Cooja simulator [29] which emulates exactly the binary on real IoT devices is used in our study to conduct the experiments. This has been exploited to emulate the MSPsim [30] of the Tmote sky platform, a well-known IoT sensor device with a low power IEEE 802.15.4 compliant CC2420 radio chip. The radio protocol (UDGM), Unit Disk Graph Radio Medium, is used to simulate the propagation model. For Link layer, we used the CSMA/CA whereas the ContikiMAC was used as the radio duty cycling (RDC) protocol. The attack itself (i.e., DAO attack) has been implemented based on the ContikiRPL library within Contiki operating system. In particular, the attack was mounted by having an insider attacker send DAO messages periodically at pre-specified interval to its parent. The number of attackers in our simulation is set to three nodes.

A periodic data gathering application where sensor nodes send their readings to the DODAG root every minute was simulated at the application laye,r where the DODAG root sends a reply for each received message as a downward traffic. We simulated a stationary network with 50 nodes, the predominant pattern that you will find in a typical home network. The nodes in our simulation were distributed uniformly in an area of 100m x 100m while the DODAG root is positioned outside the deployment area. The simulation is timed out to end in 30 minutes for each simulated scenario.

Table 1 summarizes the experimental parameters used in our study.

Table 1: SIMULATION PARAMETERS.

Parameter Name	Values
Simulation Area	100 x 000 m
Number of nodes	50
Simulation time	1800s
Mote Type	Tmote Sky Mote
Mac/Adaptation Layer	IEEE802.15.4/6LoWPAN
Radio Model	CC2420
Transmission Range(m)	30 m
Interference Range	25 m
Routing Protocol	RPL
Mode Of Operation	Storing mode
Rank Metric	MRHOF
Nominal Capacity	1000mAh
Battery Capacity	1000mAh
Voltage	3 V
Packet sent interval	60 s
Node Distribution	Uniform Distribution

The protocols evaluated for each scenario are RPL, RPL with attack (InsecRPL), RPL under attack with first proposed solution (SecRPL1), RPL under attack with second proposed solution (SecRPL2). In terms of the following metrics:

1) The average number of DAO messages forwarded by the parents in the network (Number of DAOs Forwarded).
2) The average power consumption in the network in milliwatts (Power Consumption (mW)).
3) The Packet Delivery Ratio (PDR) of the upward traffic (i.e., from nodes to the DODAG root)
4) The PDR of downward direction (i.e., from the DODAG root to nodes)
5) The average end-to-end delay from nodes to the DODAG root in seconds (i.e. latency of the upward traffic)
6) The average end-to-end delay from the DODAG root to nodes in seconds (i.e. latency of the downward traffic)

A. THE EFFECT OF THE DAO ATTACK FREQUENCY

In the simulated scenario, three nodes located at the edge of the deployment area farther away from the DODAG root were selected to run as the attacker nodes as this will ensure covering the vast majority of forwarding paths, a phenomenon that an attacker will prefer to maximize the damage in the network. The maximum number of DAOs allowed to be forwarded for each child by a parent is set to 10 empirically (i.e., DAOMax threshold). The attack interval, the rate in milliseconds at which the malicious nodes transmits DAOs, is chosen between 250 and 10000 milliseconds. Five runs were conducted for each simulated scenarios under different random seeds for getting statistically solid results which are depicted in the following graphs.

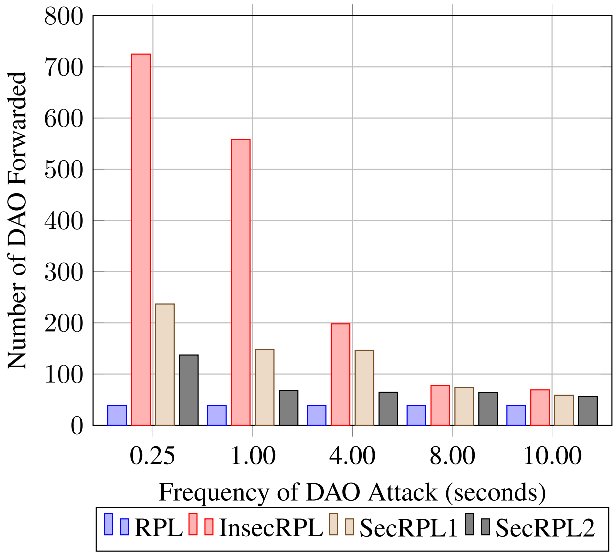

Figure 1: DAOs forwarding Overhead vs Attack intervals

The performance of the network under the simulated scenarios in terms of Forwarded DAO messages and under different attacking intervals is depicted in Figure 1 where the DAOMax threshold per child is set to ten. Figure 1 shows that the overhead of forwarded DAOs in InsecRPL, SecRPL1 and SecRPL2 is higher than that of normal model (i.e., RPL) regardless of the attacking interval value. However, we can also observe from Figure 1 that SecRPL2 has performed better, especially under attack interval of 250 milliseconds, in terms of DAOs overhead compared to other models apart from normal RPL.

