On the Impact of the RPL Decreased Rank Attack on 6TiSCH Networks

Mohammed Mahyoub, Sazzad Hossain, and Ashraf Matrawy

Abstract—**The 6TiSCH protocol stack was designed to provide a reliable and time-bound multi-hop routing solution for the Industrial Internet of Things (IIoT), integrating the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) and Time-Slotted Channel Hopping (TSCH) protocols seamlessly. However, deviations from standard procedures by malicious nodes can severely affect network formation and operations, resulting in degraded performance. This study investigates the impact of the decreased rank attack (DRA) on RPL within the 6TiSCH network, examining its effects on network operations and performance. Experimental evaluation reveals that DRA can lead to an average delay of 21.4% in network formation and runtime disruptions, thereby affecting the 6TiSCH synchronization process. Consequently, node departures from the network and subsequent rejoining to maintain the topology increase by an average of 60.71%. To deal with this disruption, the nodes need to send more keep-alive and RPL messages, resulting in an average increase of 69.70% and 20.08%, respectively, leading to a 49. 9% increase in energy depletion. Furthermore, the DRA reduces the packet delivery ratio and increases the average end-to-end packet delay by averages of 5.13% and 20%, respectively. However, it is important to note that the impact of the attack can vary significantly depending on the specific configurations and setups used, such as network topology, network size, attacker position, neighboring density, and RPL/TSCH parameter settings.**

Index Terms—**6TiSCH, TSCH, RPL, Decreased Rank Attack, Performance Evaluation, Industrial IoT.**

I. Introduction

The time-slotted channel hopping protocol (TSCH) is widely adopted as the Medium Access Control (MAC) mechanism in industrial applications. It offers predictable and deterministic communication, making it essential for real-time and mission-critical industrial applications [1]. TSCH protocol enhances the resilience of communication against interference by spreading communications across different time slots and frequency channels. The 6TiSCH stack (IPv6 over TSCH mode of IEEE 802.15.4e), which is based on TSCH, encompasses the management of a distributed communication schedule that continuously adapts to network changes [2]. The 6TiSCH Working Group[1] established mechanisms for seamless integration of the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) [3] to efficiently operate on the TSCH link layer protocol. This highlights the importance of the 6TiSCH protocol stack for the Industrial Internet of Things (IIoT) as it enables reliable and energy-efficient communication between devices in industrial settings.

The minimal configuration (6TiSCH-MC) [4] specified by the working group in the *RFC* 8180 outlines the interaction between the TSCH mode and the upper layers, as well as the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL), to promote optimal performance and ensure a reliable mapping between the RPL routing topology and the TSCH time source graph. The process of forming a 6TiSCH network involves nodes gradually joining the TSCH network and executing RPL operations to gather topology information and determine the most efficient multi-hop routes for data transmission. To establish network configuration and allocate transmission opportunities during the bootstrap phase, 6TiSCH-MC utilizes a static resource allocation implemented by all nodes to facilitate the transmission of control messages during network formation.

To ensure smooth network operations and successful initial topology discovery processes, it is essential to adhere to the standard procedures of TSCH and RPL. Deviation from these standards by malicious nodes can severely disrupt or impede network functions [5]–[8]. RPL, in particular, is vulnerable to several types of attacks, including the DIS attack [9], Sybil attacks, selective forwarding attacks, and sinkhole attacks [10]. Among these attacks, the decreased rank attack (DRA) has received significant attention in the literature [11].

DRA Explanation: In this type of attack, the malicious node initially joins the network as a regular node, which means that it gets a legitimate rank that reflects its distance from the root. However, whenever the malicious node advertises its rank to the neighborhood, it includes a fake rank that is less than its real rank. By presenting a lower rank, the attacker appears to be more favorable in terms of distance from the root and routing efficiency. As a result, neighboring nodes select the attacker as their preferred parent, allowing the attacker to gain control over the routing path and influence network traffic. This tactic allows the attacker to manipulate the behavior of the network and potentially carry out further malicious activities within the compromised network [12].

