A Novel Countermeasure for Selective Forwarding Attacks in IoT Networks

Okan Yaman
Department of Computer Engineering
Izmir Institute of Technology
Izmir, TURKEY
okanyaman@iyte.edu.tr
ORCID: 0000-0001-7292-2344

Barış Sokat
Independent Researcher
Innovia Technology
Izmir, TURKEY
barissokat@iyte.edu.tr
ORCID: 0000-0003-2051-815X

Tolga Ayav
Department of Computer Engineering
Izmir Institute of Technology
Izmir, TURKEY
tolgaayav@iyte.edu.tr
ORCID: 0000-0003-1426-5694

Yusuf Murat Erten
Department of Computer Engineering
Izmir University of Economics
Izmir, TURKEY
yusuf.erten@ieu.edu.tr
ORCID: 0000-0001-9537-7414

2022 3rd International Informatics and Software Engineering Conference (IISEC) | 978-1-6654-5995-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/IISEC56263.2022.9998204

***Abstract*—As the Internet of Things (IoT) devices become more widespread there are rising public concerns about whether or not IoT devices and their services are secure. One of the major threats they face is selective forwarding attacks performed by malicious nodes. Although packets can be lost inherently due to network conditions, malicious nodes, such as those performing blackhole attacks, may deliberately drop some, but not all of them. Therefore, distinguishing these nodes from legitimate ones is not so easy. This study has proposed a lightweight countermeasure to deal with this kind of attack in IoT networks, using the standard IPv6 Routing Protocol for Low Power and Lossy Networks (RPL). The mechanism is based on Mobile Trusted Nodes (MTNs). For the given threat model, we showed that our model has robust detection accuracy and brings no additional overhead to the network.**

Keywords—IoT, selective forwarding attacks, RPL, WSN

I. Introduction

In today’s world, we are surrounded by IoT technology, and it is estimated that IoT devices will outnumber the human population of the world by the end of 2050 [1]. We exploit these devices in smart cities [2, 3], healthcare systems [4], industry [5], and many other areas [6, 7, 8, 9, 10, 11]. However, this technology has brought severe security and privacy concerns, as well as advantages. Due to the growing numbers of IoT devices, they collect huge amounts of data therefore, it is important to make sure that data is protected. Hence, many models are proposed to provide more secure systems that keep our data private [12, 13, 14, 15, 16, 17, 18].

IoT devices are connected to the Internet using modified versions of existing protocols because computing power in them are restricted as well as their memory capacity and energy. IPv6 has been modified, for example, and new lightweight protocol, 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) has been introduced [19].

Since IP-connected WSNs are formed this way and connected directly to the untrusted Internet, these resource-constrained devices are vulnerable to various attacks, as stated before [20]. At the same time, the areas where IoT applications are adopted, such as healthcare and automation, usually require high security, and this introduces new loads to the structural challenges.

Contiki-NG operating system uses IPv6 Routing Protocol for Low-Power and Lossy Network (RPL), which selects the shortest path, to transmit the packets reliably. This protocol, however, may be subject to attacks from within the network [21, 22, 23, 24].

The blackhole attack in IoT networks is one such attack that must be detected and prevented for the safe operation of the network. The most basic form of the blackhole attack is performed by dropping all packets, and a more sophisticated type is the selective forwarding attack (SFA), which drops not all but some, selected packets. The network analysis was performed in many studies, and the Intrusion-Detection Systems (IDSs) were created against these attacks. This study analyzes the effects of the SFA that drops only the User Datagram Protocol (UDP) packets, without affecting the control packets, making detection more difficult. The following sections present the network behavior and performance under these circumstances.

There are four main contributions of this paper:

- The classical scheme, which is based on counting the sent and received messages, was improved by incorporating the packet drop time of the attacker and the duty cycle period of Mobile Trusted Nodes (detecting entities), hence, introducing novel detection probability,
- No additional overhead compared to existing models and it was shown to less than some
- Malicious nodes can be detected with almost 100% accuracy for the studied threat,
- It is effectively applicable to small networks.

