Comment on "DIO Suppression Attack Against Routing in the Internet of Things"

Abhishek Verma [1] and Virender Ranga [2]

[1]National Institute of Technology Kurukshetra
[2]Affiliation not available

October 30, 2023

Abstract

We have thoroughly studied the paper of Perazzo et al., which presents a routing attack named DIO suppression attack with its impact analysis. However, the considered simulation grid of size 20mx20m does not correspond to the results presented in their paper. We believe that the incorrect simulation detail needs to be rectified further for the scientific correctness of the results. In this comment, it is shown that the suppression attack on such small sized network topology does not have any major impact on routing performance, and specific reason is discussed for such behavior.

Comment on "DIO Suppression Attack Against Routing in the Internet of Things"

Abhishek Verma*, *Student Member, IEEE*, and Virender Ranga

***Abstract*—We have thoroughly studied the paper of Perazzo et al., which presents a routing attack named DIO suppression attack with its impact analysis. However, the considered simulation grid of size 20m×20m does not correspond to the results presented in their paper. We believe that the incorrect simulation detail needs to be rectified further for the scientific correctness of the results. In this comment, it is shown that the suppression attack on such small sized network topology does not have any major impact on routing performance, and specific reason is discussed for such behavior.**

***Index Terms*—Internet of Things, RPL, secure routing, routing attacks, Trickle algorithm**

I. Introduction

Perazzo et al. [1] presented a replay mechanism based routing attack named DIO suppression attack. The authors claimed that the attack severely degrades the routing service of IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) by conducting experiments on a small simulation grid of size 20m×20m having 30 non-root nodes and 5 malicious nodes. They considered Multi Ray-Tracer Medium (MRM) for simulating the realistic channel. The present work concerns about incorrect simulation detail and corresponding results included in the paper of Perazzo et al. [1]. Comment on their work is discussed in Section II. The replay interval and suppression threshold values have been retained for easy comparison between this and reference paper. We obtained MRM parameters used in their paper from one of its co-authors [2]. Table I shows the MRM parameters values used in the experiments.

In our experiments we used Zolertia 1 (Z1) platform (MSP430 architecture based ultra-low power micro-controller board). The simulation experiments are performed on Cooja. Contiki's RPL library is modified to implement suppression attack on attacker nodes. Specifically, an attacker node is programmed to eavesdrop and capture DIO message from a legitimate replay source node, and then replay the captured message in fixed replay interval. A random topology containing one gateway node and 30 non-root nodes which are placed randomly on a grid of 20m×20m is considered. Each non-root sends a data packet of 30 bytes after every interval of 60 seconds.

II. Comment 1

The results presented in Perazzo et al. [1] are questionable because the authors considered small sized simulation grid of size 20m×20m (on page 2, IV section, 2^{nd} paragraph of their paper) in their experiments, hence we have implemented the attack and performed an extensive experimental study using same simulation parameters and settings (as provided by one of the co-authors [2]). The impact of DIO suppression attack is analyzed in terms of Packet Delivery Ratio (PDR) and Average End-to-End Delay (AE2ED). Fig. 1 shows the effect of attack on PDR with different intervals ($1, 3, 5$ second) and varying suppression thresholds (DIO redundancy), namely $k = 3, 6, 10$. It is observed that the attack does not have any major effect on overall PDR of the network in each attack scenario, i.e. attack scenario with $1, 3$, and 5 second replay interval. The reason behind this observation can be credited to small size grid (considered by Perazzo et al. [1]) in which the attack which is not able to make any deep impact on routing service of RPL. Fig. 2 illustrates the AE2ED with different replay intervals and suppression thresholds. It can be seen that the attack with shorter interval has a greater impact on AE2ED as compared to attacks with a longer interval. This is because of the congestion and interference caused by the frequently replayed packets. The experimental results depicted in Fig. 1 clearly show that the attack does not severely degrade the PDR of the network deployed in such small sized grid. The only affected routing performance parameter is AE2ED which is increased in case of very short replay interval only, i.e. 1 second, and not presented in the concerned paper. The PDR values achieved under attack scenarios are similar to that of non-attack scenario, this is mainly because of 20m×20m simulation grid.

Parameter	Value
tx_power	0.0
tx_with_gain	false
captureEffect	false
obstacle_attenuation	-10.0
system_gain_mean	-20.0
system_gain	0.0

Table I: MRM parameters considered in Perazzo et al. [1]

The PDR results shown in Perazzo et al. [1] indicate approximately $0.75(75\%)$ value in case of non-attack scenario, which is incorrect. The network deployed in 20m×20m grid has most of the nodes which can directly communicate with root node. Moreover, in a small network where many nodes are directly in communication with the root node the attack is less effective, as the suppression of the DIOs emitted from a node can be balanced by the messages emitted by other neighbors. To prove this claim we generated multiple random topology in Cooja, two of them are shown in Fig 3 and Fig. 4. It can be observed

* Corresponding Author
A. Verma and V. Ranga are with the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India, 136119.
E-mail: abhiverma866@gmail.com, virender.ranga@nitkkr.ac.in

