A Study on Detection and Detour Methods against Packet Dropping Attacks in IPv6-based IoT

Sooyeon Shin[1] , Seulgi Kim[1], Jaewoo Choi[2], and Taekyoung Kwon[1]*
[1]Yonsei University, Seoul, 03722, Republic of Korea
shinsy80@gmail.com, ksg0131@yonsei.ac.kr, taekyoung@yonsei.ac.kr
[2]Korea Internet & Security Agency, Seoul, 05717, Republic of Korea
jw.choi@kisa.or.kr

Abstract

In this paper, we propose new detection and detour methods against packet drop attacks for availability in the Internet of Things (IoT) based on the IEEE 802.15.4e and RPL protocol standards that employ IPv6. We consider the rank value of RPL and the consecutive packet drops to improve the detection metrics, and also take into account the use of both sibling and child nodes on a RPL routing path to construct the detour method. Our simulation results show that the proposed detection method is faster than the previous results, and the detour method improves the detour success rate.

Keywords: Internet of Things, Malicious Packet Dropping Detection, Detour method, IPv6, RPL

1 Introduction

As Internet of Things (IoT) has received attention as a key industry in the future of the IT industry, technologies and services development is actively underway for IoT. The IoT is the connection of various objects to the Internet to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing. While IoT provides us many valuable benefits, IoT also brings tremendous challenges to its security. IoT devices have strong resource constraints (energy, memory, processing) and their communication links are by nature characterized by a high loss rate and a low throughput. Thus, consideration should be given to secure communication throughout its lifecycle.

In this paper, we propose a detection and detour methods against packet dropping attacks for secure communication and availability in the IoT environments. We consider IoT devices based on the IEEE 802.15.4e and RPL protocol standards that employ IPv6. By employing additional detection metrics which influence on the malicious packet dropping detection for the IoT, the proposed detection method can improve the detection speed. When malicious nodes which drops packets are detected, the proposed detour method can repair broken routes using both sibling and child nodes. Through simulation, we evaluate the performance of proposed methods and compare it to the previous works.

The remainder of this paper is organized as follows: In Section 2, we present a detection method of malicious dropping and detour method to find another route without malicious nodes. In Section 3, we evaluate the performance of the proposed methods and compare it to the previous works. In Section 4, we review the previous related works. We conclude this paper in Section 5.

IT CoNvergence PRActice (INPRA), volume: 4, number: 3 (September 2016), pp. 20-27
*Corresponding author: Graduate School of Information, Yonsei University, 50 Yonsei-ro Seodaemun-gu, Seoul, 03722, Republic of Korea, Tel: +82-2-2123-4523

2 Detection and Detour Methods against Malicious Packet Dropping

In this section, we propose a malicious packet dropping detection for IoT environments. By considering features for the vision in IoT, we extend a method for malicious packet dropping detection in MANETs [15] in order to guarantee availability of IoT services. We then present a detour method when malicious nodes are detected.

2.1 System and Threat Models

As the IoT continues to grow, many standards have been issued for different IoT application domains such as IEEE 802.15.4 [1], 6LoWPAN (IPv6 over Low power WPAN) [11], RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [16] and CoAP (Constrained Application Protocol) [14]. In particular, IEEE 802.15.4 has become a representative wireless standard for IoT but there are several limitations. As an enhanced version of IEEE 802.15.4, the IEEE 802.15.4e working group was created in 2008 and IEEE 802.15.4e adopted channel hopping strategy to support new network structures and functionalities for various applications. According to Gartner, Inc. there will be nearly 20.8 billion devices on the internet of things by 2020 [6]. To accommodate a large number of devices, IPv6 is considered the most suitable technology for the IoT. IETF proposed RPL, a routing protocol primarily designed for LLNs (Low-power Lossy Networks). RPL is recently standardized for IPv6 constrained IoT networks and runs over radio layers such as IEEE 802.15.4. RPL is a distance vector routing protocol that builds a routing tree, referred to as a DODAG (Destination Oriented Directed Acyclic Graph) considered as a logical routing topology over a physical network. RPL constructs the graph and determines the routes using an OF (Objective Function) which defines how routing metrics, optimization objectives, and related functions are used to compute rank. A rank is a node's position relative to other nodes with respect to the DODAG root, namely the hop count from the DODAG root. Reflecting on the trend of IoT standards, we design system and threat models in order to detect and detour malicious packet dropping in IoT environments.