The paper is organized as follows: Section 2 provides the general literature overview on SFAs in networks using the RPL and the IDS mechanisms against such attacks. Our system model is described in Section 3, and section 4 gives details of the performance analysis and results. We conclude the paper in Section 5.

II. Related work

An IDS which exploits the Sequential Probability Ratio Test (SPRT) and the Expected Transmission Count (ETX) to determine an adaptive threshold is proposed in [25] for the SFA in IPv6-based mobile WSNs. Two-factor reputation

978-1-6654-5995-2/22/$31.00 ©2022 IEEE

mechanism to detect compromised nodes is discussed in [26]. The first-hand employs direct monitoring, and the second checks the first-hand values sent by neighbors. They also have an extensive statistical approach for the acceptable packet loss threshold. There is a feedback-based trust-aware security protocol for IoT networks presented in [27]. The trust value is based on the packet forwarding performance. Trust-based RPL protocol is tested with testbed experiments in [28]. The authors of [29] introduced the neighborhood watch and the threshold-based analysis for detecting and correcting the SFA for medical WSNs in the IoT. The global monitoring capability and the infrastructure of fog computing are exploited in [30]. The vulnerability of home security devices to the SFA is demonstrated with some recommendations and solutions [31]. The authors of [20] propose one of the earliest IDS for the IoT to prevent the sink-hole attack and the SFA. The Heartbeat protocol is also introduced in [32] as a countermeasure for routing attacks. The channel-aware reputation system with an adaptive threshold is used to detect the SFA in [33], who also discusses an attack-tolerant data forwarding scheme. The authors in [34] extend SVELTE, one of the first IDS for the IoT, in which the geographical hint is employed to improve the detection rate.

III. Model

In this section, we state our system and threat models. A detailed attacker model is proposed in [35].

In this study, we employ the Contiki-NG, which is a version of the Contiki-OS operating system, and used on devices with limited resources in IoT applications. Using this open-source Contiki operating system a malicious version of it was created. The blackholes use this malicious operating system and they drop the packets selectively. Some of the nodes were compiled using malicious Contiki-NG and they performed the malicious activities.

The RPL implementations in Contiki-NG may be the RPL Classic or the RPL Lite [36]. We used the RPL Lite in this implementation, which is the default version for the Contiki-NG. The malicious Contiki-NG selected to perform the SFA was tested in advance in the Cooja simulation environment on the "Cooja mote," which is the native mote of the Cooja.

Unit Disk Graph Medium (UDGM): Distance Loss was chosen as the radio medium. The startup delay of a mote was set to 1 ms, and the random seed was 123.456. The Contiki processes (firmware) and the Contiki process sources are given in Table 1. The properties of the simulating machine are stated in Table 2.

TABLE I. Contiki processes (firmware) and sources

ENTITY	***FIRMWARE***	***SOURCE***
MTNs and Nodes	Rpl-udp	Udp-client
Root	Rpl-udp	Udp-server

TABLE II. The properties of the simulating machine

PROCESSOR	Intel Core i5-6600K CPU 3.50 Ghz
RAM	16.0 GB
SYSTEM TYPE	64-bit os, x64-based processor
O.S.	Windows 10 Pro Version 21h1

A) System Model

Let $N = \{n_1 ,\ldots, n_j\}$ be a set of j distinct nodes that send messages to the Root. Let $M = \{m_1 ,\ldots, m_k\}$ be a subset of N with k distinct malicious nodes that perform SFA. Time is assumed to be discrete and let $T = \{1 ,\ldots, j\}$ be a set of time instants where the Mobile Trusted Node (MTN) stops and sends messages through the corresponding nodes. We assume that the MTN's motion starts from the Root and ends at the leaf nodes of each tree.