Paper Contribution: As this area is gaining significant attention because of its importance to IIoT, this paper makes the **timely contribution** to investigating the impact of the DRA that specifically targets the RPL protocol to analyze its effect on 6TiSCH networks. Although the DRA has been explored in existing research, its impact on 6TiSCH networks has not yet been addressed. Existing studies that we found in the literature, such as [12], have focused on Carrier-Sense Multiple Access (CSMA) as a link layer protocol. Unlike CSMA, which does not rely on the routing protocol (i.e. RPL) for its operations, TSCH in the context of 6TiSCH heavily

Mohammed Mahyoub, Sazzad Hossain, and Ashraf Matrawy are with the School of Information Technology, Carleton University, Ottawa, Canada (e-mail: mohammedmahyoub@cunet.carleton.ca; amatrawy@sce.carleton.ca; sazzadhossain1206@gmail.com).

[1] 6TiSCH WG, https://datatracker.ietf.org/wg/6tisch/about/

depends on the routing protocol. Therefore, it is not clear to what extent the current observations and conclusions about DRA's impact on CSMA will apply to 6TiSCH. To the best of our knowledge, this paper is the first study to explore how the DRA in the RPL protocol can affect the formation, operations, and performance of 6TiSCH networks.

II. RPL's Relation to TSCH

This section briefly presents the TSCH shared cell, the 6TiSCH network formation process (i.e. joining process), and how the TSCH and RPL protocols relate to each other.

TSCH Shared Cell: TSCH divides time into fixed-length intervals known as slot frames. Each slot frame consists of multiple timeslots, and within each timeslot, a node can utilize a set of available frequencies or channels. This creates a matrix-like schedule where cells represent potential communication opportunities between a node and its neighboring nodes. In the context of 6TiSCH-MC, it is recommended to use only one cell per slot-frame, known as a minimal or shared cell. This shared cell is used to transmit control messages from both the TSCH and RPL layers. TSCH control messages include enhanced beacon (EB) and keep alive (KA) messages, while RPL control messages include DODAG Information Element (DIO), Destination Advertisement Object (DAO), and DODAG Information Solicitation (DIS). As the shared cell operates on a contention-based link, it requires a CSMA / Collision Avoidance (CA)-like protocol to allow nodes to transmit their control messages.

Network Formation: To become fully functional within the network, a new joining node, also known as a pledge, undergoes two essential steps. First, the pledge needs to establish a connection with the TSCH network, becoming a TSCH-synchronized node. This synchronization allows the pledge to engage in direct single-hop communication with its neighboring nodes. In this step, the pledge waits to receive a valid EB packet from already joined nodes. EBs are generated at regular intervals and contain timing information, such as slot frame length, timeslot timing, and channel hopping sequence, which facilitates initial synchronization. The pledge may receive multiple EBs, from which it chooses one sender as a Joined Proxy (JP). The selection of the JP is influenced by connectivity metrics such as link quality and the value of the Join Metric contained within the EB.

Subsequently, the node needs to join the logical topology of the RPL routing protocol, becoming an RPL-joined node. This step allows the node to populate its routing table and gain the ability to forward data over multiple hops, ensuring efficient and reliable data transmission across the network. To join the RPL topology, the synchronized node waits to receive DIO messages from its neighbors. DIO dissemination is controlled by the Trickle algorithm. Additionally, the synchronized node periodically sends DIS messages to solicit DIO messages and join the RPL topology. It may receive multiple DIO messages from neighbors, among which it selects one as a preferred parent. The preferred parent is the designated neighbor for data transfer to the root node and is chosen based on factors such as the neighbor's rank, representing its relative position or the cost to reach the root [13]. To calculate the rank of a node, the 6TiSCH-MC protocol incorporates the Expected Transmission Count (ETX) [3] and follows the normalization guidelines specified by the Objective Function Zero [14].