We consider IoT environments such as smart factory or smart manufacturing, which include n nodes. Each node as an IoT device monitors manufacturing facilities, detects a risk, and alerts an warning. Although there are some applications where the IoT device is used for both mobile and fixed use cases, we assume that every node is distributed in a given area and its location is fixed after distribution. We assume that IEEE 802.15.4e is employed as the PHY (Physical) and MAC (Media Access Control) layer protocols and the RTS/CTS (Request to Send/Clear to Send) mechanism is used to send packets. Although he RTS/CTS mechanism is designed for the IEEE 802.11 wireless networking protocol, it is possible to use this mechanism in IEEE 802.15.4 in order to overcome the hidden node problem in IEEE 802.15.4 [5], [3]. We also assume that IPv6 is employed as the NWK (Network) layer protocol and nodes communicate using the IPv6 routing protocol, RPL. To detect malicious packet dropping, each node, as an uncompromised node, monitors neighbour nodes including its parent and child nodes within the communication range using a watchdog approach (i.e, the watchdog method in [9]).

We consider the existence of attackers who try to compromise normal nodes to be malicious nodes. Malicious nodes behave like the legitimate ones but drop received packets instead of forwarding them.

2.2 Malicious Packet Dropping Detection Method

We propose a detection methodology for malicious packet dropping in IoT. For this purpose, we extend the detection approach in MANETs [15]. In [15], the probability of occurrence of packet dropping, P_D, is estimated based on the model of data forwarding in MANETs. If the probability P_D is greater than a predefined detection threshold, malicious node is detected. Based on the RTS/CTS mechanism,

three kinds of probabilities, P_F, P_C, and P_M are considered to compute P_D. P_F is the percentage of data packets forwarded by the node with regard to the number of packets received by it, P_C, and P_M are the probabilities of packet losses due to collisions or channel errors and broken links caused by mobility circumstances, respectively.

The RTS/CTS mechanism runs over the MAC layer thus the mechanism runs normally even if malicious nodes deliberately drop the packets. In addition, in RPL as the NWK layer, a node with a lower rank is closer to a DODAG root and has more child nodes than other nodes with higher ranks. That means the effect of packet dropping on the whole network can vary according to the rank of node. To improve the detection speed when a node with a lower rank is detected as a malicious packet dropping attacker, we consider W_R, the rank weight for a single dropped packet meaning that one dropped packet can be interpreted into one more packet dropping. If n nodes are located into proper positions, a DODAG may have the form of complete binary tree and the height of the tree will be $\log_2 n$. Since a node's rank is related to the height of tree, W_R is computed as $W_R = \log(\log_2 n - rank)$, where n is the number of nodes and *rank* is the rank value for a monitored node.

During the detection of packet dropping, it is important to distinguish between deliberately dropping attacks and forwarding errors, i.e., collisions or channel errors. However, it is difficult to distinguish between them because communication errors frequently occur in wireless networks. No matter what may happen, if a node consecutively drops packets, it could have negative effects on the availability of IoT services. In this case, such node should be removed from the route for forwarding packets. Therefore, we consider another metric, W_C which is the weight with regard to consecutive packet drops. Let node C be located within the communication range of both node A and B. If so, C can monitor all of the two nodes, A and B. To detect consecutive packet drops, C records the sequence numbers of forwarded and received packets from both nodes and calculate the number of consecutive dropped packets as the gap of packet sequence number between last received packet and next received packet once one more intermediate packets are lost. Within the detection windows, C then increases a corresponding counter C_i for each node, where i is the number of consecutive dropped packets. For example, if A drops two consecutive packets three times, C records 3 into C_2 for A. As the number of consecutive dropped packets increases, the chance that the node is malicious may increase. Therefore, W_C is computed as $W_C = \sum_{i=2} a_i C_i$, where a_i is a constant with regard to the degree of influence of the number of consecutive dropped packets has in the communication reliability and the availability of IoT services.

