A Theil Index-Based Countermeasure Against Advanced Vampire Attack in Internet of Things

Cong Pu Jacqueline Brown Logan Carpenter
Department of Computer Sciences and Electrical Engineering
Marshall University
Huntington, WV 25755, USA
Email: {puc, brown1062, carpenter190}@marshall.edu

***Abstract*—In the last decade, design, development, and advancement in embedded processing, sensing, and wireless communication have fueled the emergence of Internet of Things (IoT), where various smart devices communicate and cooperate with each other and existing communication systems to achieve the goal of sharing information and coordinating decisions. Meanwhile, IPv6-based Low Power and Lossy Network (LLN), which is a major building block of IoT, has attracted a fair amount of attention for all sorts of IoT applications and deployments. In order to provide IPv6 connectivity to an enormous number of resource-constrained smart devices in IoT environment, an efficient routing protocol for IPv6-based LLNs, also widely known as RPL, has been standardized. However, RPL lacks security protection and is vulnerable to various Denial-of-Service (DoS) attacks. In this paper, we first present an advanced vampire attack, which is a novel routing layer specific service disruption and resource exhaustion attack, against RPL in IPv6-based LLNs. Then we propose a Theil index-based countermeasure to effectively detect and mitigate advanced vampire attack. The basic idea of the proposed Theil index-based countermeasure is that each node measures the distribution of destination MAC addresses in the received data packets to detect advanced vampire attack. Through experimental study, the effectiveness of the Theil index-based countermeasure is validated, indicating a viable approach against advanced vampire attack in the IoT.**

***Index Terms*—Internet of Things (IoT), RPL, Advanced Vampire Attack, Theil Index**

I. Introduction

The on-going miniaturization of electronic devices (later nodes) and the maturation of wireless communication technologies provide a solid foundation for the emergence and development of Internet of Things (IoT), where a variety of multi-sized and heterogeneous nodes seamlessly interact and collaborate with each other to achieve common goals [1]. These smart and connected devices can cater to a variety of civilian and military IoT applications like smart grid [2], smart transportation [3], smart city [4], smart home [5], etc. Due to the huge economic impact and business value of IoT, not surprisingly that tech giants like Amazon (AWS IoT), Microsoft (Azure IoT), Google (Google Cloud IoT), Huawei (Huawei IoT), and Cisco (Cisco Kinetic) have rapidly proliferated in business and industrial IoT application market in the last few years. The revolution brought by the IoT technology has been compared to the building of complex transportation system including roads, rail, canals and underground during the industrial revolution in the period of 1700-1900, and is expected to enhance information accessibility and availability as well as improve our life further [6], [7].

In this context, IPv6-based Low Power and Lossy Networks (LLNs) are rapidly proliferating and leading to the further development of IoT applications. However, IoT applications usually consist of a large number of resource-constrained devices that require light-weight, energy-efficient, and scalar communication, which can only be accomplished by means of routing protocol for Quality of Service (QoS) provisioning [8]. To meet these demands and requirements, a novel routing protocol for LLNs, also referred to as *RPL* [9], has been proposed by Internet Engineering Task Force (IETF) Working Group. Thanks to its tree-based network structure suitable for data collection and its ability to use IPv6 base addressing to perform interoperability with other Internet devices, RPL has became the most adequate routing protocol for LLNs and IoT applications since it came into being [10]. On the other hand, due to the lack of security mechanisms for internal attacks in RPL [11], LLNs are particularly vulnerable to a specific Denial-of-Service (DoS) attack, which can not only cause data packet losses, but also drain nodes' limited battery energy. This specific attack is coined with the name *advanced vampire attack*. Unlike traditional vampire attack [12], where an adversary only amplifies the cumulative network energy consumption, the advanced vampire attack can disrupt immediate service availability as well as permanently disable the entire network.

