.

**Notations:**

- $\omega, SS, BS, s_{min}, R_{rec}, R_{inc}, \alpha, MT, t_{lp}, t_{fp}, ls, fs, \varphi, inc_{seq}, th_{seq}$ , and  $c_{mis}$ : Defined before.
- $t_{cur}, H_s$ : The timestamp when a node receives a data message. The set of sequence number in the Buffered Message Set  $BS$ .
- $pkt[src, seq, type]$ : A message containing a source node id ( $src$ ), sequence number ( $seq$ ), and message type ( $type$ ). Here,  $type$  can be *data*, *control*, or *Isolate*. If the  $type$  is *Isolate*, the  $seq$  field is the identifier of suspected malicious node.

**Event-driven MPL Algorithm:**

- ◊ When a source node  $n_s$  has a data message to send:  
Generate and multicast data message  $pkt[s, seq, data]$ ;
- ◊ When a legitimate node  $n_i$  receives  $pkt[s, seq, data]$  from  $n_m$ :  
if  $pkt[s, seq, data]$  is the **first** received data message within  $\omega^m$   
 $MT_i[m].fs = seq; MT_i[m].t_{fp} = t_{cur}$ ;  
if  $pkt[s, seq, data]$  is the **last** received data message within  $\omega^m$   
 $MT_i[m].ls = seq; MT_i[m].t_{lp} = t_{cur}$ ;  
if  $pkt[seq] < SS_i[s_{min}]$  /\* Old data message \*/  
Discard  $pkt[s, seq, data]$ ;  
elif  $pkt[seq] \in BS_i.H_s$  /\* Old data message \*/  
Discard  $pkt[s, seq, data]$ ;  
elif  $pkt[seq] == SS_i[s_{min}]$  /\* Expected new message \*/  
 $SS_i[s_{min}] += 1$ ;  
for  $seq \in BS_i.H_s$  /\* Clean old messages from  $BS$  \*/  
if  $seq < SS_i[s_{min}]$   
Delete  $BS_i.H_s[seq]$ ;  
else /\* Cache new message \*/  
Add  $pkt[s, seq, data]$  into  $BS$ ;

**Event-driven HED Algorithm:**

- ◊ When observation window of  $n_m, \omega^m$ , ends at legitimate node  $n_i$ :  
 $R_{rec} = \frac{MT_i[m].ls - MT_i[m].fs}{MT_i[m].t_{lp} - MT_i[m].t_{fp}}$ ; /\* Eq. 2 \*/  
 $R_{inc} = \alpha \times R_{inc} + (1 - \alpha) \times R_{rec}$ ; /\* Eq. 1 \*/  
 $inc_{seq} = MT_i[m].ls - MT_i[m].fs$ ;  
 $th_{seq} = (MT_i[m].t_{lp} - MT_i[m].t_{fp}) \times R_{inc}$ ;  
if  $inc_{seq} > th_{seq}$  /\* Multicasting misbehavior \*/  
 $c_{mis}^m += 1; \omega^m = \frac{\omega^m}{2}$ ;  
if  $c_{mis}^m \geq \varphi$   
Broadcast  $pkt[s, m, Isolate]$ ;

Figure 5. The pseudo code of MPL protocol and the proposed HED scheme.

#### 4. Analysis of the Proposed Countermeasure

In this section, we analyze the HED in terms of average miss detection rate. When multiple spoof data messages are frequently lost because of the bad channel quality, however, a series of spoof data messages may not cause the increment of sequence numbers to be larger than the heuristically calculated increment threshold of sequence numbers, resulting in miss detection. In Figure 4, 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  $n_a$ . Due to the bad channel quality, multiple spoof data messages can be lost during the transmission from  $n_m$  to  $n_a$ . Then,  $n_a$  may observe an increment of sequence numbers to be smaller than the heuristically calculated increment threshold, which results in a miss detection. In this analysis, we assume that the bad channel quality in terms of channel error primarily causes packet loss, and the channel error rate ( $r_{cer}$ ) is set to 10%.