RPL and TSCH Relationship: Once the pledge becomes a joined node, 6TiSCH-MC suggests aligning the link layer topology (TSCH) and the routing topology (RPL) by representing the Join Metric field as the RPL rank. This alignment enables the pledge to choose a JP close to the root of the network, increasing the likelihood that it is the preferred parent in the RPL topology as well. The joined node synchronizes its timing schedule with the JP using KA messages. Since the node's rank is calculated based on the Expected Transmission Count (ETX), it is a dynamic value that can change over time due to network congestion. Each node is required to react to changes in its current parent rank or any neighboring node, which are detected through the DIO announcements. The response includes adjusting its own rank, switching its parent if the current parent has a higher rank than the sending neighbor, and sending a DAO message to the root to report the new parent. These changes affect all the child nodes. When a parent switch occurs, resynchronization with the new parent is required at the TSCH layer, facilitated by KA messages.

III. Simulation Setup

We conducted a set of experiments to evaluate the impact of the DRA on 6TiSCH network operations and performance using the Contiki-NG[2] operating system and the Cooja emulator [15]. The emulator comes within the Contiki NG, which creates the node with the exact configuration as real-world devices. It allows the uploading of code to work directly in real devices and performs hardware-level simulations utilizing real hardware profiles of emulated nodes. It permits taking advantage of the network models already in place, such as radio propagation, medium interference, typologies, and connection quality, to assess the project design in actual-world scenarios. The network shown in Fig. 1 is considered for these experiments. It has a simple tree topology with 12 nodes in which Z1 motes are adopted in this simulation. All participating nodes in the setup employ the unit disc graph medium (UDGM) with a uniform transmission range of 30 m and an interference range of 50 m. We set the RPL objective function to OF0 as specified in the 6TiSCH-MC specifications. The TSCH and RPL parameters are set based on the default recommended configurations. The attacker was almost placed in the center of the network with an ID of 13. This malicious node consistently reduces its actual rank by 70% prior to transmitting the updated DIO message to the neighborhood. The average of neighbor densities is 4 neighbors, which forces the creation of a multihop topology to reach the root. Periodically, all nodes except the root and the attacking node transmit four data packets per minute toward the root of ID #1. The packet size is 127 bytes, of which 15 bytes are used by the payload and the remaining by networking and framing overhead. The experiment lasts for 30 minutes. The reported results are averaged over 10 runs with random seed values. A

[2] Contiki-NG OS, https://github.com/contiki-ng

JavaScript code is deployed to extract the data and log them to text files for further examination. Furthermore, all the log files from each run are analyesd using a bash shell script to calculate the necessary statistics. The graph generation process was automated by developing GNU PLOT-based scripts. The error bar is shown for the 95% confidence interval to ensure the statistical significance of the results.

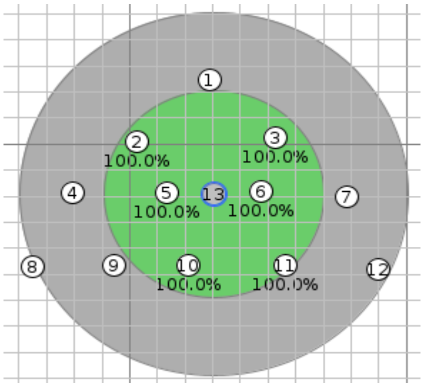


Fig. 1. The figure illustrates the network topology. The node with **ID #13** is identified as the malicious node. The green and gray areas represent the transmission and interference ranges of the malicious node, respectively. These ranges are consistent for all other nodes in the network. The sink (i.e. root), labeled **1D #1**, is located at the first row of the topology.

IV. Results and Discussion

In this section, we discuss the findings of our evaluation of the impact of the DRA on 6TiSCH networks. The evaluation is divided into two parts: the impact of the DRA on (1) 6TiSCH network operations and (2) 6TiSCH network performance. In this evaluation, we report the results for two scenarios: when the network is attack-free and when DRA is applied. These two scenarios are labeled ATTK-FREE and DRA, respectively, in the following figures.