Let $S = \{s_1 ,\ldots, s_j\}$ be a set of the number of sent messages to the Root through the corresponding nodes. Let $R = \{r_1 ,\ldots, r_j\}$ be a set of the number of received messages by the Root through the corresponding nodes. Then the system's probability distribution function (malicious node detecting probability) is as follows:

$$P\ (s_i - r_i > \Delta \mid n_i \epsilon M) \qquad (1)$$

where $s_i \epsilon S$, $r_i \epsilon R$, $n_i \epsilon N$, and Δ is the threshold value (the precision of the system).

Note that no children of attackers can send messages to the Root. Hence, detecting their malicious children through the abovementioned process is impossible, and we need to introduce an extended check with an additional MTN.

Let $N' = \{n_1' ,\ldots, n_j'\}$ be a subset of N with q distinct children of attackers. Let $T' = \{1' ,\ldots, q'\}$ be a subset of time instants when MTNs send messages to each other between the corresponding nodes. We assume that MTNs' motions start from the first child of attackers and end at leaf nodes of each tree. Let $S' = \{s_1' ,\ldots, s_q'\}$ be a set of the number of messages sent by the MTN_1 to the MTN_2 through the corresponding nodes. Let $R' = \{r_1' ,\ldots, r_q'\}$ be a set of the number of messages received by the MTN_2 that are sent by the MTN_1. Then the system's probability distribution function (malicious children detecting probability) is as follows:

$$P\ (s_i' - r_i' > \Delta \mid n_i' \epsilon M) \qquad (2)$$

where $s_i' \epsilon S'$, $r_i' \epsilon R'$, $n_i' \epsilon N'$, and Δ is the threshold value (the precision of the system).

As the number of MTN increases, it is possible to increase the detection rate of malicious nodes (see Section 4). We also assume that the Root cannot be compromised. Therefore, all the nodes apart from the Root and MTNs are prospective attackers.

A sample network with five nodes is given from Fig. 1. to Fig. 3. Node 1 is the Root, and the MTN is represented by node 5. It stops close to node 3 at time t_1 to check node 2 by sending UDP packets to the Root (see Fig. 1). The other nodes (2, 3, and 4) are potential attackers. However, we assume node 3 is malicious. The radio traffic is also shown with red arrows.

In Fig. 2, the second stop of the MTN is near node 4 at t_2 to check node 3 and the final destination is below node 4 to check it at t_3. However, we need to implement an extended check since node 4 is the attacker's child (see Fig. 3).

