The performance of the routing protocol for low-power and lossy networks in mobile networks

Fimme Neeleman[1] , **Mauro Conti**[1] , **Chhagan Lal**[1]
[1]TU Delft

***Abstract*—The IPv6 routing protocol for low-power and lossy networks (RPL) is a routing protocol that is standardized for constrained devices. This standard only considers static nodes and consequently underperforms in networks with moving nodes. Several studies exist intending to mend this problem, but analyses of RPL's performance in mobile situations are too scarce. These studies are needed to help researchers find related future work directions and improve RPL's support for moving nodes. This paper, therefore, analyzes the performance of RPL in dynamic networks and compares this to its performance in static networks by considering several routing and security metrics. It focuses on the impact of mobility when a node joins, leave, or moves within the network. The analysis concludes by discussing the effects of dynamic nodes on larger scale networks, DODAG's with multiple roots and networks with mobile roots. Afterward, DIS flooding is considered as an example of how attacks and their mitigations can be impacted by mobility, showing that more work is needed to secure RPL in these situations. This paper is constructed with a literature review and includes no experiments as the analyses in this research are broader than a few testable configurations.**

1 Introduction

The Internet of Things (IoT) refers to the interconnection of a set of smart objects that will upgrade our daily lives at home and work. All these devices are connected to each other and the internet to give the best service by working together. These devices might not handle connections like a personal computer can since the devices used in IoT are usually small, constrained, and with a more specific purpose than a personal computer. Some of the constraints that often limit these devices being running on batteries, having less power, having little storage capabilities, and the networks used to interconnect these devices usually use lossy links. Therefore, to work on constrained devices and in lossy networks, more efficient protocols are needed in IoT networks. One such protocol is the IPv6 routing protocol for low-power and lossy networks (RPL) which is a routing protocol that is standardized for use in IoT. RPL is designed to be energy efficient, with optional security, multiple modes of communication, and applicability in multiple network scenarios.

In recent years IoT devices have been embedded in many mobile objects: humans, bicycles, vehicles, ships, and airplanes [1]. Since RPL is a widely used routing protocol for IoT, it must also work in mobile networks. Its standard does not consider mobile nodes in networks but relies on a self-healing network topology [2] [3]. In mobile networks, nodes will frequently connect to, disconnect from and move around inside the network. Each time this happens, RPL will rebuild part(s) of its network topology. Rebuilding the network topology is troublesome as it introduces data loss, disruption of connections, higher overhead and increases energy consumption of nodes [1] [2] [4]. Therefore, research on the difference in the performance of RPL in static and mobile networks is needed. Parameters might indicate what causes the difference in performance. With this cause known, it can be easier to find an update or extension to RPL that improves its performance in mobile networks.

Multiple publications propose an amelioration on RPL or analyze its performance. In the work proposing EMA-RPL [2] the authors start with a small analysis of RPL's mobility support and then propose a protocol to support mobility based on this. EMA-RPL uses a Received Signal Strength Indicator, which can be unreliable in indoor environments. A performance analysis of RPL is proposed in the work of Lamaazi *et al.* [5]. This analysis is extensive as it tests RPL's performance in networks with an incrementing number of nodes, roots, and mobile nodes. The work shows concrete data and links this to their results, but a more general analysis without this specific data is missing.

There have been several studies on mobility support in RPL, but more effort is still needed [1] [5]. According to IoT's mobile developments, there is a high demand for efforts to come to a standard RPL supporting mobile nodes [1]. To achieve this standard, more research is required into mobility supporting extensions of RPL [6]. Furthermore, more research is essential in routing metrics and new mobile supporting Objective Functions that RPL uses [1] [2] [7] [8]. To improve RPL, for mobility support, more performance analyses of RPL in different static and mobile scenarios is necessary, as these analyses set the groundwork for improving RPL [1] [5]. Finally, there is little research on attacks on RPL in mobile networks, which is needed as some mitigations are proposed that do not work in mobile situations.

In this paper, RPL's behavior (concerning specific performance parameters) in mobile networks and static networks

are compared. To achieve this, specific performance parameters are chosen based on their impact on routing. With the specific routing and security metrics in mind, RPL's behavior in static and mobile networks is interpreted and compared. RPL's performance in mobile networks will be divided into three situations: a node joins, leaves, and moves within the network. For the analysis of all the situations, a network with a single root and nodes randomly moving around is kept in mind. Finally, an attack on RPL and its possible mitigations which are impacted by mobility are analyzed.