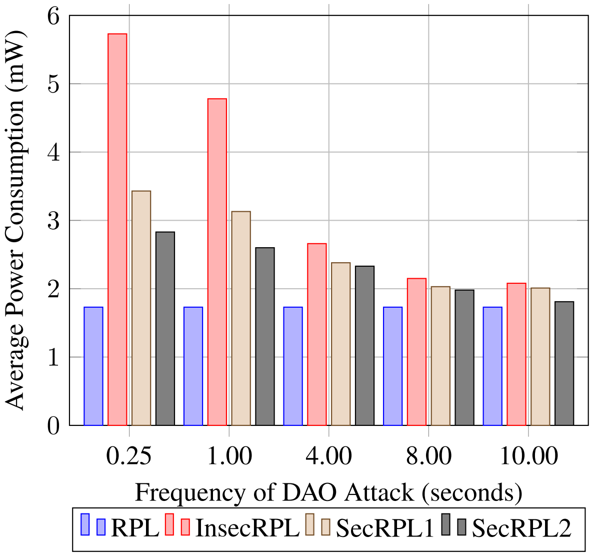

Figure 2: Power Consumption vs Attack interval

The same can be said in relation to the power consumption as demonstrated in Figure 2. This better performance in terms of overhead and power consumption is easily justified by having the parent restricts the number of forwarded messages per child as proposed in our mechanism. It can be observed in Figure 2 that the insecure version of RPL has suffered heavily in relation to average power consumption due the attackers being able to flood the network with large amount of DAOs with no defence mechanism in place. This has been mitigated in both SecRPL1 and SecRPL2 applying the idea of threshold-based security with SecRPL1 showing relatively better performance compared to SecRPL2.

Indeed, the amount of power consumed is calculated in Contiki by adding up the power consumed in four of states of the nodes which are: power consumed in the listening state, power consumed in the idle state, power consumed in the transmission state and power consumed in the running state. Hence, the high overhead in terms of DAOs will surely lead to an increase in the power consumed in the transmission and listening states of the forwarder nodes along the path to the DODAG root, consequently increasing the average power consumption of the network.

The performance of the network in terms of upward latency is shown in Figure 3, whereas upward latency is depicted in Figure 4. Similarly, it is evident from figures that the latency in both downward and upward traffic has been adversely affected by the DAO attack. This again can be attributed to high overhead at the forwarder nodes that induces a higher congestion. In the same context, this degradation in the network performance in terms of latency has been mitigated by applying our mitigation mechanism (i.e., SecRPL1 and SecRPL2) specifically under heavy attacking intervals.