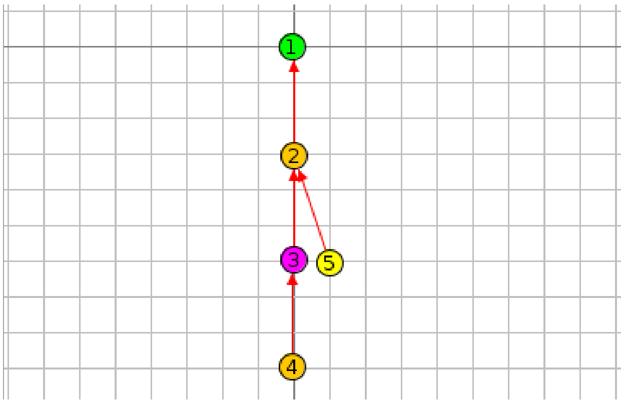

Fig. 1. A sample network for time instant t_1

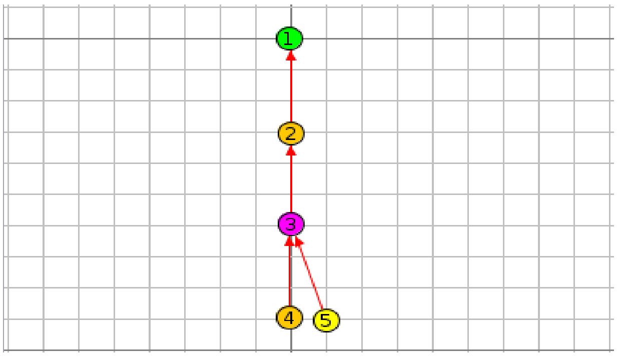

Fig. 2. A sample network for time instant t_2

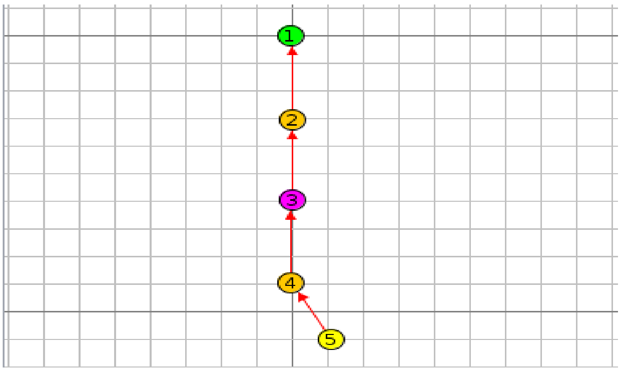

Fig. 3. A sample network for time instant t_3

A simulation for 1 hour duration was run. The number of sent and received packets is given for two check mechanisms where I.C and E.C refer to initial and extended checks, respectively (see Table 3). For node 2, the Root received all the sent packets, i.e., this node is not malicious. However, because none of the packets reached the Root through node 3, we can infer that node 3 is malicious, and, we made the same observation for node 4, as expected, similar to node 3. Nevertheless, an extended check is necessary to confirm that node 4 is not malicious.

TABLE III. SENT AND RECEIVED PACKETS IN 1 HOUR FOR VARYING CHECKS

NODE	***s***		***r***		***DECISION***	
	I.C.	***E.C.***	***I.C.***	***E.C.***	***I.C.***	***E.C.***
1	-	-	-	-	-	-
2	58	-	58	-	0% Mal.	-
3	58	-	0	-	100% Mal.	-
4	58	58	0	58	50% Mal.	0% Mal.
5	-	-	-	-	-	-

B) Threat Model

A network with one root (server) node, eight client nodes and a node which acted as a blackhole was designed. The client nodes running Contiki-NG and the blackhole mode running the modified malicious operating system were randomly distributed in the network and the clients were programmed to transmit a UDP packet every minute within the network.

The malicious node performs the SFA to drop all UDP packets while transmitting ICMPv6 control messages. The Contiki-NG first decapsulates packets arriving at the node. After the packet is identified as a UDP packet it is dropped.

The SFA only works if attacker is selected as the parent by neighbor nodes. To ensure this, the attackers' Rank has been manipulated. While testing SFA, the lowest Rank is assigned to the attacker which increases its chance to be selected as the parent. This approach reduces the time needed for the Rank assignment process, hence although it is not optimal is is effective.

In the simulations, it is assumed that the malicious node becomes active at the 57th second, and the SFA was launched at the 58th second. The Clients in all scenarios sent UDP messages to the Root with a period of 1 minute, starting at t= 0. One-minute intervals were chosen based on the assumption that sensors would send data in a similar manner in a real-life scenario. Each UDP message sent by the Client was recorded in the log file. To indicate that the message is received, the Root also also incremented the log file every time it receives a UDP message. This makes sure that the Client's UDP message had reached the Root. The Root which received UDP messages resends the same message back to the Client, and also records this process as an entry in the log records. The Client which received the reply message also logs this record to verify that package from the Root had reached the Client. If the Root receives no messages for a period of time, it resets the tree and forms it again. Thus the malicious node is eliminated. If the control packets are sent by the malicious node, however, then the Root has no means of detecting the attack.

IV. EVALUATION

This section includes the malicious node detection probability analysis of our proposed system. This likelihood depends on three factors: the number of sent messages, the number of received messages and the system's precision.

The system can be considered successful (detection of the attacker) when the MTN sends packets through the malicious checking node, and the Root does not receive them. In this case, our system deduces that the node is an attacker. However, some packets might drop, and the Root might not receive all the messages in a network even when there is no attacker. To reduce the frequency of this situation we should use a threshold value (the system's precision), and thus, it will occur only if the difference between the sent and received messages is greater than the threshold (see (1) and (2)).