As we mentioned in Section 2.1, locations of nodes are fixed thus we do not consider the mobility metric P_M in [15]. Taking additional metrics into consideration, we slightly modify P_F in [15] as follows:

$$P'_F = \frac{\#Data_F - (\#Data_D \times W_R + W_C)}{\#Data_R}, \tag{1}$$

where $\#Data_D = \#Data_R - \#Data_F$. $\#Data_F$, $\#Data_R$, and $\#Data_D$ mean the number of forwarded packets, the number of received packets, and the number of dropped packets, respectively. Based on the equation (1), the probability of occurrence of packet dropping can be calculated as follows:

$$P'_D = 1 - \frac{P'_F}{1 - P_C}, \tag{2}$$

where P_C is same as the probability for the RTS or CTS packets to be lost due to collisions or channel errors in [15]. If P'_D is greater than a predefined detection threshold θ, malicious packet dropping can be detected. Otherwise, the analyzed node can be regarded as a legitimate node.

2.3 RPL based Detour Method

In the network topology of IoT services where RPL is used, the relationship between nodes (i.e., parent, sibling, and child) is critical to packet forwarding. Even if there is one malicious node in the DODAG,

Algorithm 1 Detour algorithm using sibling and child nodes

Require: list of siblingNodes, list of childNodes, Node parentNode, int parentRank, int parentNodeID
Ensure: newParentNode

```
while SN ∈ siblingNodes do                                   ▷ SN: Sibling Node
    id = SN → getParentNodeID()
    rank = SN → getParentNodeRank()
    if id ≠ parentNodeID and rank ≥ parentRank then
        return SN
    end if
end while
while CN ∈ childNodes do                                     ▷ CN: Child Node
    id = CN → getParentNodeID()
    rank = CN → getParentNodeRank()
    if id ≠ parentNodeID and rank ≥ parentRank then
        return CN
    end if
end while
return NULL
```

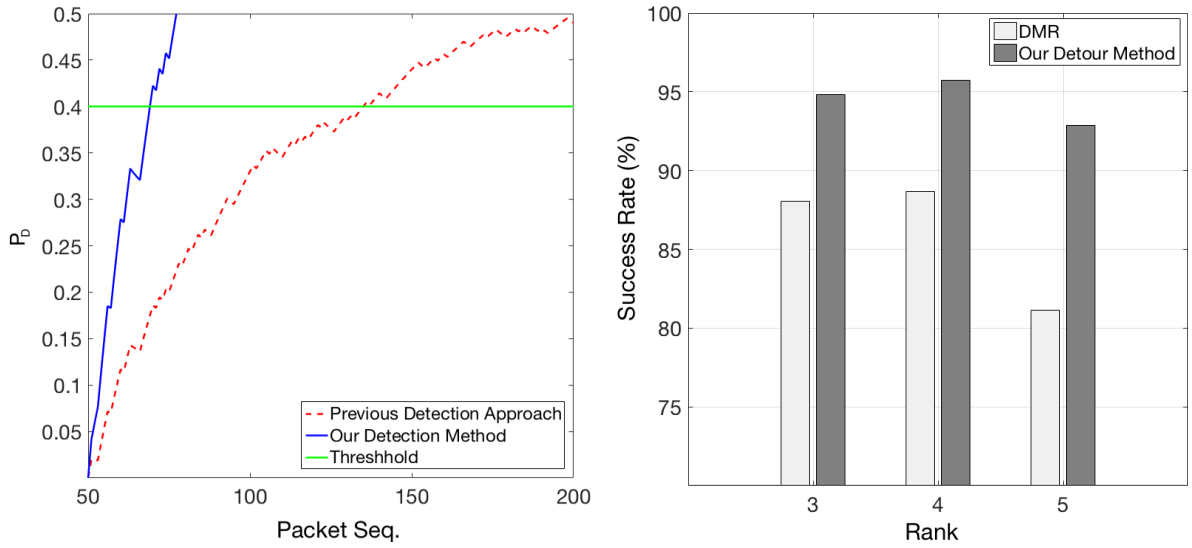
this can be problematic because malicious behaviors of the corresponding node will corrupt communications of its all child nodes. When malicious nodes are detected, packets should forwarded by detouring the corresponding nodes for the availability of IoT services. For this purpose, we propose a detour method by extending a DAG (Directed Acyclic Graph)-based multipath routing protocol based on RPL, called DMR [7]. DMR can repair broken routes locally using sibling nodes with same rank values when there is no valid parent node a route failure. However, there can be no sibling nodes because in RPL, the DODAG construction for setting routes depends on the locations of nodes. In addition, there is a possibility the sibling nodes are not work normally due to the inside and outside factors (i.e., communication errors and another malicious nodes). To improve this problem, our detour method repairs broken routes using child nodes when both parent and sibling nodes are malicious or they are not valid nodes on a route. The detour method is described in Algorithm 1.