Let  $P_{miss}$  be the average miss detection rate observed in the observation window, which can be expressed as

$$P_{miss} = 1 - \sum_{i=0}^{N_{atk}} P_{det}^i \cdot P_{atk}^i \quad (4)$$

where

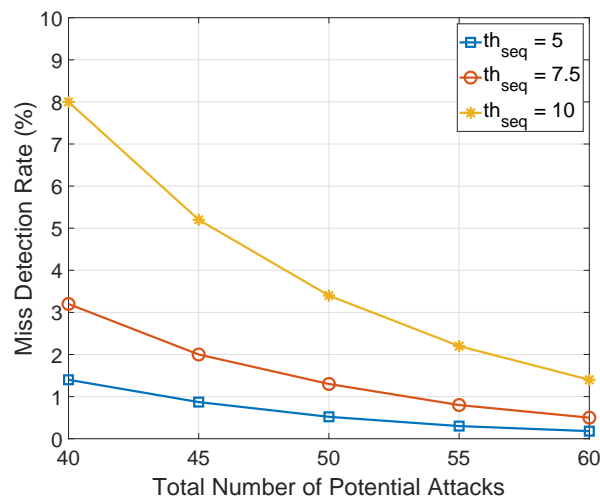
$$P_{atk}^i = \binom{i}{N_{atk}} \cdot R_{atk}^i \cdot (1 - R_{atk})^{N_{atk}-i} \quad (5)$$

$$P_{det}^i = \sum_{N_{lst}=0}^{N_{spf}^i - th_{seq}} \binom{N_{lst}}{N_{spf}^i} \cdot r_{cer}^{N_{lst}} \cdot (1 - r_{cer})^{N_{spf}^i - N_{lst}} \quad (6)$$

$$N_{spf}^i = N_{spkt} \cdot i \quad (7)$$

Here,  $N_{atk}$  is the total number of times that the malicious node decides whether to perform suppression attack and broadcast a series of spoof data messages,  $R_{atk}$  is the suppression attack rate, and  $N_{lst}$  is the number of spoof data messages that get lost during transmission due to bad channel quality,  $N_{spkt}$  is the number of spoof data messages broadcasted by malicious node in each attack, and  $th_{seq}$  is the heuristically calculated increment threshold of sequence numbers.  $N_{spf}^i$  is the number of spoof data messages broadcasted by malicious node during the  $i$  number of suppression attacks.  $P_{atk}^i$  is the probability that the malicious node performs the  $i$  number of suppression attacks during the observation window.  $P_{det}^i$  is the detection rate of the  $i$  number of suppression attacks.

In Figure 6, we show a numerical result of the impact of the total number of times that the malicious node decides whether to perform suppression attack  $N_{atk}$  and the heuristically calculated increment threshold of sequence numbers  $th_{seq}$  on the average miss detection rate based on the aforementioned analyses. Here, we assume the length of observation window is 50 s. As shown in Figure 6, when  $th_{seq}$  decreases, the miss detection rate decreases significantly. This is because the malicious node broadcasts a large number of spoof data messages and causes the minimum sequence number to increase greatly, and these multicasting misbehaviors can be easily detected with a smaller  $th_{seq}$ . As  $N_{atk}$  increases, the malicious node has more chances to perform suppression attack and multicast a series of spoof data messages within the observation window, which makes the minimum sequence number increase quickly, thus, the HED can easily compare the significant increment of a sequence number with the heuristically calculated  $th_{seq}$  to detect multicasting misbehaviors.



**Figure 6.** Miss detection rate against the total number of times that the malicious node decides whether to perform suppression attack.

## 5. Performance Evaluation

### 5.1. Simulation Testbed

We conduct simulation experiments using OMNeT++ [14] to evaluate the performance of the proposed approach. A  $150 \times 150 \text{ m}^2$  square network area is considered, where 51 nodes including single source node are placed using a random uniform distribution. 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/s 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 [40]. The channel error rate is set to 10%. We assume that the source node is always trusted, and 2–10% 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/s, and the number of spoof data messages in each attack is 10 or 15. The total simulation time is 10,000 s. The simulation parameters are summarized in Table 1.