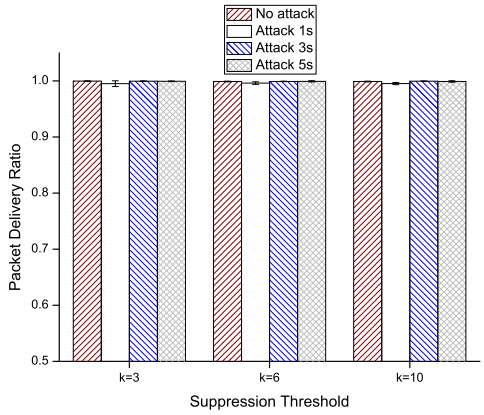

Figure 1: Packet Delivery Ratio of the network

from both the random topology that all the non-root nodes are in direct communication range of root node with good quality links. Thus PDR value in case of non-attack scenario will be close to 1. Irrespective of any random topology, with such small sized simulation grid the PDR under attack scenario will be almost similar to that of non-attack scenario. The authors assumed a static network with no discussion on node failure model, hence it is obvious that the network with considered simulation settings will achieve high PDR in all the experiments. The correct PDR value in such small-sized grid and simulation settings will be close to $1(100\%)$ as shown in Fig. 1. However, if we consider a comparatively large sized network (e.g. $200\text{m}\times200\text{m}$) where most of the non-root nodes may have multiple hops towards the root node, and less non-root nodes are in direct communication range of the root node, the suppression attack can be more effective as it can impair significantly the network formation. In that case, even in normal scenario the PDR value will decrease due to packet loss.

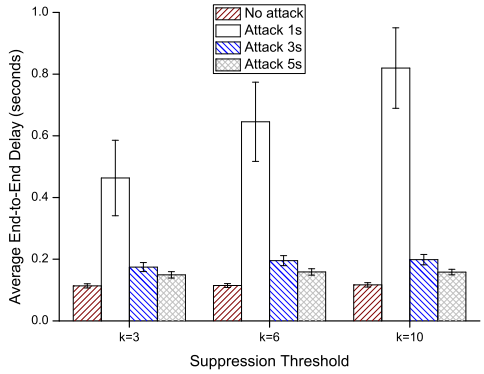

Figure 2: Average End-to-End Delay of data packets

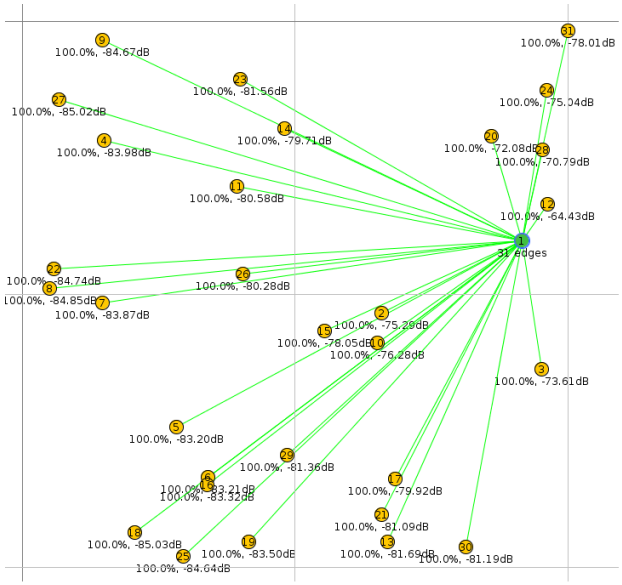

Figure 3: Random topology scenario 1

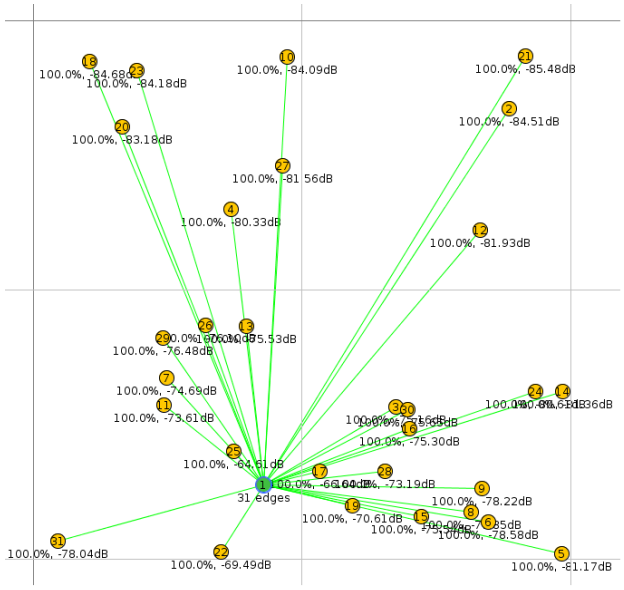

Figure 4: Random topology scenario 1

REFERENCES

[1] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, "DIO Suppression Attack Against Routing in the Internet of Things," *IEEE Communications Letters*, vol. 21, no. 11, pp. 2524–2527, Nov 2017.
[2] C. Vallati, personal communication, 8 May 2019.