In this paper, we propose a Theil index-based countermeasure to effectively detect and mitigate advanced vampire attack in RPL, where an adversary manipulates the received data packet with fictitious and unreachable destination to induce legitimate intermediate node to drop the tampered data packet and reply error message. The basic idea of the proposed countermeasure is to measure the distribution of destination MAC addresses in the received data packets to detect whether there is an advanced vampire attack based on Theil index theory [13]. If so, the attack mitigation procedure will be triggered to immediately eliminate advanced vampire attack. We develop a customized discrete event-driven simulation framework using OMNeT++ [14] and evaluate its performance

978-1-7281-4846-5/20/$31.00 ©2020 IEEE

through extensive simulation experiments in terms of detection rate and cumulative energy consumption. We also revisit two prior approaches, route examination-based mechanism [12] and error message forwarding rate-based mechanism [15], and modify them to work in the simulation framework for performance comparison. The simulation results indicate that the proposed Theil index-based countermeasure is a viable detection approach against advanced vampire attack.

The rest of the paper is organized as follows. Section II presents and analyzes the existing and relevant literature. The RPL routing protocol and advanced vampire attack with preliminary result are provided in Section III. Section IV focuses on the proposed Theil index-based countermeasure. Extensive simulation experiments and results are provided and analyzed in Section V. Finally, concluding remarks with future research direction are provided in Section VI.

II. Related Work

In this section, we review and analyze the existing literature on security mechanisms and features to secure RPL in the context of Internet of Things.

In [15], a DAO forwarding rate-based approach is proposed to address a DAO insider attack in RPL, where an adversary periodically sends fictitious DAO control messages to its parent nodes to affect energy consumption, latency, and reliability of the entire network. The basic idea is that each parent node associates a counter with every child node in its sub-DODAG. When the number of forwarded DAOs for a child node exceeds a pre-specified threshold, the parent discards any DAO message carrying the prefix of the respective child. However, the proposed countermeasure cannot efficiently detect the DAO insider attacker who dynamically changes malicious traffic patterns or mimic realistic DAO traffic patterns to remain undetected. The [16] investigates RPL version number attack and presents a couple of lightweight mitigation techniques in LLNs. The first mitigation technique eliminates the malicious version number updates which may come from the strongest attacking positions in the network. The second mitigation technique makes use of a trust mechanism in addition to the first scheme and promises a complete solution to version number attack. But, if adversaries also exist in the neighbor nodes and perform bad-mouthing attack, the proposed mitigation techniques are likely to fail.

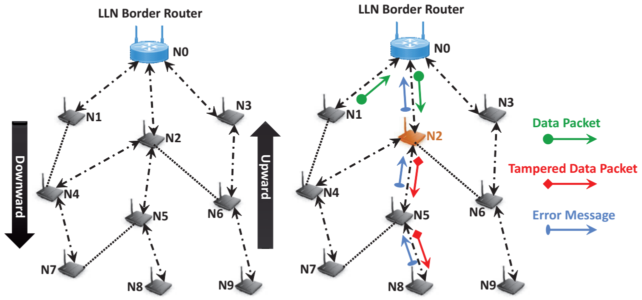
The [17] builds power-positive networking and uses it to dispatch energy DoS threat. Through building communications on wireless charging signals, the proposed lightweight approach can replenish the receiving node's energy and thwart energy DoS attack from its vulnerability surface. In [18], an address shuffling algorithm integrated with keyed-hash message authentication code is designed to protect IoT devices and their applications from privacy leaks, where attackers can infer network topology and learn what the node functionalities are without compromising system. The proposed approach enables a controlled and collision-free MAC address shuffling, and only the legitimate nodes and network controller are able to predict the MAC address renew outcomes. A key synchronizing algorithm for chaining cipher encryption [19] is proposed for LPWAN IoT networks, where a random number generator is incorporated in the synchronization algorithm, and a hashing method is used to regenerate the key. The authors in [20] model sybil attack using artificial bee colony algorithm and then propose an intrusion detection algorithm against sybil attack in the Internet of Things. Since sybil attack is a population-based attack and the foraging behavior of fictitious identities is similar to the foraging behavior of honey bees, sybil attack is modeled into five phases, namely initialization phase, fitness factor computation, compromising or fabricating phase, contagious phase, and hive selection and launching phase. To detect sybil attack, three new variables, namely nonce ID, control message counter, and timestamps, are added in the DODAG Information Object (DIO) control message. The nonce ID is allocated to each node when it joins the network, and also broadcasted with unique DODAG ID to the neighbor nodes. If the nonce ID and DODAG ID in the received message do not match with the previous record, there is a potential possibility of sybil attack. Control message counter and timestamps is used to track the number of received control messages and the time of arrival of received control messages to detect the sign of sybil attack, respectively.