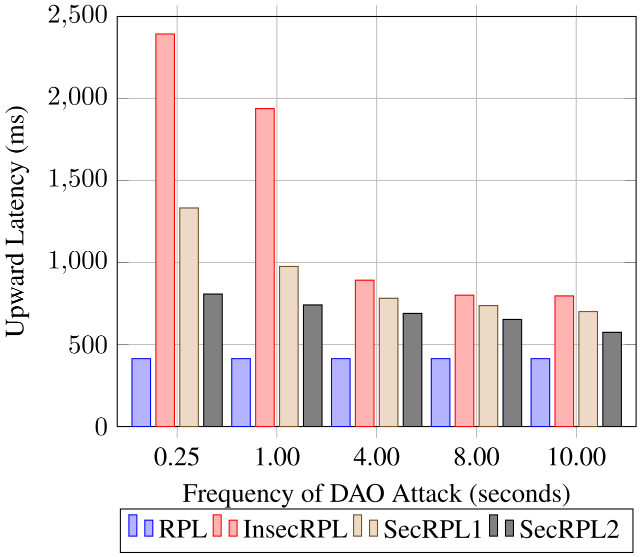

Figure 3: Upward Latency vs Attack intervals

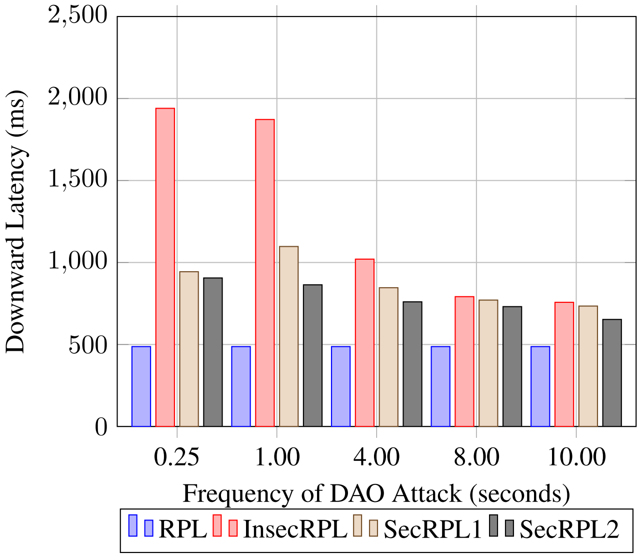

Figure 4: Downward Latency vs Attack intervals

The PDRs of the upward traffic and downward traffic are shown in Figure 5 and Figure 6 respectively. It is again evident from both figures that the PDR in both directions suffer heavily when running the attack under a high attack interval. Note, however, that this may not hold true when mounting the attack under different data rates or topologies. This degradation can be mainly justified by the congestion incurred due to the high overhead at the forwarder nodes under the effect of the attack which again has been alleviated applying our proposed mitigation mechanisms. Both RPLSec1 and RPLSec2 have shown comparable PDR rates in both directions to that of the reference model. The insecure version of RPL (i.e., InSecRPL) has experienced the worst results in terms of PDR, with 7% lower than that of the reference model of RPL. Both SecRPL1 and SecRPL2 have managed to enhance the performance in terms of PDR by up 4% and 6% respectively.

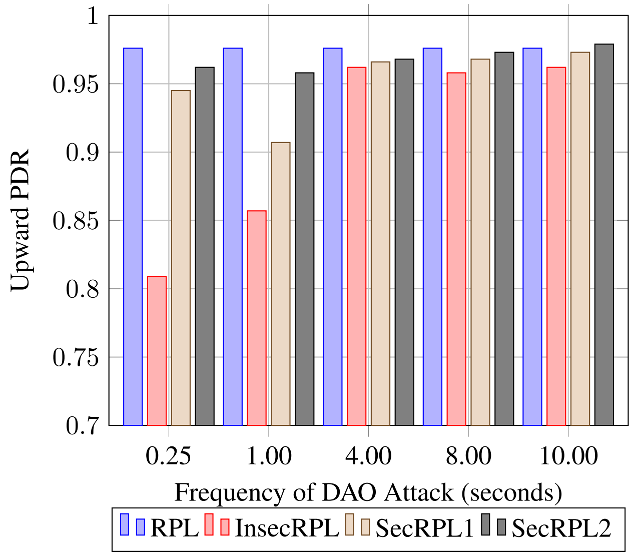

Figure 5: Upward PDR vs Attack intervals

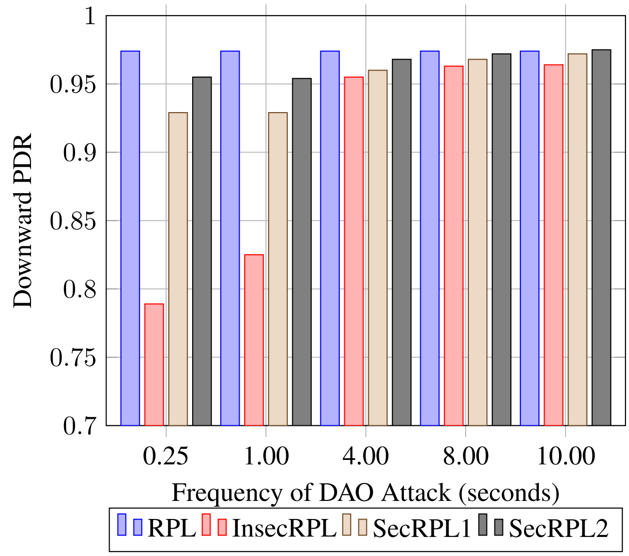

Figure 6: Downward PDR vs Attack intervals

B. THE EFFECT OF INCREASING THE NUMBER OF ATTACKERS

In this scenario, the attack will be implemented by increasing the number of attackers, starting with two attackers and incrementing it by two to a maximum of 10. The value of DAOMax threshold in all cases was fixed to 10 in both RPLSec1 and RPLSec2.