We assume that s_i and s_i' are constant for all i. Hence, we are left with two factors: Δ and r_i. These depend on the duty cycle period of MTNs and the attacker's drop period. Consider two systems with the same duty cycle period of MTNs. In this case, it is more challenging to detect the attacker with a longer drop period, since there may be no dropped messages. Hence, the success probability of an attacker is directly proportional to the drop period. If we have two attackers with the same drop period, the system with a shorter duty cycle period of MTNs is notably more vulnerable to attacks, since it might also be shorter than the drop period. Thus, this system might not be able to detect the attacker, and the probability of a successful attack has inverse proportionality with the duty cycle period of MTNs. Therefore, the success probability of the attacker is as follows

$$P=\begin{cases} D/C \; if \; D<C \\ 1 \; if \; D\geq C \end{cases} \tag{3}$$

such that D is the attacker's drop period and C is the duty cycle period of MTNs.

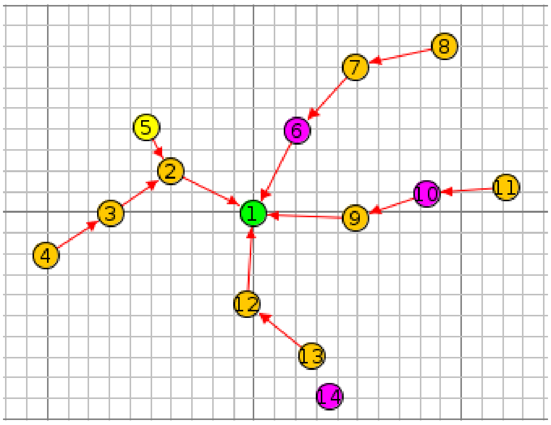

Fig. 4. The sample network with four trees

The sample network with fourteen nodes is given in Fig. 4 on a 30 m x 30 m area. Node 1 is the Root, and the MTN is represented by Node 5. All the other nodes are potential attackers, and we assume 6, 10, and 14 are malicious. The radio traffic is also shown with red arrows.

In Fig. 5, it is possible to observe the effect of the attacker's drop period on his success probability for varying systems. Here, System 1 refers to the system with 5 minute duty cycle period of MTNs, and System 2 and 3 have 10 and 15 minute periods, respectively. As the drop period increases, inherently, the greater the likelihood that the attacker is able to cheat our system.