The [21] proposes a misbehavior-aware detection scheme against energy depletion attack in RPL-based LLNs. In [22], a security mechanism, named micro moving target IPv6 defense, is proposed to secure low power and low resource devices utilized for IoT applications. The basic idea is to rotate IPv6 addresses based on the use of a lightweight hashing algorithm. In [23], a stealthy collision attack is investigated in energy harvesting motivated networks. In [24], a survey on the most promising techniques proposed so far to defend ad hoc networks from sybil attack is presented. In addition, an overview of the state of the art of routing attacks and mitigation techniques for RPL-based IoT is presented in [25].

In summary, various countermeasures have been well studied to defend against various attack in the IoT. However, to the best of our knowledge, there is no comprehensive detection and mitigation of advanced vampire attack.

III. RPL Overview and Advanced Vampire Attack

RPL is an IPv6-based proactive distance vector routing protocol designed for low power and lossy networks, driven by the unique characteristics of those networks, such as the limited memory, computing, and power resources, low data rate, and unstable wireless links. The entire network is organized into one or more Destination Oriented Directed Acyclic Graphs (DODAGs), where each DODAG comprises of a set of normal nodes and is rooted at the LLN Border Router (LBR), as shown in Subfig. 1(a). The LBR acts as a gateway between the Internet and LLN. To construct a DODAG and build upward routes, the LBR issues a DODAG Information Object (DIO) control message. Any node that receives the DIO message and is willing to join the DODAG will add the sender address to its parent list, calculate its own network rank, select its preferred parent node from parent list, finally pass on the DIO message



(a) RPL with a Single DODAG (b) Advanced Vampire Attack

Fig. 1. A snapshot of the network. (a): A RPL network with a single DODAG. (b): An example of advanced vampire attack, where $N2$ is an adversary.

with its own rank information. If a node is willing to advertise itself as a reachable destination from the LBR point of view, it unicasts a Destination Advertisement Object (DAO) control message recording the nodes visited along the upward routes. In order to save memory storage, nodes do not store routing information to any destination node except for the LBR. Thus, when a node wants to send a data packet to another node within the DODAG, the data packet must be first sent through the upward route to the LBR, which will piggyback the source route of the destination node in the packet header and forward the data packet to the next hop. Any intermediate node who receives the data packet will simply inspect the source route and determine which node it should forward the data packet to. If an intermediate node fails to forward the data packet with the piggybacked source route, it immediately drops the data packet and replies an error message back to the LBR.

Due to the absence of security features, however, RPL is not immune to advanced vampire attack. The goal of advanced vampire attack is to cause legitimate intermediate nodes to drop the received data packets and reply error messages back to the LBR, which can lead to two consequences. First, immediate service availability is seriously disrupted because an excessive number of data packets are dropped by legitimate nodes. Second, the entire network could be disabled permanently because each intermediate node along the forwarding path has to receive and forward a large number of error messages back to the LBR, which significantly exhausts nodes' limited battery energy. For example, suppose that node $N1$ wants to send a data packet to destination node $N8$ as shown in Subfig. 1(b). The data packet will be first sent through the upward route to the LBR ($N0$), which will attach the source route, $[N0,N2,N5,N8]$, to the packet header, and forward the data packet, $pkt[N0,N2,N5,N8]$, to destination $N8$. When the adversary $N2$ receives the data packet, it manipulates the piggybacked source route by replacing all the post-hops (i.e., $N8$) of the target node (i.e., $N5$) with unreachable destination (i.e., $N^{\otimes}$), and then sends the tampered data packet (i.e., $pkt^{*}[N0,N2,N5,N^{\otimes}]$) to the target node (i.e., $N5$). When $N5$ receives the tampered data packet, $pkt^{*}[N0,N2,N5,N^{\otimes}]$, it has to drop the packet because it cannot forward the data packet to next hop node, which is unreachable destination. In addition, $N5$ will reply an error message back to the LBR to report the forwarding error. Here, $N^{\otimes}$ is the fictitious node address and does not exist in the network.