A. The Impact of the DRA on the Network Operations

The operations under evaluation include the parent switching process, RPL-related message transmission, KA message transmissions, leaving process, and joining process (i.e., network convergence). The impact of the DRA attack on these operations is closely tied to its effect on the RPL layer, which interacts closely with the TSCH layer.

Parent-switching and RPL control messages (Fig. 2 and Fig. 3): The default operation of the RPL protocol is such that if a node engages in an attack and modifies its rank value, the impact extends beyond its neighboring nodes and can also affect the child nodes associated with it. This situation arises because each node is obligated to respond to the DIO message received from the attacking node in the following ways: a) Adjusting its rank in response to the message, b) Changing its parent to the attacker if the rank through the current parent is higher than the rank through the attacker, c) Sending an updated DIO to the neighborhood to inform them about its new rank, and d) Sending a DAO message to the root node to inform about the new parent. By modifying its rank value, the attacking node triggers a chain of events that affect the connectivity and hierarchy of neighboring and child nodes, ultimately impacting the overall network structure.

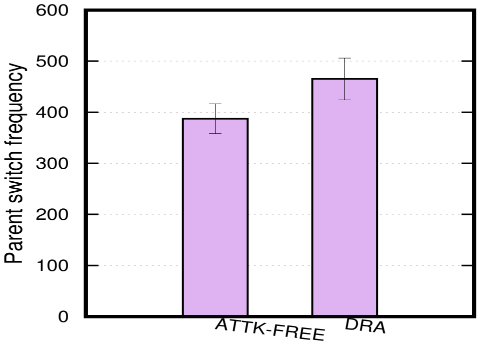
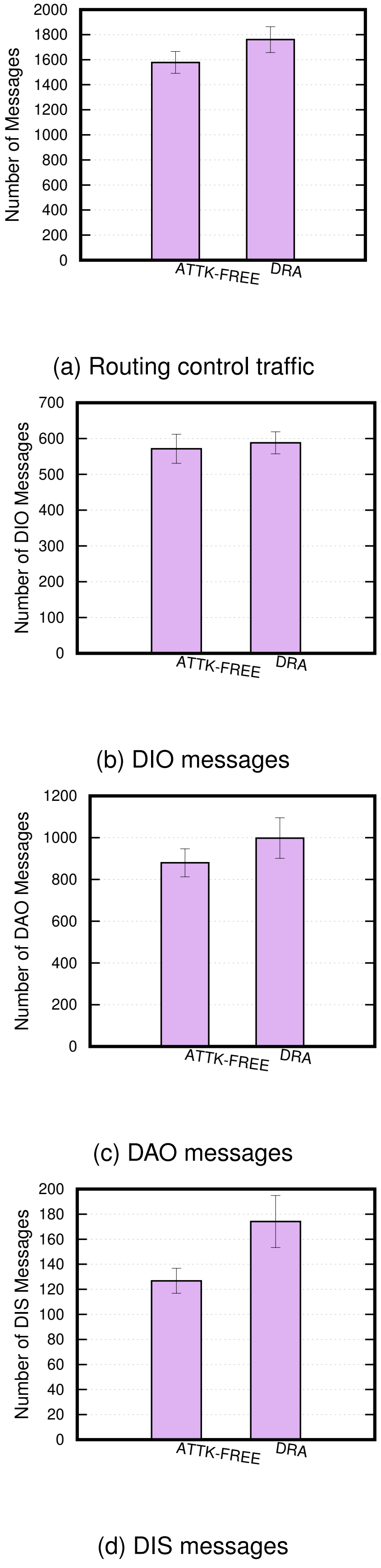


Fig. 2. The impact of the DRA on the RPL parent switching

Our results find that, as shown in Fig. 2, the DRA contributes to the increase of the total number of parent switching counts by an average of 20.08%. This impact increases the number of RPL control packets (that is, DIO, DAO and DIS) transmitted by nodes in the network, as shown in Fig. 3a, by an average of 11.54%. This includes the increase in the number of DIOs, DAOs, and DISs by an average of 2.90% which is not significant (Fig. 3b), 13.44% (Fig. 3c), and 37.30% (Fig. 3d), respectively. The increase in the number of DIS messages is mainly due to nodes waiting to join the network, as explained later in this paper . These nodes periodically broadcast DIS messages to request DIOs and join the network. Once they receive at least one valid DIO, they cease the solicitation process. The increasing frequency of parent changes has a negative impact on network stability, leading to increased control packet overhead and increased energy consumption of nodes.