3 Performance Evaluation

In this section, we evaluate the performance of proposed methods and compare it with the previous works. Figure 1 shows our simulation and experimental results. As illustrated in Figure, the simulated results show a considerable enhancement in the detection speed when compared with the detection approach in MANETs [15]. The experimental results show that the proposed detour method improves the detour success rate comparing to the previous approach, DMR [7].

3.1 Detection Speed

Our method for detection of malicious packet dropping utilizes rank values in RPL and consecutivity in packet dropping to improve the detection performance. MATLAB simulation was used to verify the proper performance of our method. For simulation, we assume that a target node normally forwards packets until the sequence number of packets to be 50, but whereafter the node will be compromised and will drop packets with the probability of 0.6 due to the attack. We also assume that the maximum height of DODAG is 8 and the detection threshold θ is 0.4. Table 1 shows parameters chosen for simulation.



(a) Packet dropping detection according to the sequence number of packets.

(b) Detour success rate according to rank values.

Figure 1: Comparison of simulation results.

Table 1: Simulation Parameters.

Parameter	Value
Maximum height of DODAG	8
Rank value of target node	5
Probability of packet dropping ($Seq. > 50$)	0.6
Detection threshold θ	0.4
Maximum number of consecutive packet drops	4
Constants in W_C: a_2, a_3, a_4	0.1, 0.2, 0.3

*$Seq.$: the sequence number of packets

As shown in Figure 1(a), the detection probability of our method reaches the detection threshold when the sequence number of packets is 69 (the 19th packet after $Seq. = 50$), while that of the previous method reaches the threshold when the sequence number of packets is 135 (the 85th packet after $Seq. = 50$). As expected, the detection speed of our method is 1.96 times faster than the previous method.

3.2 Detour Success Rate

To evaluate the performance of our detour method and compare it to the previous method, DMR [7], we developed a simulation program written in C++ language. The simulation area covers a 1000 m $\times$ 1000 m region, where 100 nodes are randomly distributed. We then constructed the DODAG and estimated rank values of all nodes based on RPL. We assume that a target node with the rank value between 3 and 5 is selected and the target node is detected as a malicious packet dropping node. Namely, three target nodes with different rank values (i.e., 3, 4, and 5, respectively) are selected. We estimated the detour success probability for child nodes of the malicious node. All the simulation results for each target node represent the mean of 30 trials.

Figure 1(b) shows the results of comparison between our method and the previous method in terms of the detour success probability. As shown, the success probabilities of the previous method range from 81.15% to 88.69%, while that of our method range from 92.88% to 95.74%. Namely, our method improved the detour success probability by almost 6∼10%.