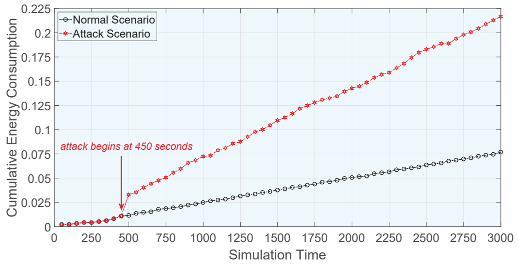


Fig. 2. Cumulative Energy Consumption (joule) vs. Simulation Time (sec).

In Fig. 2, we measure the cumulative energy consumption under various scenarios. As the simulation time elapses, the cumulative energy consumption of normal scenario is increasing slowly and linearly. This is because the intermediate nodes along the forwarding path regularly receive and forward a small amount of data packets to the LBR, the total energy consumption experiences normal increment. As expected, the advanced vampire attack causes excessive energy usage for the entire network. After the advanced vampire attack begins at 450 seconds, the cumulative energy consumption of the network significantly increases as the simulation time elapses. When the simulation ends, the total energy consumption of attack scenario is about 3 times than that of normal scenario. Since a large number of tampered data packets with fictitious destination MAC address cause intermediate nodes to reply a mass of error messages, each intermediate node has to receive and forward more error messages, which results in a significant amount of energy consumption.

IV. The Proposed Theil Index-Based Approach

In Theil index-based countermeasure, each node records the destination MAC address of each received data packet, measures the evenness or randomness of the distribution of destination MAC addresses, and then detect whether advanced vampire attack exists in the network. If that is the case, the attack mitigation procedure will be triggered to eliminate the attack. The countermeasure is designed based on Theil index theory [13], which can be viewed as a measurement of non-evenness or non-randomness of samples among all classes. In particular, if the samples are evenly distributed among all classes, a higher Theil index value can be observed. However, a lower Theil index value indicates that the samples are not distributed evenly among all classes. When an adversary launches an advanced vampire attack, it randomly generates the fictitious and unreachable destination MAC address to tamper the data packet. As a result, the evenness or randomness of the distribution of destination MAC addresses in data packets will increase significantly, and the Theil index value calculated using the destination MAC addresses increases abnormally, which can determine the existence of advanced vampire attack.

First, each intermediate node records the destination MAC address of the received data packet within a specific window (ω). When ω ends, the node calculates the Theil index value of destination MAC addresses according to

$$T_{eil} = \sum_{i=1}^{M} s_i \cdot T_{eil}^{i} + \sum_{i=1}^{M} s_i \cdot \ln \frac{\bar{x}_i}{\mu}. \quad (1)$$

In this paper, the entire MAC address space [1] (2^{24}) is equally divided into M groups. s_i is the share of destination MAC address of group i, and calculated as $s_i = \frac{D_i}{D} \cdot \frac{\bar{x}_i}{\mu}$. Here, D and D_i is the total number of destination MAC addresses among all groups and the total number of destination MAC address in group i, respectively. In addition, $\bar{x}_i$ is the average value of destination MAC addresses of group i, and μ is the average value of destination MAC addresses of all groups. T^i_{eil} is the Theil index value of group i, and represented as

$$T^i_{eil} = \frac{1}{D_i} \cdot \sum_{j=1}^{D_i} \frac{m_{ij}}{\bar{x}_i} \cdot \log \frac{m_{ij}}{\bar{x}_i}, \qquad (2)$$

where m_{ij} is the destination MAC address of the j^{th} packet in group i. Then, the node compares the calculated Theil index value of current window ω, T_{eil}, with the Theil index value of previous window ω^*, T^*_{eil}, according to

$$Atk(T_{eil}) = \begin{cases} 1, & \frac{T_{eil} - T^*_{eil}}{T^*_{eil}} > \Delta^{avg}_T \\ 0, & \frac{T_{eil} - T^*_{eil}}{T^*_{eil}} <= \Delta^{avg}_T \end{cases} \qquad (3)$$

Here, $Atk(T_{eil})$ = 1 indicates that the node detects advanced vampire attack. Δ^{avg}_T is an empirical threshold value updated by the low pass filter with a filter gain constant α,

$$\Delta^{avg}_T = \alpha \cdot \Delta^{avg}_T + (1 - \alpha) \cdot \Delta^{avg}_{T^*}, \qquad (4)$$

where $\Delta^{avg}_{T^*}$ is the threshold value in the previous window ω^*.