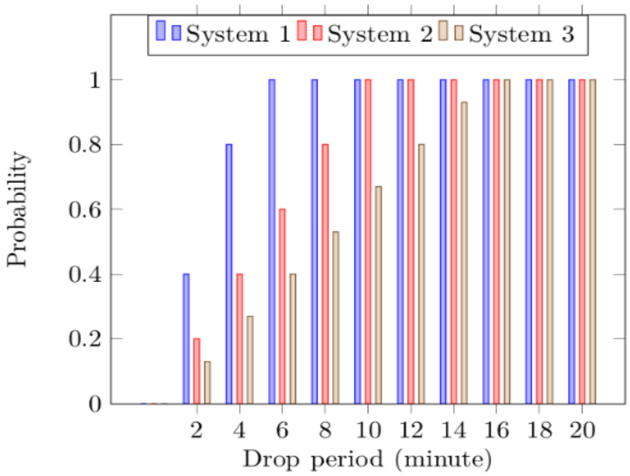

Fig. 5. Effect of drop period for varying systems

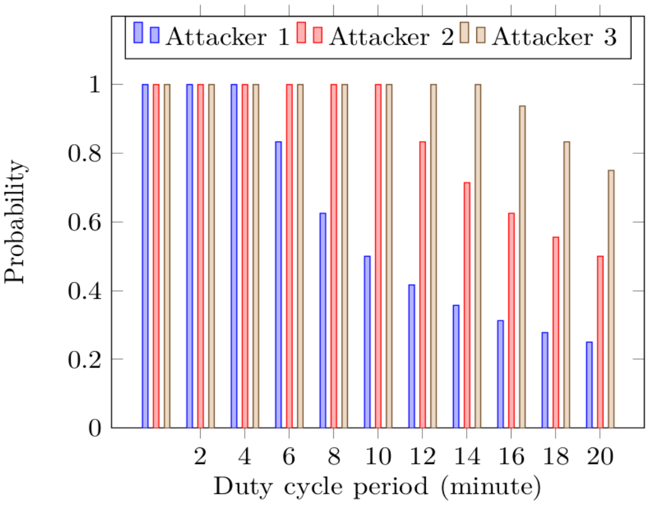

Fig. 6. Effect of duty cycle period for varying attackers

In Fig. 6, the plots show the relationship between the MTN duty cycle period and the attacker's probability of success for different attackers. Attacker 1 corresponds to the malicious node with 5 minute drop period. Attackers 2 and 3 have a 10 and 15 minute drop period, respectively. As expected, the increase in the MTN duty cycle period provides robustness.

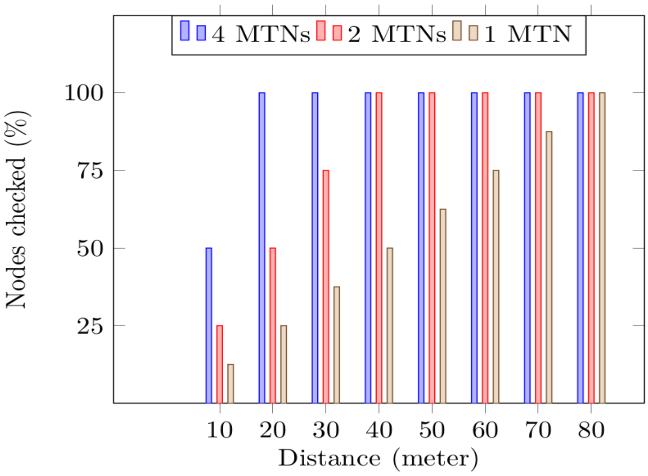

Fig. 7. Impact of covered distance on percentage of checked nodes

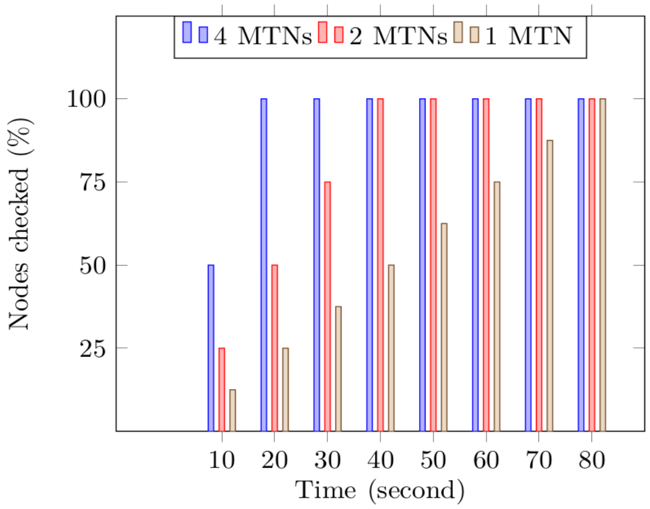

Fig. 8. Impact of elapsed distance on percentage of checked nodes

In Fig. 7 and Fig. 8, we examined the impact of MTNs on our sample network given in Fig. 4. Let MTNs start their motion from the Root and cover the whole network through each tree. We also assume that their speed is 1 m/s, and that they pause near each node. Since each node has a 5 m range and each tree has four nodes, a single MTN has to move 20 m on average to check all the nodes in a tree. It follows that 80 m is the required distance to cover the whole network. We can observe that as the number of MTNs increases, there is an increase in the number of distances that can be monitored, and the speed at which they are monitored.