**Table 1.** Simulation parameters.

Parameter	Value
Network Area	$150 \times 150 \text{ m}^2$
Number of Nodes	51
Communication Range	30 m
Packet Injection Rate	0.1 packet/s
Packet Size	40 bytes
Radio Data Rate	250 Kbps
Channel Error Rate	10%
Number of Malicious Nodes	1 to 5
Suppression Attack Rate	0.0125 to 0.1 time/s
Number of Spoof Data Messages	10 and 15
Simulation Time	10,000 s

In this paper, we measure the performance in terms of the following four major performance metrics by altering some key simulation parameters, including suppression attack rate, number of malicious nodes, observation window ( $\omega$ ), number of spoof data messages ( $N_{spkt}$ ), and filter gain constant ( $\alpha$ ). First, the detection rate is computed as the ratio of the number of detected multicasting misbehaviors to the total number of launched multicasting misbehaviors. The objective is to show the detection efficiency of the proposed scheme. Second, the packet reception rate (PRR) is calculated as the ratio of the number of received data messages to the total number of generated data messages from source node, indicating the performance resiliency of the proposed scheme. Third, a false detection rate, namely false positive rate, measures the ratio of the number of anomalous increment of sequence number due to a sudden increase of packet injection rate to the total number of detected multicasting misbehaviors. Fourth, the change of increment rate of minimum sequence number is observed and offers an explanation of how the increment rate has changed due to the multicasting misbehaviors of malicious nodes. For performance comparison, we compare the proposed HED scheme with the standard MPL multicast protocol with and without adversary, respectively.

### 5.2. Simulation Results and Analysis

**Detection Rate:** First, we measure the detection rate against suppression attack rate, number of malicious nodes and  $N_{spkt}$  in Figure 7. Overall, the detection rate of HED can be maintained above 90%. In Figure 7a, 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.

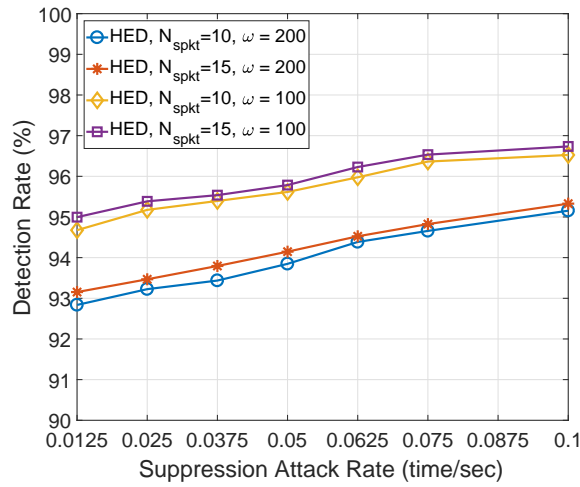
As shown in Figure 7b, the detection rate of HED is not sensitive to the number of malicious nodes. The HED is a stand-alone approach [18] where the same detection scheme is running on each node but no information is exchanged for detection. Thus, each neighbor node of malicious node can record the multicast operations of malicious node and detect the potential multicasting misbehaviors. However, the detection rate is responsive to the length of the observation 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.

**Packet Reception Rate (PRR):** Second, the packet reception rate (PRR) is measured against suppression attack rate, number of malicious nodes, and simulation time in Figure 8, in which the MPL without adversary provides the highest PRR, around 90%, and it is used as the upper bound of PRR. In Figure 8a, as the suppression attack rate varies between 0.0125 and 0.1 time/s, 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 because 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 messages 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.

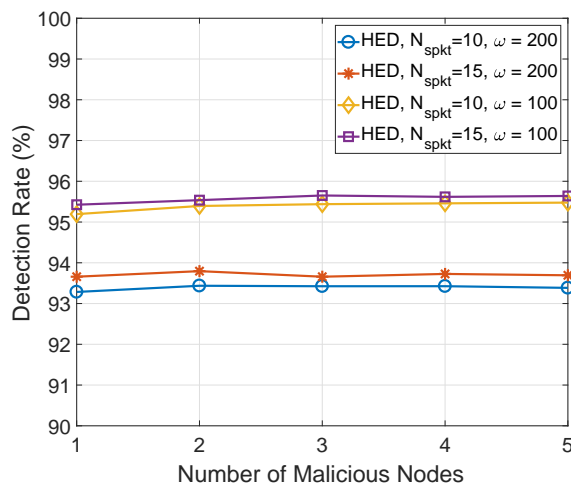
As shown in Figure 8b, when the number of malicious nodes increases, the PRR of MPL under suppression attack decreases. This is because more number of malicious nodes can launch more multicasting misbehaviors, and more valid data messages from source node will be rejected. However, the HED provides much 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. In Figure 8c, as the simulation time elapses, the PRR of both MPL under the suppression attack and HED fluctuate around 77% and 30%, respectively. However, the PRR of both MPL under the suppression attack and HED are sensitive to the number of spoof data messages  $N_{spkt}$ , and lower PRR is observed with larger  $N_{spkt}$ . This is because the minimum sequence number increases greatly and quickly with larger  $N_{spkt}$ , and fewer data messages will be accepted.