Second, once advanced vampire attack is detected, the attack mitigation procedure will be first triggered at the intermediate node who is the next hop of the suspected adversary to eliminate attack by reducing the number of accepted data packets from the adversary. In order to take into account the changing state of the network and react to varying attack patterns quickly, we propose to utilize an adaptive acceptance rate of data packets to determine how many new data packets should be accepted from the suspected adversary within next window ω. The acceptance rate of data packets γ^{pkt} is calculated as

$$\gamma^{pkt} = \delta + \varphi \cdot e^{1 - R^{det} \cdot \lambda}, \qquad (5)$$

where δ and φ are system parameters and δ is an asymptote to ensure that the γ^{pkt} never reach 0. λ has an impact on the change of γ^{pkt}, and a larger value for λ leads to a smaller γ^{pkt} being reached quicker generally. R^{det} is the accumulated detection rate of advanced vampire attack, and is calculated as $R^{det} = \frac{c_{atk}}{c_{win}}$, where c_{atk} is the total number of attack detection and c_{win} is the total number of elapsed windows. Major operations of the proposed Theil index-based countermeasure are summarized in Fig. 3.

```
Notations:
• $\omega$, $M$, $D$, $D_i$, $\bar{x}_i$, $\mu$, $T^i_{eil}$, $T_{eil}$, $T^*_{eil}$, $\Delta^{avg}_T$, $m_{ij}$, $s_i$, $R^{det}$, $c_{atk}$, $c_{win}$, $\delta$, $\varphi$, $\lambda$, and $\gamma^{pkt}$: Defined before.
• $pkt[N_{id}, data]$: A data packet containing a node ID ($N_{id}$).
• $MT_i$: A destination MAC address table at node $n_i$. Each entry consists of two components: destination MAC address ($N_{id}$) and timestamp ($T_{cur}$).
◇ When $N_i$ receives a data packet $pkt[N_j, data]$ from $N_j$:
  $MT_i$ = $MT_i \cup [N_j, T_{cur}]$;
◇ When the window period $\omega$ ends at $N_i$:
  for $i$ = 1 to $M$
    $T^i_{eil} = \frac{1}{D_i} \cdot \sum_{j=1}^{D_i} \frac{m_{ij}}{\bar{x}_i} \cdot \log \frac{m_{ij}}{\bar{x}_i}$;
  $T_{eil} = \sum_{i=1}^{M} s_i \cdot T^i_{eil} + \sum_{i=1}^{M} s_i \cdot \ln \frac{\bar{x}_i}{\mu}$;
  if $\frac{T_{eil} - T^*_{eil}}{T^*_{eil}} > \Delta^{avg}_T$
    $c_{atk}$ += 1;
  $R^{det} = \frac{c_{atk}}{c_{win}}$;
  $\gamma^{pkt} = \delta + \varphi \cdot e^{1 - R^{det} \cdot \lambda}$;
```

Fig. 3. The pseudocode of the proposed Theil index-based countermeasure.