4 Related Work

The detection of malicious packet dropping and its countermeasures in wireless networks including MANETs have been studied by many researchers, e.g., [2], [10], [4], [13].

Balakrishnan et al. proposed a network-layer acknowledgement-based scheme which detects misbehaving nodes using a special type of acknowledgement packets, termed TWOACK packets [2]. Other nodes then may avoid them in future route selections. Liu et al. proposed the 2ACK scheme [8] based on an improvement of their previous scheme, TWOACK. The 2ACK scheme detects and mitigates the effect of routing misbehavior by serving as an add-on technique for routing schemes. To reduce routing overhead, only a portion of received packets are acknowledge in the 2ACK scheme.

Miranda and Rodrigues proposed the Friends and Foes algorithm based on reputation-system to discourage selfish behavior in MANETs [10]. In this algorithm, for justifying selfishness, nodes are allowed to publicly declare that they refuse to forward messages for some nodes by periodically broadcasting one message. Thus, this algorithm rewards the cooperating nodes and punishes the selfish nodes which refuse to cooperate. Basile et al. introduced the notion of inner-circle consistency, where local node interaction is used to neutralize errors and attacks at the source [4]. When a node sends a message, all neighbours in an inner-circle, check and filter any information originating from the corresponding node. To prevent propagation of errors and attacks in the wireless network and to improve the fidelity of the propagated information, authors combined statistical and threshold cryptography techniques.

Nadeem and Howarth illustrated how intruders can cause DoS attacks in MANETs and proposed an anomaly-based intrusion detection system for detecting DoS attacks [12]. This system used a combination of chi-square and control chart to detect intrusion and to identify an intruder. Based on the previous work [12], they proposed an IDAR (intrusion detection & adaptive response) mechanism for MANETs [13]. The IDAR detects a range of attacks and provides an effective response with low impact on network performance.

5 Conclusion

For availability of the IoT based on the IEEE 802.15.4e and RPL protocol standards, in this paper, we proposed a detection method against malicious packet dropping and a detour method for repairing broken routes when malicious packet dropping is detected. By considering the rank value of RPL and the consecutive packet drops, we improved the detection speed. The propose detour method had higher detour success rate than the previous work by using not only sibling nodes but also child nodes.

Acknowledgements

This work was supported in part by the National Research Foundation of Korea (NRF-2016-R1C1B2011095 and NRF-2015-R1A2A2A01004792). This research was also supported in part by the MSIP(Ministry of Science, ICT and Future Planning, Korea, under the ITRC(Information Technology Research Center) support program (IITP-2016-R2718-16-0003) supervised by the IITP(National IT Industry Promotion Agency).

References

[1] Part 15.4:Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS): Amendment to Add Alternate Phy (Amendment of IEEE Std 802.15.4), January 2006. http://ieeexplore.ieee.org/Xplore/defdeny.jsp?url=http

[2] K. Balakrishnan, J. Deng, and V. K. Varshney. Twoack: preventing selfishness in mobile ad hoc networks. In *Proc. of the 2005 IEEE Wireless Communications and Networking Conference (WCNC'05), New Orleans, Louisiana, USA*, pages 2137–2142. IEEE, March 2005.

[3] N. Barroca, L. M. Borges, F. J. Velez, and P. Chatzimisios. Ieee 802.15.4 mac layer performance enhancement by employing rts/cts combined with packet concatenation. In *Proc. of the 2014 IEEE International Conference on Communications (ICC'14), Sydney, Australia*, pages 466–471. IEEE, June 2014.

[4] C. Basile, Z. Kalbarczyk, and R. K. Iyer. Inner-circle consistency for wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, 6(1):39–55, January 2007.

[5] J. Duan, Y. Zhuang, and L. Ma. An adaptive rts/cts mechanism in ieee 802.15.4 for multi-hop networks. In *Proc. of the 2012 International Conference on Computational Problem-Solving (ICCP'12), Leshan, China*, pages 155–159. IEEE, October 2012.