**False Detection Rate:** Third, the false detection rate is measured by varying suppression attack rate, number of malicious nodes, and  $N_{spkt}$  in Figure 9. Overall, the false detection rate of HED is below 6.5%. In Figure 9a, the false detection rate of HED decreases as the suppression attack rate increases. With larger suppression attack rate, the malicious node can show multicasting misbehaviors more frequently. However, these multicasting misbehaviors can be detected by the proposed scheme, resulting in lower false detection rate. When a short observation window is adopted, a lower false detection rate is achieved because each node can frequently compare the increment of a sequence number with threshold value to detect more multicasting misbehaviors. In Figure 9b, the false detection

rate remains steady as the number of malicious nodes increases. However, the HED with smaller observation window and larger  $N_{spkt}$  achieves the lowest false detection rate.

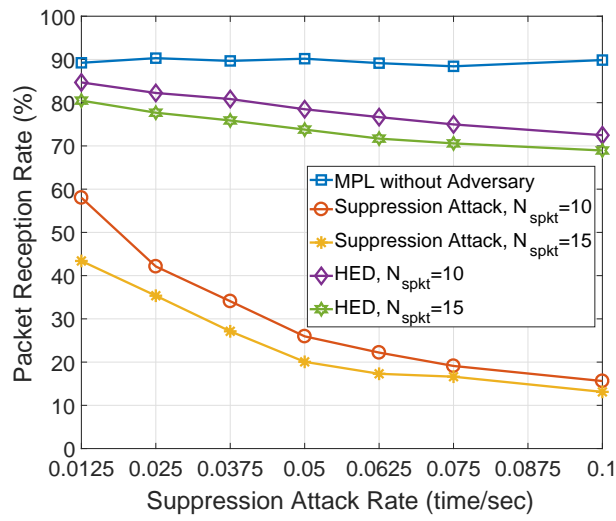


(a) Detection Rate vs. Attack Frequency

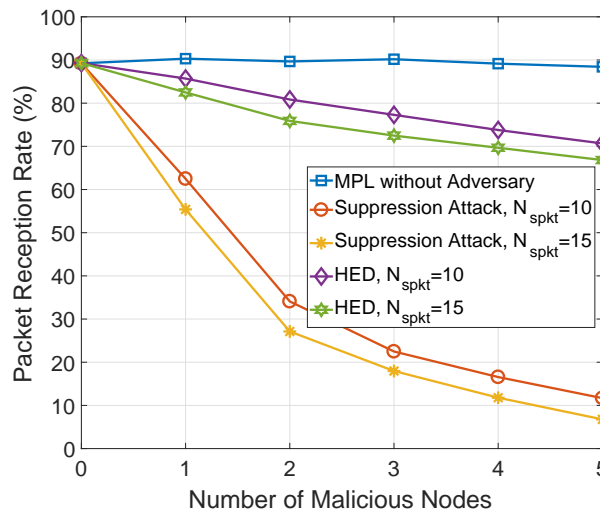


(b) Detection Rate vs. Number of Adversary

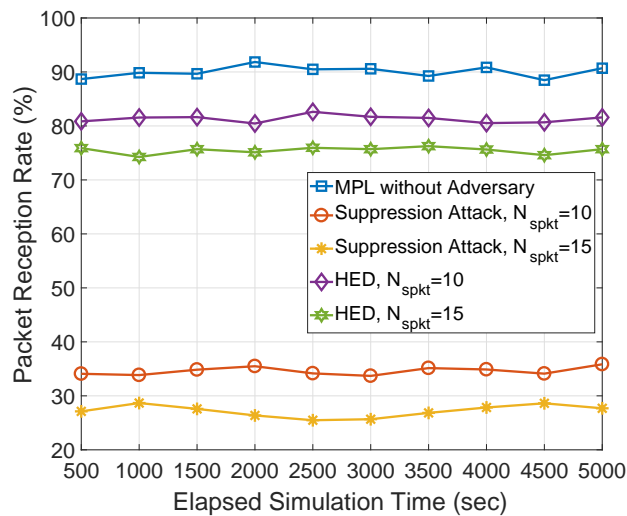
Figure 7. The detection rate against suppression attack rate and number of malicious nodes.



(a) Packet Reception Rate vs. Attack Frequency

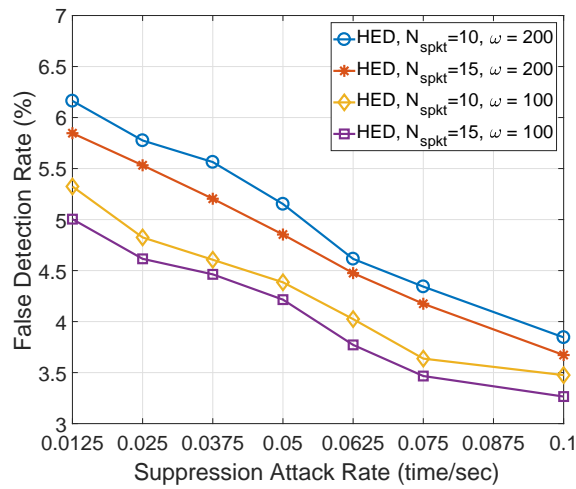


(b) Packet Reception Rate vs. Number of Adversary

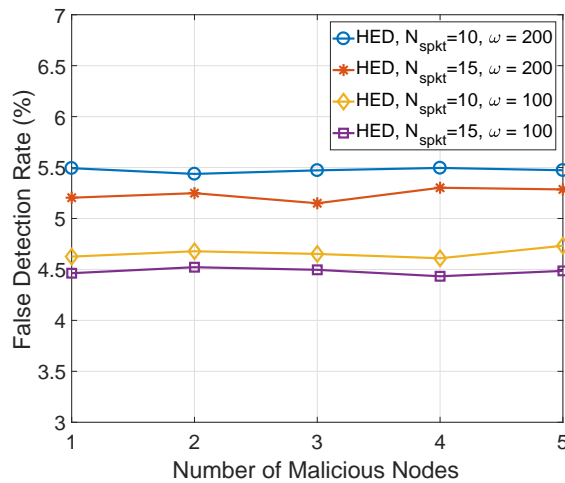


(c) Packet Reception Rate vs. Elapsed Simulation Time

**Figure 8.** The packet reception rate (PRR) against suppression attack rate, number of malicious nodes, and elapsed simulation time.



(a) False Detection Rate vs. Attack Frequency

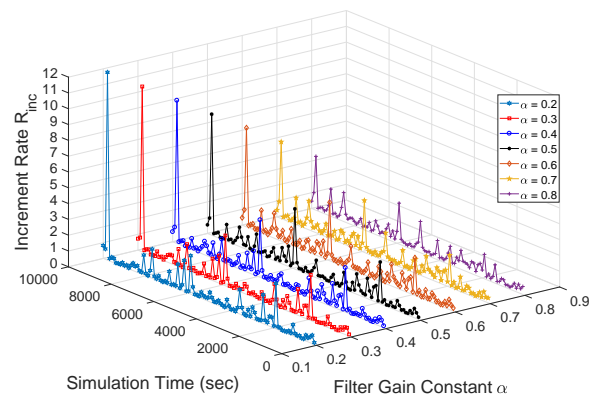


(b) False Detection Rate vs. Number of Adversary

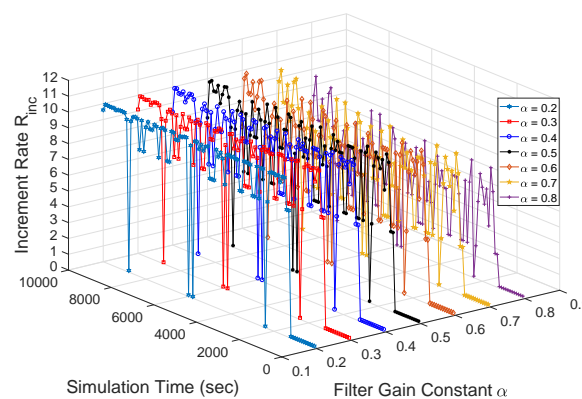
Figure 9. The false detection rate against suppression attack rate and number of malicious nodes.