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Network area	150×150 m^2
Number of root node	1
Number of normal nodes	8
Number of malicious nodes	1
Attack traffic	3-15 pkt/attack
Window size	30-90 seconds
Packet loss ratio	5%
Radio data rate	250 Kbps
Radio model	CC2420
Simulation time	3000 seconds

V. PERFORMANCE EVALUATION

To validate the effectiveness of the proposed countermeasure, we conduct a set of simulation experiments using OMNeT++ [14]. The network topology shown in Subfig. 1(b) is deployed in a 150×150 m^2 network area in the presence of a single attacker. To emulate the real radio used in LLNs, CC2420 (2.4 GHz IEEE 802.15.4 compliant RF transceiver) with an effective data rate of 250 Kbps is configured. The total simulation time is set to 3000 seconds, and each simulation scenario is repeated 10 times with different seed to obtain steady-state performance. We measure the performance in terms of detection rate and cumulative energy consumption by changing key simulation parameters, such as attack traffic and window size. In addition, we compare the proposed countermeasure with the route examination-based mechanism [12] and error message forwarding rate-based mechanism [15] for performance comparison and evaluation. The simulation parameters are summarized in Table I.

In Fig. 4, we measure the detection rate by varying attack traffic. Here, the attack traffic is the number of data packets piggybacked with randomly generated fictitious and unreachable destination MAC address per attack. When the

[1] Traditional MAC addresses are 48 bits. The leftmost 24 bits called a ”prefix” is associated with the manufacturer, which is assigned by the IEEE. The rightmost 24 bits of a MAC address represent a manufacturer-assigned identification number for the specific device [26].

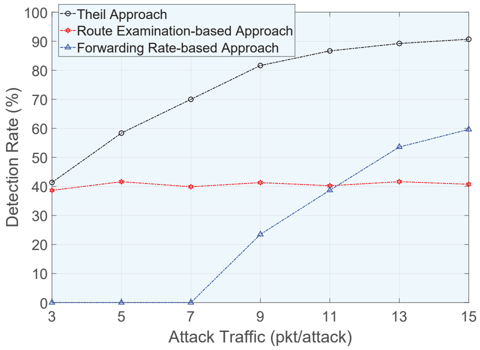


Fig. 4. The performance of detection rate against attack traffic.

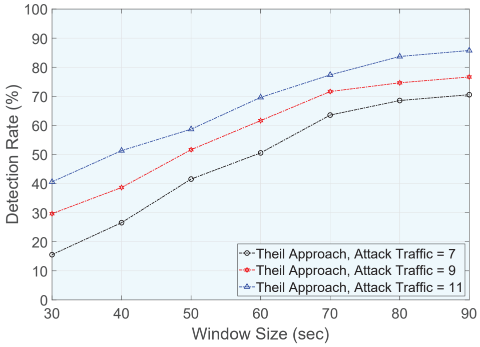


Fig. 5. The performance of detection rate against window size.

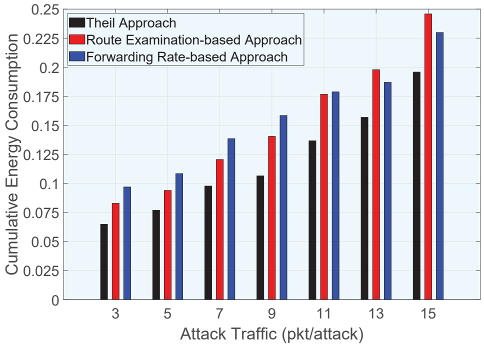


Fig. 6. The performance of cumulative energy consumption against attack traffic.

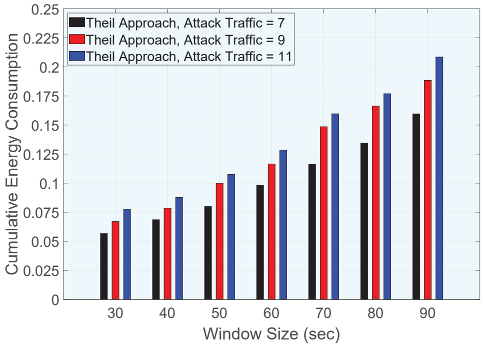


Fig. 7. The performance of cumulative energy consumption against window size.