The DAO overheads in terms of the average number of forwarded messages per node with different attacking intervals is depicted in Figure 7. The figure demonstrates that InsecRPL have increased the DAO overhead in comparison with SecRPL2 and RPL. In fact SecRPL1, SecRPL2 have managed to mitigate the effect of the DAO attack, especially in the case under ten attacking nodes with 76.36% and 205% respectively decrease in the DAO overhead compared to the InsecRPL.

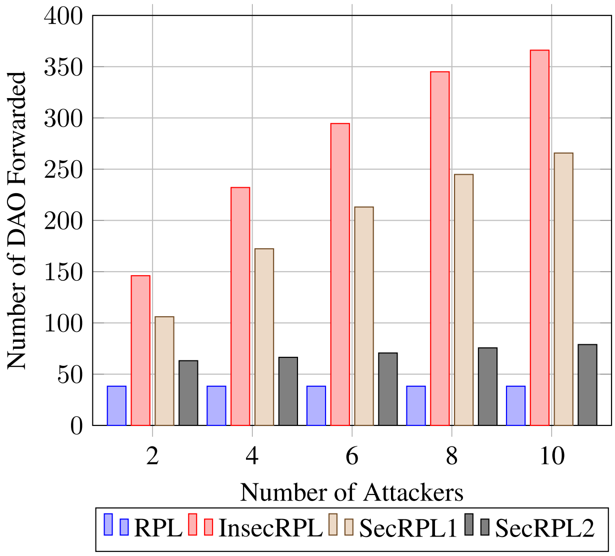

Figure 7: DAOs forwarding Overhead vs Number of Attackers

The superior performance of SecRPL2 over SecRPL1 is related to the value of the DAOMax chosen as SecRPL2 can only forward up to 10 DAOs in total in a given interval while SecRPL1 can forward 10 DAOs per destination, hence, the superiority of SecRPL2 over SecRPL1. This has been translated into a decrease in the power consumption under the proposed schemes as depicted in Figure 8 which can be easily justified by the capacity of secure versions of RPL (i.e., SecRPL1 and SecRPL2) to restricted the number of forwarded DAOs per child due to the attack. Both mitigation schemes SecRPL1 and SecRPL2 were able to reduce the effect of the attack by 24% and 87% respectively; however, both consumed more power than the reference network (RPL).

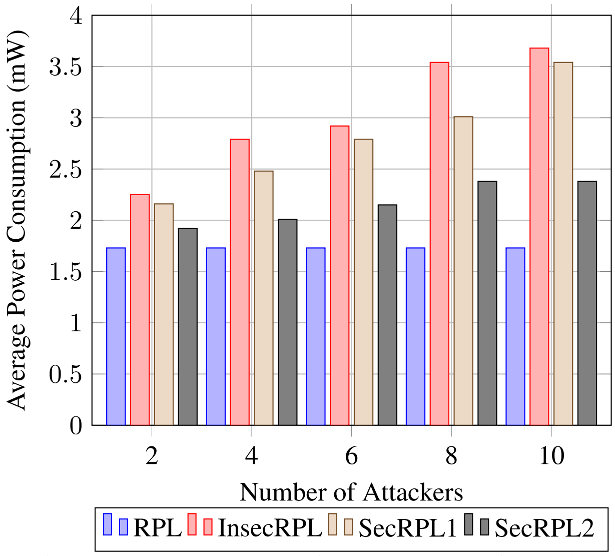

Figure 8: Power Consumption vs Number of Attackers

Figures 9 and 10 demonstrate the latency of the upward and downward traffic respectively for protocols under comparison. Similarly, it is evident that the latency has suffered significantly under the attack for both traffic patterns as a result of the significant congestion at the forwarder nodes. SecRPL1 has improved the upward latency by 65.88% and the downward latency by 181.19%. With SecRPL2 both upward and downward latency are greatly reduced outperforming SecRPL1 which can be attributed again to the DAO threshold chosen.