KA messages (Fig. 4a): In 6TiSCH networks, the nodes rely on their parent node, selected through the RPL protocol, as the time source for synchronization. When a node switches its parent, the synchronization process and time source must be updated to reflect the new routing topology. This process includes rescheduling communication with the new parent and updating the timing parameters. Consequently, the frequent need for updates results in a higher number of KA messages sent in the TSCH layer of the network. Fig. 4a depicts that the DRA results in an average increase of 69.70% in KA messages compared to the attack-free scenario. These messages are used to ensure that nodes maintain synchronization with each other. However, this higher frequency leads to congestion, energy consumption, and reduced network capacity, as discussed in the next subsection.

Node departure frequency (Fig. 4b): TSCH protocol uses information from the RPL protocol to allocate resources such as time slots and communication channels. If a malicious node manipulates its rank, it can gain access to more resources than other nodes, leading to unfair resource allocation and network congestion. Additionally, the increased transmission of RPL control messages, as well as the necessary KA messages, causes contention at the shared slot assigned for transmitting



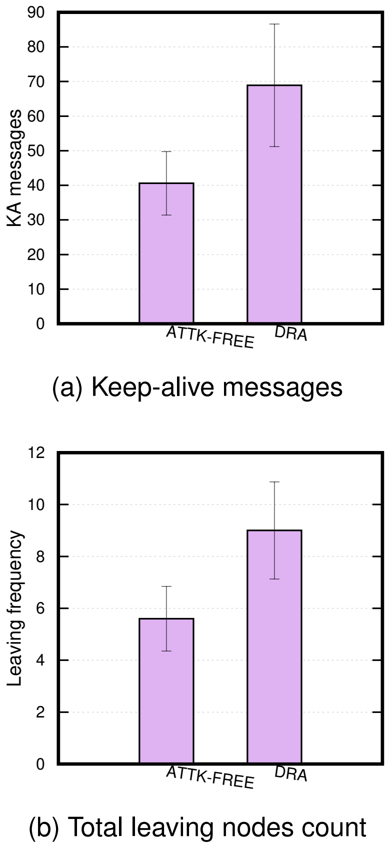
(a) Routing control traffic

(b) DIO messages

(c) DAO messages

(d) DIS messages

Fig. 3. The impact of the DRA on the RPL control messages transmission



(a) Keep-alive messages

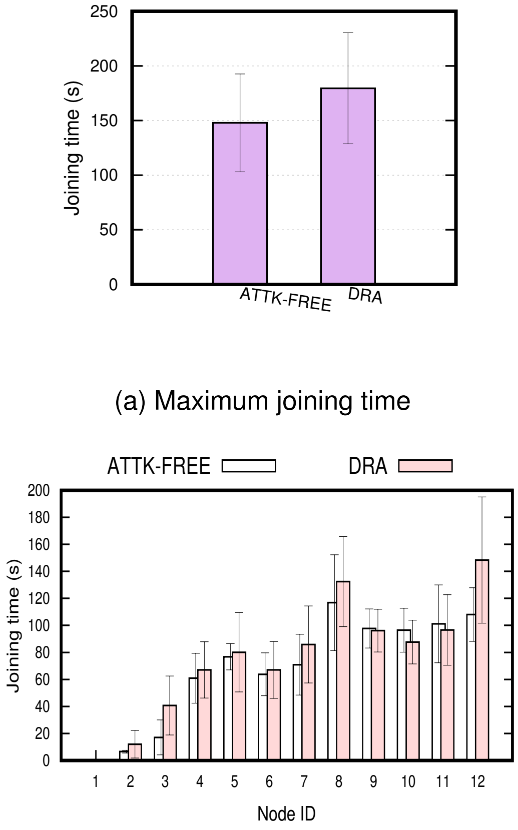
(b) Total leaving nodes count

Fig. 4. KA messages and node departure frequency

them. Experiments have revealed that due to the high congestion in the shared cell, the DRA attack hinders legitimate nodes from efficiently transmitting their control messages such as DISs. Furthermore, these nodes face difficulties receiving other control messages, including EBs and DIOs. As a result, the nodes become desynchronized with the TSCH network and may attempt to rejoin as new nodes to maintain connectivity and repair the topology, leading to an increase in the leaving count, which in turn increases the parent switch count. Fig. 4b shows that the DRA increases the frequency of nodes leaving by an average of 60.71%.