attack traffic increases, the detection rate of Theil approach increases linearly. If the adversary sends more attack packets with randomly generated fictitious and unreachable destination MAC address when launching attack, more destination MAC addresses will be evenly and randomly distributed among the entire MAC address space, which causes the increment of Theil index value. As a result, more attacks can be detected according to Eq. (3), thus, the overall detection rate of Theil approach increases. The error message forwarding rate-based approach shows zero detection rate when the attack traffic is varying from 3 to 7. This is because the error message forwarding rate-based approach uses the threshold value to detect the potential attack. If the number of received error messages is less than the threshold value, the potential attack cannot be detected and zero detection rate is observed. However, when the attack traffic increases from 7 to 15, the detection rate of error message forwarding rate-based approach increases since more attacks can be detected due to a large number of error messages. The route examination-based approach is not sensitive to the change of attack traffic. Each node examines the destination MAC address piggybacked in the received data packets, if the destination MAC address falls in the legal MAC address space, it will not be treated as potential attack. Since the adversary randomly generates fictitious and unreachable destination MAC addresses, each node has around 50% chances to detect the attack.

In Fig. 5, we measure the detection rate by varying window size. As shown in Fig. 5, the detection rate of Theil approach is measured against window size. As the window size increases, the overall detection rate of Theil approach decreases. This is because more tampered data packets with fictitious and unreachable destination MAC address can be received within a larger window, thus, more attacks can be detected due to a large increase of Theil index value. When the attack traffic increases, a higher detection rate is observed. Since more tampered data packets with fictitious and unreachable destination MAC address will be sent to legitimate intermediate nodes with a larger attack traffic, the intermediate node can easily measure the changes of Theil index value to detect attacks.

In Fig. 6, as the number of tampered data packets per attack increases, the overall energy consumption of all three approaches increase. With a larger attack traffic, more tampered data packets with fictitious destination MAC address will be generated and sent to intermediate nodes, which causes them to generate and reply more error messages back to the LBR. As a result, each intermediate node has to receive and forward a large number of error messages, leading to a significant energy consumption. The Theil approach shows the lowest energy consumption because it can quickly detect the attack and reduce the number of accepted data packets from the suspected adversary. Thus, a less number of error messages will be generated and forwarded in the network, and energy consumption is reduced.

As shown in Fig. 7, as the window size increases, the overall energy consumption of Theil approach increases slowly. Since more tampered data packets will be received within a larger window, thus, more attacks can be detected and the number of accepted tampered data packets from the suspected adversary significantly decreases in the next window. However, the elapsed time of each window increases as the size of window increases. Thus, in the current window, a large number of tampered data packets still can be received by intermediate nodes, resulting in a large number of error messages and exhausts nodes' energy. When the attack traffic increases, a higher energy consumption is observed because more tampered data packets could be accepted by intermediate nodes.

VI. Discussion and Conclusion

In the proposed countermeasure, there is one major constraint that needs to be further discussed for possible future extensions. The approach is designed based on an assumption that the MAC addresses of all legitimate nodes in the network are assigned and centralized in one group only, rather than randomly distributing among all groups. Since the adversary does not know exactly how the MAC addresses of legitimate nodes are assigned, it only can use randomly generated fictitious and unreachable destination MAC address to create tampered data packet. As a result, the MAC addresses in the received tampered data packets randomly spread out in the entire MAC address space, which causes the Theil index value to increase significantly. However, if the MAC addresses of all legitimate nodes in the network are randomly assigned and distributed in the entire MAC address space, the proposed Theil-index based countermeasure probably cannot accurately detect advanced vampire attack because the Theil index value in normal and attack scenarios does not have significant difference.

In this paper, we proposed a Theil-index based countermeasure, which can efficiently detect and mitigate advanced vampire attack in LLNs running with RPL, where each node measures the distribution of destination MAC addresses in the received data packets to detect whether there is an advanced vampire attack based on Theil index theory. In addition, we conducted simulation experiments to validate the effectiveness of the proposed approach and compared it with other mechanisms against similar attack. The simulation results show that our approach can improve detection accuracy and network energy consumption, indicating a viable approach to defend against advanced vampire attack. As a future work, since radio propagation and its channel dynamics cannot easily be captured by simulation, we plan to develop a small-scale testbed and deploy a real network composed of TelosB motes in an indoor environment to see the full potential of the proposed countermeasure.

Acknowledgment

This work was supported in part by Summer Undergraduate Research Experience (SURE) Award, Research Committee Funding Award, NASA WVSGC Undergraduate Affiliate Fellowship Program Award, and Startup grant in the Dept. of CSEE at Marshall University.