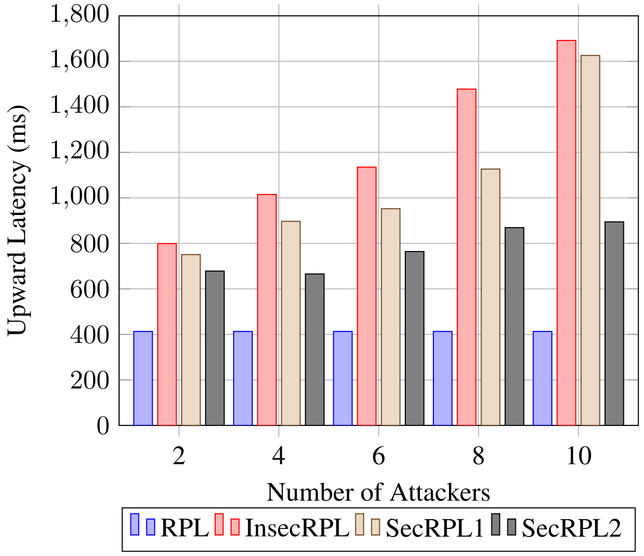

Figure 9: Upward Latency vs Number of Attackers

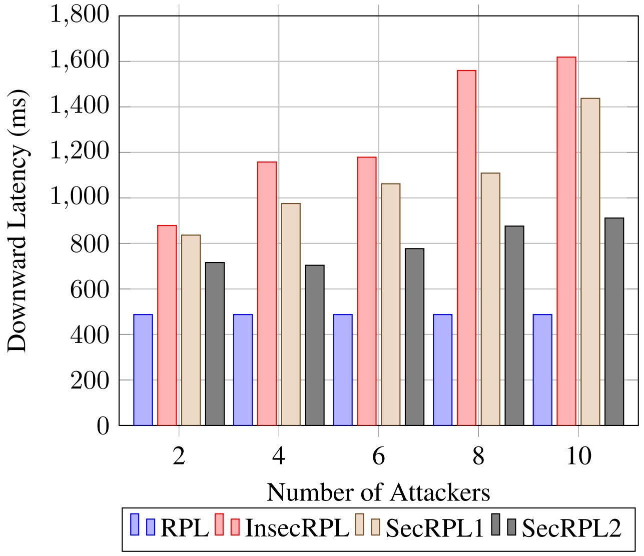

Figure 10: Downward Latency vs Number of Attackers

The PDRs of upward and downward traffic for the four models are depicted in Figure 11 and Figure 12 respectively. The figures again demonstrate that the PDRs of both traffic patterns have been affected negatively and the amount of the affect is proportional to the number of the attackers in the network, which can be attributed to the congestions experienced by the forwarder nodes. The degradation in the PDR rate has been overcome by the proposed solutions, in which we almost restore the same efficiency of the reference model. From Figure 11 and Figure 12, we can conclude that SecRPL1 has slightly improved PDR over InsecRPL with a 2% increase. SecRPL2, however shows an increase of 3% indicating best performance comparable to the reference model with 3% difference.