Network convergence (Fig. 5): Network convergence time is a crucial parameter to assess network performance, as it directly affects network formation and topology maintenance [16]. The maximum joining time in Fig. 5a represents the time required for the last node to join the network (that is, the network convergence time). As seen in the figure, DRA increases the average maximum joining time for nodes by approximately 21.4% compared to the attack-free scenario. However, the overlap in confidence intervals suggests that this difference may not be statistically significant. This could be attributed to factors such as the specific network topology, network size, and other configuration setups used in the study. These factors might have influenced the overall impact of DRA-induced contention on joining time. It is possible that in different network setups, the effect of DRA-induced contention on joining time could be more pronounced or statistically significant. Further analysis of the joining time per node in

Fig. 5b indicates that the time required for nodes to join the network increases as they are farther from the root, consistent across both scenarios evaluated in the study. For example, as illustrated in the figure, nodes with IDs 8 and 12 exhibit the highest joining time. This is attributed to their position as the furthest nodes from the root.



(a) Maximum joining time

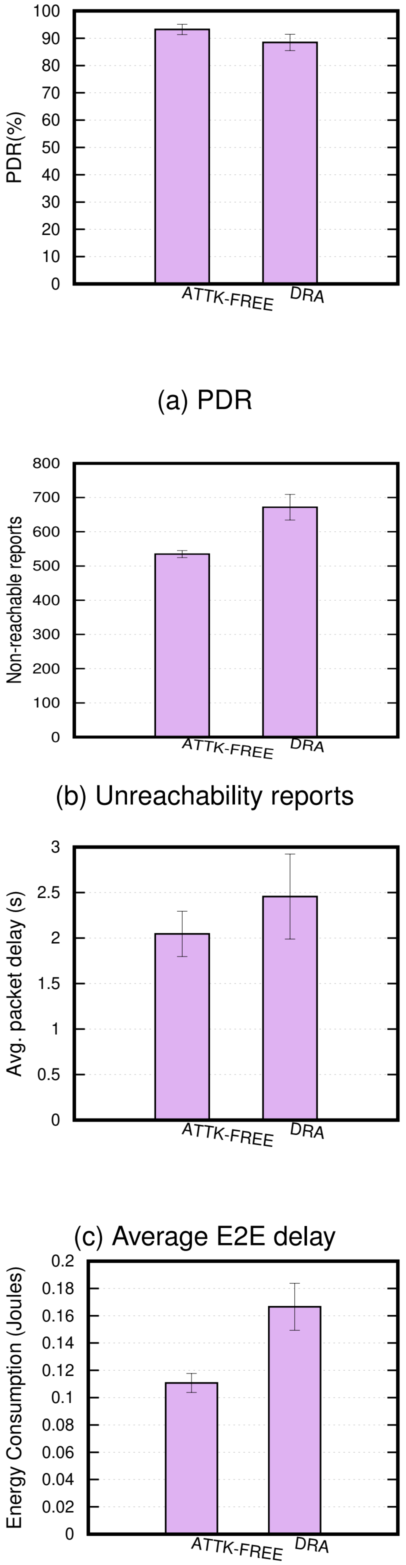
(b) Joining time per node

Fig. 5. The impact of DRA on network convergence. It is important to note that, for Fig. 5b, the identification numbers assigned to the nodes do not necessarily correspond to their physical distance from the root. Nodes #8 and #12 are the farthest from the root in the studied topology.