**Changes of Increment Rate:** Finally, we measure the changes of the increment rate without and with adversary against simulation time and a filter gain constant  $\alpha$  in Figure 10. Since a low packet rate is adopted, the increment rate of the sequence number without adversary fluctuates below 2 seq/s. Due to exponential distribution of the packet rate, it is possible to have a sudden increase of packet rate at the source node, that in turn, leads to a high increment rate. However, as shown in Figure 10a, the sudden increase of a packet rate resulting in high increment rate is very rare. Under the suppression attack, the malicious node can multicast a series of spoof data messages within a short period of time and thus, a higher increment rate is observed as shown in Figure 10b. As the value of a filter gain constant increases, the increment rate slightly decreases because the recently calculated increment rate of a sequence number contributes less weight according to Equation (1).





(a) Increment Rate Without Adversary



(b) Increment Rate With Adversary

**Figure 10.** Changes of increment rate of minimum sequence number ( $R_{inc}$ ) against simulation time and filter gain constant  $\alpha$ .

## 6. Discussion

In this section, we first analyze and compare the suppression attack with well-known jamming attack in terms of attack method, stealthiness, attack energy efficiency, and level of denial of service. Then, we further explore design issues and extensions of HED for future research.

The basic idea of suppression attack is that a malicious node multicasts a series of spoof data messages with continuous sequence number to increase the minimum sequence number stored in the Seed Set, which can prevent the legitimate nodes from accepting valid data messages and cause them to delete the cached data messages. For jamming attack, a malicious node needs to continually transmit a radio signal to block any legitimate access to the medium and interfere with reception. Compared to the jamming attack, the suppression attack is much stealthier. This is because the malicious node acts as a normal node but multicasts a limited number of data messages to legitimate nodes to increase the minimum sequence number stored in the Seed Set, which can cause the legitimate nodes to reject valid data messages by themselves. In addition, the suppression attack has lower energy consumption compared to that of jamming attack because the less number of attack packets (e.g., spoof data messages) are generated and multicasted by malicious node in the suppression attack. However, the jamming attack has to continually broadcast a radio signal, consuming more energy. The suppression attack makes all one-hop neighbor nodes reject valid data messages and delete the cached data messages. Thus, the valid data messages cannot be transmitted and shared further in the network. Eventually, the suppression attack can lead to an extremely severe denial of service in MPL-based LLNs.

In the HED, each node individually monitors the malicious node to detect the potential multicasting misbehaviors. Similar passive monitoring-based approaches are also found in [41,42]. Since the detection rate highly depends on how many spoof data messages are received from a single malicious node, it can be significantly reduced if multiple malicious nodes collude together. Inspired by the camouflage-based detection approach [15], in which each node pretends not to overhear on-going communication but monitors the forwarding behavior of its adjacent nodes to detect a deep lurking malicious node, we plan to extend the HED by deploying an active detection approach. The basic idea of active detection is that each legitimate node hides the information of MPL control messages, counts the number of forwarding misbehaviors, and rejects certain number of data messages from malicious node with a large number of forwarding misbehaviors.

## 7. Concluding Remarks

In this paper, we present and analyze the suppression attack with a preliminary result 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 propose 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 but low false detection rate. Thus, the proposed scheme is 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 in an indoor office environment to see the full potential of the proposed countermeasure.

**Author Contributions:** Conceptualization, C.P.; Methodology, C.P.; Simulation, C.P.; Validation, C.P.; Formal Analysis, C.P.; Mathematical Analysis, X.Z.; Writing—Original Draft Preparation, C.P.; Writing—Review and Editing, C.P.; Supervision, C.P.; Project Administration, C.P.; and Funding Acquisition, C.P.