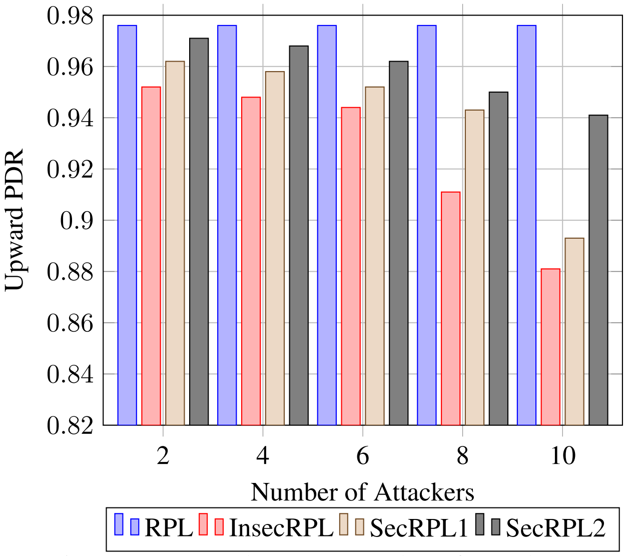

Figure 11: Upward PDR vs Number of Attackers

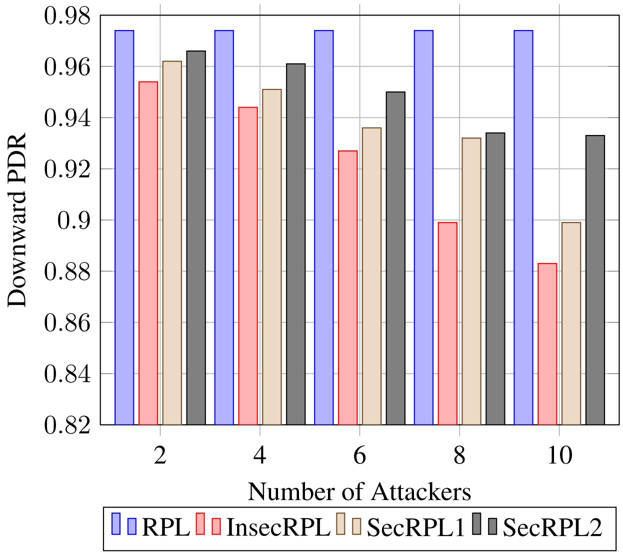

Figure 12: Downward PDR vs Number of Attackers

C. THE EFFECT OF THE THRESHOLD PARAMETER (DAOMAX)

We also investigated the effect of the threshold value (i.e. DAO threshold Max) on the network reliability in terms of PDR. Intuitively, the smaller the value of the threshold, the lower the DAO overhead and power consumption but at the expense of network reliability. We have depicted how setting the threshold value can affect the performance of the network in terms of mentioned metrics in Figure 13 and Figure 14. It is clear from Figure 13 and Figure 14 that selecting a very small value for the threshold has reduced the control overhead and power consumption in both mitigation mechanisms with SecRPL2 again being more efficient in overcoming the effect of the attack, reducing the DAO overhead and the power consumption to up to 48.5% and 18% respectively compared to SecRPL1.

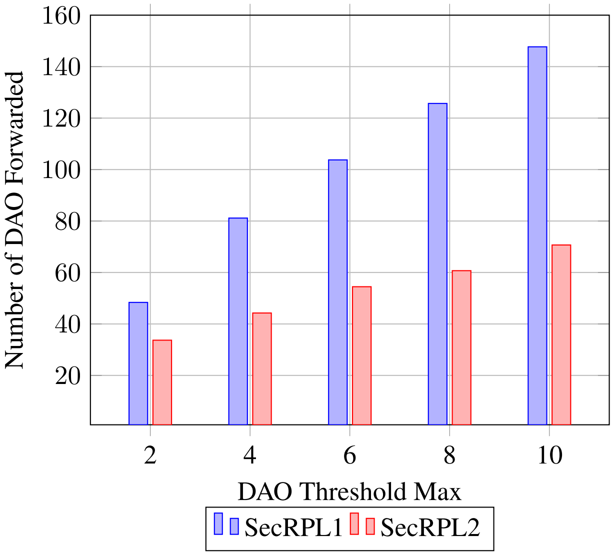

Figure 13: DAOs forwarding under various DAO Threshold

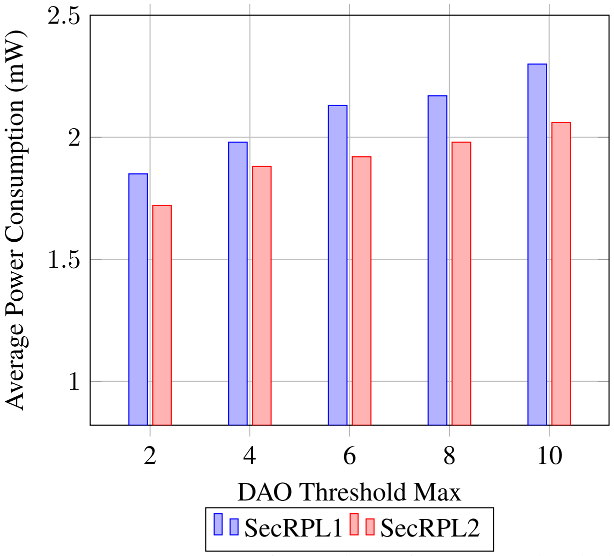

Figure 14: Power consumption under various DAO Threshold

However, this has impacted the PDR of the downward traffic negatively as illustrated in Figure 15 and Figure 16. This holds true for any value of the threshold less than four. This can be explained easily by the fact that the small value of the threshold will lead into preventing the forwarding of critical DAO messages necessary to build more efficient downward routing paths, hence, the lower PDR of the downward traffic. The figures show also that SecRPL2 performs better than SecRPL1 under both traffic patterns in terms of PDR as the DAO threshold are only restricted partially.