[6] Gartner. Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015: available at `http://www.gartner.com/newsroom/id/3165317`, Nov 2015.

[7] K.-S. Hong and L. Choi. Dag-based multipath routing for mobile sensor networks. In *Proc. of the 2011 International Conference on ICT Convergence (ICTC'11), Seoul, Korea*, pages 261–266. IEEE, September 2011.

[8] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan. An acknowledgment-based approach for the detection of routing misbehavior in manets. *IEEE Transactions on Mobile Computing*, 6(5):536–550, May 2007.

[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proc. of the 6th annual international conference on Mobile computing and networking (MOBICOM'00), Boston, Messachusetts, USA*, pages 255–265. ACM Press, August 2000.

[10] H. Miranda and L. Rodrigues. Friends and foes: preventing selfishness in open mobile ad hoc networks. In *Proc. of the 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03), ,*, pages 440–445. IEEE, May 2003.

[11] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, September 2007. https://tools.ietf.org/html/rfc4944.

[12] A. Nadeem and M. Howarth. Adaptive intrusion detection & prevention of denial of service attacks in manets. In *Proc. of the 2009 International Wireless Communications and Mobile Computing Conference (IWCMC'09), Leipzig, Germany*, pages 926–930. ACM Press, June 2009.

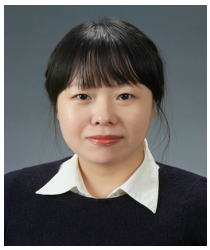
[13] A. Nadeem and M. P. Howarth. An intrusion detection & adaptive response mechanism for manets. *Ad Hoc Networks*, 13:368–380, February 2014.

[14] Z. Shelby, K. Hartke, and C. Bormann. Constrained Application Protocol (CoAP). BCP 78, June 2013. https://tools.ietf.org/html/draft-ietf-core-coap-18.

[15] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, and R. Magán-Carrión. A model of data forwarding in manets for lightweight detection of malicious packet dropping. *Computer Networks*, 87:44–58, July 2015.

[16] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. IETF RFC 6550, March 2012. https://tools.ietf.org/html/rfc6550.

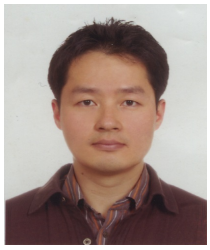
Author Biography



Sooyeon Shin received her B.S., M.S., and Ph.D. degrees in computer science and engineering from Sejong University, Seoul, Korea, in 2004, 2006, and 2012, respectively. From 2012 to 2013, she was a post-doctoral researcher at Sejong University. In 2013, she joined Yonsei University, Seoul, Korea, to continue her post doctoral research. Her current research interests include cryptography, privacy preservation, computer network security, wireless sensor network security, usable security, and Internet of Things.

Seulgi Kim received the B.S. degree in Engineering from Soonchunhyang University in 2015. Currently he is taking a master's course at Graduate School of Information, Yonsei University. His research interests include network system, usable security, and authentication.

Jaewoo Choi received the B.S. degree in game engineering from Korea Polytechnic University, Siheung, Korea, in 2014 and the M.S. degree in information systems from Yonsei University, Seoul, Korea, in 2016. He is currently a researcher at Korea Internet Security Agency, Seoul, Korea. His current research interests include computer network security and information security and privacy.



Taekyoung Kwon received the B.S., M.S., and Ph.D. degrees in computer science from Yonsei University, Seoul, Korea, in 1992, 1995, and 1999, respectively, where he is currently a Professor of Information. From 1999 to 2000, he was a Post-Doctoral Research Fellow with the University of California, Berkeley, CA, USA, and, from 2001 to 2013, a Professor of Computer Engineering with Sejong University, Seoul, Korea. From 2007 to 2008, he visited the University of Maryland, College Park, MD, USA, for sabbatical. His research interests include information security and privacy, cryptographic protocol, Internet of Things, usable security, and human-computer interaction.