It was simulated in the built-in Cooja environment of the CONTIKI-NG operating system for 1 hour, and the result can be seen in Table 4. Note that M_S is the number of sent messages by the MTN, and M_R is the number of received messages by the Root through the corresponding node. M_S and M_R are the same for nodes 2, 3, 4, 9, 12, and 13, and therefore, these cannot be malicious. However, nodes 6, 10, and 14 can be considered malicious, since the Root received nothing through these. The most challenging decisions are about the other nodes, which are attackers' children. Due to their parents, no packets can be sent to the Root, making it impossible to detect whether or not they are malicious

TABLE IV. STATUS OF NODES

	M_S	**M_R**	**DECISION**
Node 1	-	-	-
Node 2	3	3	0% Mal.
Node 3	3	3	0% Mal.
Node 4	3	3	0% Mal.
Node 5	-	-	-
Node 6	3	0	100% Mal.
Node 7	3	0	50% Mal.
Node 8	3	0	50% Mal.
Node 9	3	3	0% Mal.
Node 10	3	0	100% Mal.
Node 11	3	0	50% Mal.
Node 12	3	3	0% Mal.
Node 13	3	3	0% Mal.
Node 14	3	0	100% Mal.

without another check. We need two MTNs to perform this operation (see Table 3). Note that it is unnecessary, hence, inefficient, to implement this process for all nodes, especially for large networks. Therefore, our system checked all the network and detected malicious nodes effectively.

Finally, we discuss the overhead of the proposed model to the network. The sent and received packets are nothing but simple Hello messages. Since MTNs are also members of the network, we can assume the absence of additional overhead on the network. However, increasing the number of MTNs will bring a considerable overhead. Therefore, we can conclude that our model is effectively viable for small networks.

V. CONCLUSION

The RPL is a handy routing protocol for Low power and Lossy Networks. It is also vulnerable to many insider attacks, including the SFA. An SFA can be devised to drop only the data packets. Defense mechanisms are generally based on checking the packet drop performance. This study introduced an improved approach to the malicious node detection probability by exploiting the attacker's packet drop time and the MTN duty cycle period. We also showed that our proposed model achieved almost 100% accuracy without bringing additional overhead for the given threat model. To increase the accuracy, it is important to maximize the duty cycle period of MTNs, and increasing the number of MTNs also has a positive effect on performance. Since our model is effectively applicable to small networks, we plan to examine the relationship between the effectiveness and the size of the network as future research.

ACKNOWLEDGMENT

The first author of this study is a 100/2000 YOK Ph.D. Scholar.

REFERENCES

[1] P. Agarwal and M. Alam, "Investigating IoT Middleware Platforms for Smart Application Development", 2018, [online] Available: http://arxiv.org/abs/1810.12292.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities", IEEE Internet Things J., vol. 1, no. 1, pp. 22-32, Feb. 2014.

[3] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework of creating a smart city through Internet of Things", IEEE Internet Things J., vol. 1, no. 2, pp. 112-121, Apr. 2014.

[4] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey", IEEE Access, vol. 3, pp. 678-708, 2015.

[5] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0", IEEE Ind. Electron. Mag., vol. 11, no. 1, pp. 17-27, Mar. 2017.

[6] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey", Comput. Netw., vol. 54, no. 15, pp. 2787-2805, 2010.

[7] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey", IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2233-2243, Nov. 2014.

[8] A. Whitmore, A. Agarwal, and L. D. Xu, “The Internet of Things—A survey of topics and trends”, Inf. Syst. Front., vol. 17, no. 2, pp. 261–274, 2015.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies protocols and applications", IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347-2376, 4th Quart. 2015.

[10] A. Botta, W. D. Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things", Proc. Int. Conf. Future Internet Things Cloud (FiCloud), pp. 23-30, Aug. 2014.

[11] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision architectural elements and future directions", Future Gen. Comput. Syst., vol. 29, no. 7, pp. 1645-1660, 2013.

[12] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, "Security of the Internet of Things: Perspectives and challenges", Wireless Netw., vol. 20, no. 8, pp. 2481-2501, 2014.