B. The Impact of DRA on the Network Performance

The evaluation of network performance, on the other hand, includes network reliability in terms of packet delivery ratio (PDR), reachability, packet end-to-end (E2E) delay, and energy consumption. The 6TiSCH stack was designed with the aim to fulfill the high-reliability requirements of industrial IoT applications [1]. In a 6TiSCH network, the RPL protocol plays a crucial role in determining the best path for data transmission based on the DODAG structure. However, if a malicious node manipulates its rank with the DRA to become the preferred parent of other nodes, the resulting routing topology can be suboptimal, leading to reduced throughput, increased latency (i.e., end-to-end delay), and increased energy consumption. To assess the reliability of 6TiSCH in the presence of the DRA, this section evaluates the PDR and the node reachability. Additionally, the E2E delay of data packets and the average energy per delivered packet consumed by nodes in the network are analyzed.

PDR and reachability (Fig. 6a and Fig. 6b): In these experiments, each node in the network checks whether it can



(a) PDR

(b) Unreachability reports

(c) Average E2E delay

(d) Energy consumption

Fig. 6. The impact of the DRA on the 6TiSCH network performance and energy consumption

reach the root before sending an application data packet. If it does, it sends the packet and, eventually, the PDR is calculated as the ratio of packets delivered at the root to the total number of packets sent by all nodes throughout the entire simulation time. On the other hand, if a sending node cannot reach the root because it had not yet joined the network or was in a leaving state and trying to rejoin the network, it reports an unreachability issue. Fig. 6a shows that the PDR decreased by an average of 5.13% compared to the attack-free scenario, indicating that the DRA reduces the network's ability to deliver packets successfully. Fig. 6b shows that the number of reports of unreachability increased significantly due to the DRA by an average of 25.57%, indicating that the attack makes it more difficult for the nodes to join the network and increases the times when the nodes are not fully operational.

Packet E2E delay (Fig. 6c): In industrial applications, real-time communication is critical to ensure efficient and safe operations. The 6TiSCH stack was designed to support time sensitive applications by providing low-latency deterministic communication [17]. For this, measuring the packet E2E delay is crucial to assessing the ability of 6TiSCH networks to meet these requirements. In this experiment, we evaluated the average packet E2E delay in the presence of the DRA. Our results in Fig. 6c indicate that the DRA contributed to an average increase of 20% in the E2E delay compared to the attack-free scenario.

Energy consumption (Fig. 6d): Finally, evaluating the energy consumption of 6TiSCH networks is important because this consumption can have a significant impact on the life expectancy of battery powered devices. In many industrial applications, devices are expected to operate for extended periods of time without the need for frequent battery replacements or recharging [18]. Therefore, we evaluate the energy consumption of 6TiSCH networks in the presence of the DRA. Our results in Fig. 6d show that the average energy consumed per packet delivered was significantly higher in the presence of the DRA compared to the attack-free scenario by an average of 49.9%. The increased energy consumption observed in this experiment can be attributed to several factors: i) the DRA caused an increase in the number of keep-alive messages at the TSCH layer, frequent re-scheduling and rejoining, and RPL-related control messages, and ii) the increased congestion in the shared cell resulted in increased queuing delays and prolonged channel scanning, which also contributed to higher energy consumption.

V. Conclusion

In 6TiSCH-MC, a single slot known as the shared cell is designated at the beginning of each slot frame for various control traffic exchanges. This includes enhanced beacon, keep alive, RPL control packets, Join Request, and Join Response frames. However, under the decreased rank attack (DRA), the nodes are compelled to transmit a higher number of these frames at both the RPL and TSCH layers. As a consequence, this increased transmission results in congestion within the shared cell. As nodes compete for access to the shared cell simultaneously, it leads to contention and delays. Our findings indicate that the DRA can significantly disrupt network formation and ongoing operations. This disruption can result in more frequent node departures due to desynchronization, as nodes try to maintain the network topology. Furthermore, the DRA negatively impacts network reliability and increases latency. The increased transmission of keep-alive and RPL messages consumes more energy, further exacerbating the issue of increased energy consumption.