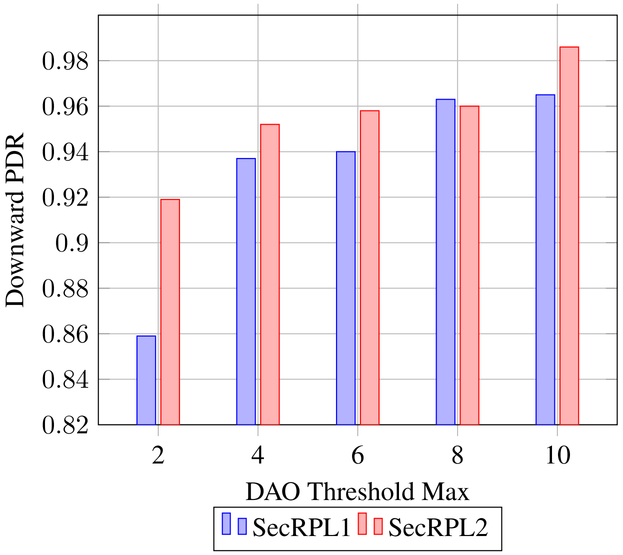

Figure 15: Downward PDR under various DAO Threshold

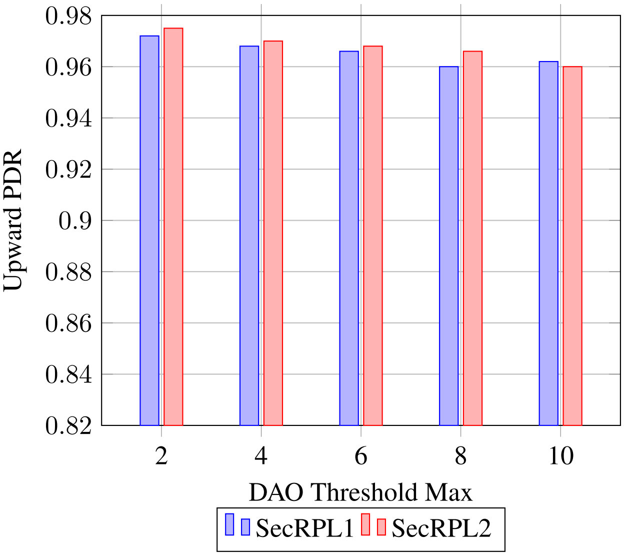

Figure 16: Upward PDR under various DAO Threshold

Fig. 17 and 18, show the effect of both mechanisms on downward and upward latency. It indicates that assigning lower threshold values will reduce the latency. SecRPL2 was able to much better overcome the effect of the attack, decreasing upward and downward latency by 53.57% and 53.71%, respectively in comparison to SecRPL1.