**Funding:** 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.

**Acknowledgments:** The authors would like to thank Dr. Sunho Lim for proofreading the conference version of this paper, which greatly improves the paper's consistency and readability. The authors would also like to thank anonymous reviewers of The 43rd IEEE Conference on Local Computer Networks (LCN) for their useful criticisms and constructive suggestions on the version of conference short paper, which undoubtedly have resulted in a stronger volume of the journal version.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Palattella, M.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 510–527. [CrossRef]
2. Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent From 2016. 2017. Available online: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016> (accessed on 26 September 2018).
3. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
4. Hui, J.; Kelsey, R. Multicast Protocol for Low-Power and Lossy Networks (MPL). RFC Stand. 7731; 2016. Available online: <https://www.rfc-editor.org/info/rfc7731> (accessed on 26 September 2018).
5. Kim, H.; Ko, J.; Culler, D.; Paek, J. Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2502–2525. [CrossRef]

6. IEEE Standards Association. *802.15.4-2011—IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*; IEEE Standards Association: Piscataway, NJ, USA, 2011.
7. Cisco Connected Grid Security for Field Area Network, January 2012. Available online: [https://www.cisco.com/c/dam/en\\_us/solutions/industries/docs/energy/C11-696279-00\\_cgs\\_fan\\_white\\_paper.pdf](https://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/C11-696279-00_cgs_fan_white_paper.pdf) (accessed on 26 September 2018).
8. Challa, S.; Wazid, M.; Das, A.; Kumar, N.; Reddy, A.; Yoon, E.; Yoo, K. Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE Access* **2017**, *5*, 3028–3043. [[CrossRef](#)]
9. Sehgal, A.; Perelman, V.; Kuryla, S.; Schonwalder, J. Management of Resource Constrained Devices in the Internet of Things. *IEEE Commun. Mag.* **2012**, *50*, 144–149. [[CrossRef](#)]
10. Sehgal, A.; Mayzaud, A.; Badonnel, R.; Chriment, I.; Schnwlder, J. Addressing DODAG Inconsistency Attacks in RPL Networks. In Proceedings of the Global Information Infrastructure and Networking Symposium (GIIS), Montreal, QC, Canada, 15–19 September 2014; pp. 1–8.
11. Tsao, T.; Alexander, R.; Dohler, M.; Daza, V.; Lozano, A.; Richardson, M. A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). RFC Stand. 7416. 2015. Available online: <https://www.rfc-editor.org/info/rfc7416> (accessed on 26 September 2018). [[CrossRef](#)]
12. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 245–257. [[CrossRef](#)]
13. Pu, C.; Zhou, X.; Lim, S. Mitigating Suppression Attack in Multicast Protocol for Low Power and Lossy Networks. In Proceedings of the IEEE 43rd Conference on Local Computer Networks LCN, Chicago, IL, USA, 1–4 October 2018.
14. Varga, A. OMNeT++, 2014. Available online: <http://www.omnetpp.org/> (accessed on 15 March 2018).
15. Pu, C.; Lim, S. Spy vs. Spy: Camouflage-based Active Detection in Energy Harvesting Motivated Networks. In Proceedings of the IEEE Military Communications Conference (MILCOM), Tampa, FL, USA, 26–28 October 2015; pp. 903–908.
16. Pu, C.; Lim, S.; Jung, B.; Chae, J. EYES: Mitigating Forwarding Misbehavior in Energy Harvesting Motivated Networks. *Elsevier Comput. Commun.* **2018**, *124*, 17–30. [[CrossRef](#)]
17. Pu, C.; Lim, S.; Byungkwan, J.; Manki, M. Mitigating Stealthy Collision Attack in Energy Harvesting Motivated Networks. In Proceedings of the IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 575–580.
18. Pu, C.; Lim, S. A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation. *IEEE Syst. J.* **2016**, *12*, 834–842. [[CrossRef](#)]
19. Cui, B.; Yang, S. NRE: Suppress Selective Forwarding Attacks in Wireless Sensor Networks. In Proceedings of the IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 229–237.
20. Pu, C.; Lim, S.; Jinseok, C.; Byungkwan, J. Active Detection in Mitigating Routing Misbehavior for MANETs. *Wirel. Netw.* **2017**. [[CrossRef](#)]
21. Yang, X.; Lin, J.; Yu, W.; Moulema, P.; Fu, X.; Zhao, W. A Novel En-Route Filtering Scheme Against False Data Injection Attacks in Cyber-Physical Networked Systems. *IEEE Trans. Comput.* **2015**, *64*, 4–18. [[CrossRef](#)]
22. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [[CrossRef](#)]
23. Dvir, A.; Holczer, T.; Buttyan, L. VeRA-Version Number and Rank Authentication in RPL. In Proceedings of the IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, Spain, 17–22 October 2011; pp. 709–714.
24. Winter, T.; Thubert, P. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC Stand. 6550; 2012. Available online: <https://www.rfc-editor.org/info/rfc6550> (accessed on 26 September 2018).
25. Le, A.; Loo, J.; Lasebae, A.; Vinel, A.; Chen, Y.; Chai, M. The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks. *IEEE Sens. J.* **2013**, *11*, 3685–3692. [[CrossRef](#)]
26. Heo, J.; Kim, J.; Bahk, S.; Paek, J. Dodge-Jam: Anti-Jamming Technique for Low-Power and Lossy Wireless Networks. In Proceedings of the 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), San Diego, CA, USA, 12–14 June 2017; pp. 1–9.
27. Perazzo, P.; Vallati, C.; Anastasi, G.; Dini, G. DIO Suppression Attack Against Routing in the Internet of Things. *IEEE Commun. Lett.* **2017**, *21*, 2524–2527. [[CrossRef](#)]