References

[1] B. Groves and C. Pu, "A Gini Index-Based Countermeasure Against Sybil Attack in the Internet of Things," in *Proc. IEEE MILCOM*, 2019, pp. 672–677.

[2] Y. Saleem, N. Crespi, M. Rehmani, and R. Copeland, "Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," *IEEE Access*, vol. 7, pp. 62 962–63 003, 2019.

[3] C. Pu, "Stochastic Packet Forwarding Algorithm in Flying Ad Hoc Networks," in *Proc. IEEE MILCOM*, 2019, pp. 480–485.

[4] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent Edge Computing for IoT-Based Energy Management in Smart Cities," *IEEE Network*, vol. 33, no. 2, pp. 111–117, 2019.

[5] P. Sharma, J. Park, Y. Jeong, and J. Park, "SHSec: SDN based Secure Smart Home Network Architecture for Internet of Things," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 913–924, 2019.

[6] J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia, and T. Melodia, "Machine learning for wireless communications in the Internet of things: A comprehensive survey," *Ad Hoc Networks*, vol. 93, p. 101913, 2019.

[7] C. Pu and L. Carpenter, "Digital Signature Based Countermeasure Against Puppet Attack in the Internet of Things," in *Proc. IEEE NCA*, 2019, pp. 1–4.

[8] 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.

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

[10] M. Bouaziz, A. Rachedi, A. Belghith, M. Berbineau, and S. Al-Ahmadi, "EMA-RPL: Energy and mobility aware routing for the Internet of Mobile Things," *Future Generation Computer Systems*, vol. 97, pp. 247–258, 2019.

[11] C. Pu, "Spam DIS Attack Against Routing Protocol in the Internet of Things," in *Proc. IEEE ICNC*, 2019, pp. 73–77.

[12] E. Vasserman and N. Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 318–332, 2011.

[13] R. Kanbur and A. Snell, "Inequality Indices as Tests of Fairness," *The Economic Journal*, vol. 129, no. 621, pp. 2216–2239, 2019.

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

[15] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO Insider Attack in RPL's Internet of Things Networks," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 68–71, 2019.

[16] A. Arış, S. Yalçın, and S. Oktuğ, "New lightweight mitigation techniques for RPL version number attacks," *Ad Hoc Netw.*, vol. 85, pp. 81–91, 2019.

[17] S. Chang, S. Kumar, Y. Hu, and Y. Park, "Power-Positive Networking: Wireless-Charging-Based Networking to Protect Energy against Battery DoS Attacks," *ACM Transactions on Sensor Networks*, vol. 15, no. 3, p. 27, 2019.

[18] F. Nizzi, T. Pecorella, F. Esposito, L. Pierucci, and R. Fantacci, "IoT Security via Address Shuffling: The Easy Way," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3764–3774, 2019.

[19] A. Bidgoly and H. Bidgoly, "A Novel Chaining Encryption Algorithm for LPWAN IoT Network," *IEEE Sensors J.*, vol. 19, no. 16, pp. 7027–7034, 2019.

[20] S. Murali and A. Jamalipour, "A Lightweight Intrusion Detection for Sybil Attack under Mobile RPL in the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379–388, 2020.

[21] C. Pu and B. Groves, "Energy Depletion Attack in Low Power and Lossy Networks: Analysis and Defenses," in *Proc. IEEE ICDIS*, 2019, pp. 14–21.

[22] K. Zeitz, M. Cantrell, R. Marchany, and J. Tront, "Changing the Game: A Micro Moving Target IPv6 Defense for the Internet of Things," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 578–581, 2018.

[23] 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.

[24] A. Vasudeva and M. Sood, "Survey on sybil attack defense mechanisms in wireless ad hoc networks," *Journal of Network and Computer Applications*, vol. 120, pp. 78–118, 2018.

[25] A. Raoof, A. Matrawy, and C. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1582–1606, 2019.

[26] C. Pu, "Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses," *IEEE Internet of Things Journal (Early Access)*, pp. 1–1, 2020.