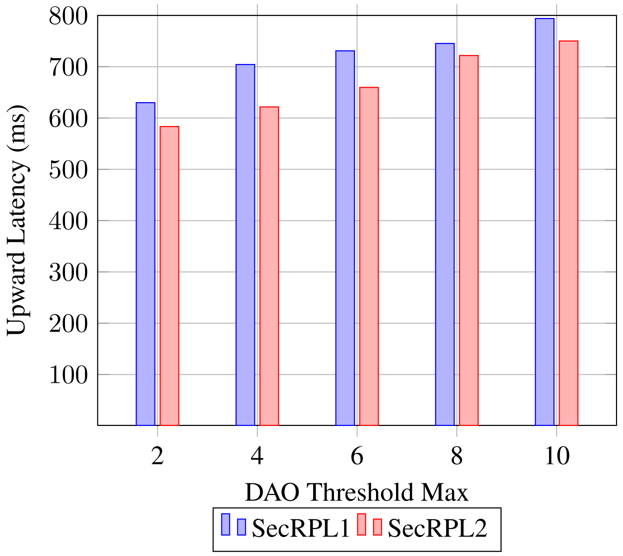

Figure 17: Upward Latency under various DAO Threshold

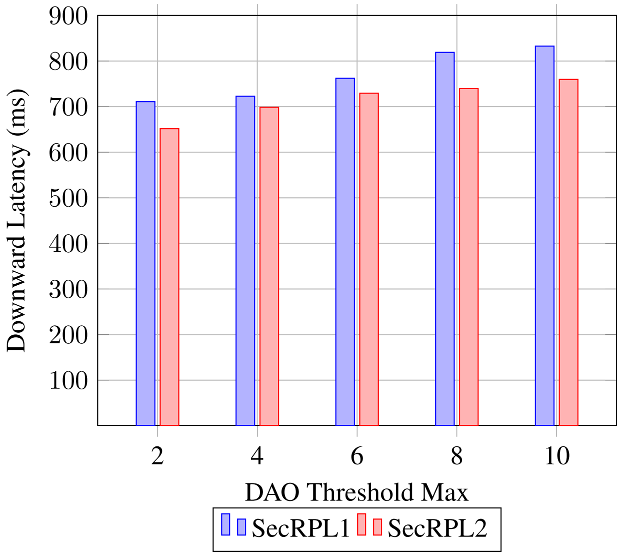

Figure 18: Downward Latency under various DAO Threshold

VIII. CONCLUSIONS

In this study, we have evaluated the effect of the DAO flooding attack on the network performance in terms of power consumption, packet delivery ratio and latency under different scenarios and operating conditions. The DAO attack can be mounted in IoT networks by having an attacker node transmitting periodically DAO messages to its preferred parent which in turn will forward the received DAOs to its own parent and so on until the DAOs reach the final destination which is the DODAG root. The DAOs in the context of the RPL protocol are transmitted in end-to-end approach (i.e., from sensors to the sink) which makes them different from other RPL's flooding attacks including the DIO and DIS attacks. Hence, not only the immediate neighbors of the attackers will get affected and harmed by the attack, but also all forwarding nodes to the DODAG root. In fact, an attacker node located at the network edge and transmitting a DAO message will prompt all other nodes in the forwarding path to the DODAG root to forward such a message. The simulation results have shown how the attack can damage the network performance by significantly increasing the DAO overhead and power consumption. The results have also demonstrated that the DAO attack may moderately affect the reliability of the downward traffic under specific conditions. To overcome the effect of the attack, two mitigation mechanisms have been proposed and evaluated showing a good capacity in restoring the optimal performance of the network in terms of the respective metrics.

References

[1] J. Hui and P. Thubert, "Rfc 6282 internet engineering task force rfc 6282," Compression Format for IPv6 Datagrams over IEEE 802.15. 4-Based Networks, 2011.

[2] J. W. Hui and D. E. Culler, "Extending ip to low-power, wireless personal area networks," IEEE Internet Computing, no. 4, pp. 37–45, 2008.

[3] J. W. Hui, "The routing protocol for low-power and lossy networks (rpl) option for carrying rpl information in data-plane datagrams," 2012.

[4] T. Clausen, U. Herberg, and M. Philipp, "A critical evaluation of the ipv6 routing protocol for low power and lossy networks (rpl)," in 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 365–372, IEEE, 2011.

[5] J. Vasseur and D. Culler, "Routing over low power and lossy networks (roll)," IETF Working group, 2008.

[6] A. Dvir, L. Buttyan, et al., "Vera-version number and rank authentication in rpl," in 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 709–714, IEEE, 2011.

[7] 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, 2013.

[8] M. Landsmann, M. Wahlisch, and T. C. Schmidt, "Topology authentication in rpl," in 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 73–74, IEEE, 2013.

[9] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Mitigation of topological inconsistency attacks in rpl-based low-power lossy networks," International Journal of Network Management, vol. 25, no. 5, pp. 320–339, 2015.

[10] A. Mayzaud, R. Badonnel, and I. Chrisment, "Detecting version number attacks in rpl-based networks using a distributed monitoring architecture," in 2016 12th International Conference on Network and Service Management (CNSM), pp. 127–135, IEEE, 2016.

[11] F. Ahmed and Y.-B. Ko, "Mitigation of black hole attacks in routing protocol for low power and lossy networks," Security and Communication Networks, vol. 9, no. 18, pp. 5143–5154, 2016.

[12] A. Aris, S. F. Oktug, and S. B. O. Yalcin, "Rpl version number attacks: In-depth study," in NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, pp. 776–779, IEEE, 2016.

[13] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.

[14] 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, 2017.

[15] U. Herberg and T. Clausen, "A comparative performance study of the routing protocols load and rpl with bi-directional traffic in low-power and lossy networks (lln)," in Proceedings of the 8th ACM Symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, pp. 73–80, ACM, 2011.

[16] D. Sharma, I. Mishra, and S. Jain, "A detailed classification of routing attacks against rpl in internet of things," International Journal of Advance Research, Ideas and Innovations in Technology, vol. 3, no. 1, pp. 692–703, 2017.

[17] 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 Communications Letters, vol. 23, no. 1, pp. 68–71, 2018.