28. Pu, C.; Hajjar, S. Mitigating Forwarding Misbehaviors in RPL-based Low Power and Lossy Networks. In Proceedings of the 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018; pp. 1–6.
29. Pu, C. Mitigating DAO Inconsistency Attack in RPL-based Low Power and Lossy Networks. In Proceedings of the IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 570–574.
30. Pu, C.; Song, T. Hatchetman Attack: A Denial of Service Attack Against Routing in Low Power and Lossy Networks. In Proceedings of the 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Shanghai, China, 22–24 June 2018; pp. 12–17.
31. Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2661–2674. [[CrossRef](#)]
32. Beigi-Mohammadi, N.; Mistic, J.; Khazaei, H.; Mistic, V.B. An Intrusion Detection System for Smart Grid Neighborhood Area Network. In Proceedings of the IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 4125–4130.
33. Hummen, R.; Hiller, J.; Wirtz, H.; Henze, M.; Shafagh, H.; Wehrle, K. 6LoWPAN Fragmentation Attacks and Mitigation Mechanisms. In Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, Budapest, Hungary, 17–19 April 2013; pp. 55–66.
34. Sajjad, S.M.; Yousaf, M. Security analysis of IEEE 802.15. 4 MAC in the context of Internet of Things (IoT). In Proceedings of the Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, June 2014; pp. 9–14.
35. Kasinathan, P.; Pastrone, C.; Spirito, M.A.; Vinkovits, M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In Proceedings of the IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 7–9 October 2013; pp. 600–607.
36. Rghioui, A.; Khannous, A.; Bouhorma, M. Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition. *J. Adv. Comput. Sci. Technol.* **2014**, *3*, 143–152. [[CrossRef](#)]
37. Levis, P.; Clausen, T. The Trickle Algorithm. RFC Stand. 6206; 2011. Available online: <https://www.rfc-editor.org/info/rfc6206> (accessed on 26 September 2018).
38. Zhao, J. On Resilience and Connectivity of Secure Wireless Sensor Networks Under Node Capture Attacks. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 557–571. [[CrossRef](#)]
39. Abdallah, A.; Shen, X. Efficient Prevention Technique for False Data Injection Attack in Smart Grid. In Proceedings of the IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
40. Boulis, A. Castalia. 2014. Available online: <http://castalia.forge.nicta.com.au> (accessed on 15 February 2018).
41. Marti, S.; Giuli, T.J.; Lai, K.; Baker, M. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6–11 August 2000; pp. 255–265.
42. Shila, D.M.; Yu, C.; Anjali, T. Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs. *IEEE Trans. on Wirel. Commun.* **2010**, *9*, 1661–1675. [[CrossRef](#)]