[13] R. H. Weber, "Internet of Things—New security and privacy challenges", Comput. Law Security Rev., vol. 26, no. 1, pp. 23-30, 2010.

[14] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision applications and research challenges", Ad Hoc Netw., vol. 10, no. 7, pp. 1497-1516, 2012.

[15] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture possible applications and key challenges", Proc. 10th Int. Conf. FIT, pp. 257-260, 2012.

[16] I. Lee and K. Lee, "The Internet of Things (IoT): Applications investments and challenges for enterprises", Bus. Horizons, vol. 58, no. 4, pp. 431-440, 2015.

[17] E. Borgia, "The Internet of Things vision: Key features applications and open issues", Comput. Commun., vol. 54, no. 12, pp. 1-31, 2014.

[18] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of Internet of Things (IoT) against security threats using cryptographic authentication", J. Supercomput., vol. 156, pp. 1-25, Jan. 2020.

[19] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15. 4: A developing standard for low-power low-cost wireless personal area networks", IEEE Netw., vol. 15, no. 5, pp. 12-19, Sept./Oct. 2001.

[20] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", Ad hoc networks 11, no. 8 (2013): 2661-2674.

[21] A. Dunkels, B. Grönvall, and T. Voigt, "Contiki—A lightweight and flexible operating system for tiny networked sensors", Proc. 29th Annu. Int. Conf. Local Comput. Netw. (LCN), pp. 455-462, 2004.

[22] A. Mayzaud, R. Badonnel, and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security 18, no. 3 (2016): 459-473.

[23] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT", In 2015 International conference on pervasive computing (ICPC), pp. 1-6. IEEE, 2015.

[24] W. Yang, Y. Wang, Z. Lai, Y. Wan, and Z. Cheng, "Security Vulnerabilities and Countermeasures in the RPL-based Internet of Things", In 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 49-495. IEEE, 2018.

[25] F. Gara, L. Ben Saad, and R. Ben Ayed, "An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs," In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 276-281. IEEE, 2017.

[26] A. Patel, and D. Jinwala, "A reputation-based RPL protocol to detect selective forwarding attack in internet of Things," International Journal of Communication Systems, vol.35, no.1, p.e5007, Jan 2022.

[27] D. Airehrour ,J. Gutierrez, and S.K. Ray, "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks," Journal of Telecommunications and the Digital Economy, vol.5, no.1, pp.50-69, Mar 2017.

[28] D. Airehrour, J. Gutierrez, and S.K. Ray, "A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the RPL routing protocol," Journal of Telecommunications and the Digital Economy, vol.6, no.1, pp.41-49, Mar 2018.

[29] A. Mathur, T. Newe, and M. Rao, "Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in IoT," Sensors, vol.16, no.1, p.118, Jan 2016.

[30] Q. Yaseen, F. Albalas, Y. Jararwah, and M.A. Ayyoub, "Leveraging fog computing and software defined systems for selective forwarding attacks detection in mobile wireless sensor networks," Transactions on Emerging Telecommunications Technologies, vol.29, no.4, p.e3183, Apr 2018.

[31] A. Hariri, N. Giannelos, and B. Arief, "Selective Forwarding Attack on IoT Home Security Kits," Computer Security, Springer, Cham, pp.360-373, Sep 2019.

[32] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," International Journal of Distributed Sensor Networks, vol.9, no.8, p.794326, Aug 2013.

[33] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks," IEEE Transactions on Wireless Communications, v.15, no.5, pp3718-3731, Feb 2016.

[34] D. Shreenivas, S. Raza, T. Voigt, "Intrusion Detection in the RPL-connected 6LoWPAN Networks," In Proc.of the 3rd ACM international workshop on IoT privacy, trust, and security, pp.31-38, Apr 2017.

[35] B. Sokat, "Blackhole attacks in IoT networks", Master's thesis, Izmir Institute of Technology, 2020.

[36] Contiki-Ng. Accessed: Nov. 25, 2020. [Online]. Available: https://github.com/contiki-ng/contiki-ng/wiki/Documentation:-RPL.