VI. Acknowledgement

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) through the Discovery Grant program.

References

1 Vilajosana, X., Watteyne, T., Chang, T., Vučinić, M., Duquennoy, S., and Thubert, P., "Ietf 6tisch: A tutorial," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 595–615, 2020.

2 Hauweele, D., Koutsiamanis, R. A., Quoitin, B., and Papadopoulos, G. Z., "Thorough performance evaluation & analysis of the 6tisch minimal scheduling function (msf)," *Journal of Signal Processing Systems*, vol. 94, pp. 3–25, 1 2022.

3 Winter, T., Thubert, P., Corporation, A. R., and Kelsey, R., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *RFC 6550*, pp. 1–157, 2012.

4 Vilajosana, X., Pister, K., and Watteyne, T., "Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration," *IETF RFC 8180*, 2017.

5 Carignani, G., Righetti, F., Vallati, C., Tiloca, M., and Anastasi, G., "Evaluation of feasibility and impact of attacks against the 6top protocol in 6tisch networks," in *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 2020, pp. 68–77.

6 Ghaleb, M. and Azzedin, F., "Trust-aware fog-based iot environments: Artificial reasoning approach," *Applied Sciences*, vol. 13, no. 6, 2023.

7 Boufenneche, Y., Zitouni, R., George, L., and Gharbi, N., "Network formation in 6tisch industrial internet of things under misbehaved nodes," in *2020 7th International Conference on Internet of Things: Systems, Management, and Security (IOTSMS)*, 2020, pp. 1–6.

8 Kalita, A., Brighente, A., Khatua, M., and Conti, M., "Effect of dis attack on 6tisch network formation," *IEEE Communications Letters*, vol. 26, no. 5, pp. 1190–1193, 2022.

9 Aljufair, G., Mahyoub, M., and Almazyad, A. S., "On mitigating dis attacks in iot networks," in *2023 18th Wireless On-Demand Network Systems and Services Conference (WONS)*, 2023, pp. 104–109.

10 Raoof, A., Matrawy, A., and Lung, C.-H., "Routing attacks and mitigation methods for rpl-based internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1582–1606, 2019.

11 Bang, A. O., Rao, U. P., Kaliyar, P., and Conti, M., "Assessment of routing attacks and mitigation techniques with rpl control messages: A survey," *ACM Comput. Surv.*, vol. 55, no. 2, jan 2022. [Online]. Available: https://doi.org/10.1145/3494524

12 Bang, A. and Pratap, U., "Impact analysis of rank attack on rpl-based 6lowpan networks in internet of things and aftermaths," *Arabian Journal for Science and Engineering*, 2022.

13 Raoof, A., Matrawy, A., and Lung, C.-H., "Enhancing routing security in iot: Performance evaluation of rpl's secure mode under attacks," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 536–11 546, 2020.

14 Thubert, P., "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)," *Request for Comments: 6552*, 2012.

15 Osterlind, F., Dunkels, A., Eriksson, J., Finne, N., and Voigt, T., "Cross-level sensor network simulation with cooja," in *Proceedings. 2006 31st IEEE Conference on Local Computer Networks*, 2006, pp. 641–648.

16 Vallati, C., Brienza, S., Anastasi, G., and Das, S. K., "Improving network formation in 6tisch networks," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 98–110, 2019.

17 Kalita, A. and Khatua, M., "6tisch – ipv6 enabled open stack iot network formation: A review," *ACM Trans. Internet Things*, vol. 3, no. 3, jul 2022.

18 Perera, C., Liu, C. H., Jayawardena, S., and Chen, M., "A survey on internet of things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, 2014.