How is RPL's performance impacted (concerning routing and security metrics) by mobile nodes in networks?

The remainder of this paper is as follows. Section 2 provides an overview of RPL and several articles related to this paper. How the research for this paper will be conducted and all relevant data are described in Section 3. In Section 4, RPL's performance in mobile networks is compared to static networks. Following section 4, an attack on RPL is analyzed, which is impacted by mobility in Section 5. This research is conducted responsibly, which is clarified in Section 6. Finally, the paper concludes with a discussion of the results in Section 7 and a conclusion of the research in Section 8.

2 Background and related works

2.1 RPL overview

As mentioned in the introduction, RPL is an IPv6 routing protocol for low-power and lossy networks. RPL was proposed by the IETF ROLL working group. Before proposing RPL, ROLL described the routing requirements of LLN's that it had to fulfill. The standardization of RPL can be found in RFC 6550 [9].

There can be multiple instances of RPL running in the same network that have unique IDs. Each RPL instance defines its metrics and routing policies using an Objective Function (OF). An OF is defined separately from RPL and determines what metrics are used in calculations such as rank. Each node calculates its rank using the OF to represent the routing distance from that node to the root. The root always has the lowest rank possible. RPL uses Destination Oriented Directed Acyclic Graphs (DODAG) as routing topology. Which is a Directed Acyclic Graph (DAG) with at least one root such that all routes starting in some leaf end at the root. A simple example of such a routing topology can be found in figure 1. Each RPL instance can have multiple DODAG's. If inconsistencies arise, for instance when a new node joins or leaves the network, the network topology is repaired, meaning it is partly or fully reconstructed. A DODAG has a version number that increments each topology repair.

RPL uses several ICMPv6 control messages to construct and maintain the DODAG and optimal routing solutions. Examples of the control messages used by RPL can also be seen in Fig. 1.

- **DODAG Information Object (DIO)**: DIO are broadcasted or unicasted as in Fig. 1, to spread essential routing information. To reduce DIO message overhead, DIO messages are transmitted based on the TrickleTimer [10]. This timer dictates how many messages can be sent, which decreases over time. When an inconsistency arises, the TrickleTimer is reset to stabilize the network.

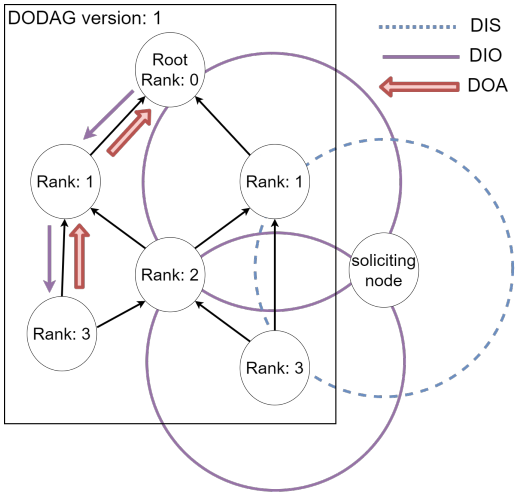

Figure 1: An example of a simple DODAG

- **Destination Information Solicitation (DIS)**: DIS are used by new nodes to probe for and join a DODAG. In Fig. 1 can be seen how a node can use a DIS broadcast to get DIO messages in response.
- **Destination Advertisement Object (DAO)**: DAO contain routing information for maintaining and creating downward routing paths. RPL has 2 Modes of operations for downwards routing:
  1. **Storing mode**: Nodes maintain downward routing information for all their children.
  2. **Non-storing mode**: Only the root has downward routing information. Therefore all messages traveling downwards first need to travel through the root node.
- **Destination Advertisement Object Acknowledgement (DAO-ACK)**: DAO-ACK messages are sent in response to a unicast DAO.

2.2 Related works

An extension of RPL that improves performance in mobile networks is the Mobility Enhanced RPL (MERPL) proposed by Korbi *et al.* [11]. MERPL differentiates static and mobile nodes to improve performance in mobile networks. RPL decreases control traffic, which causes lower reactivity to topology changes, but this is reconciled by MERPL. Gaddour *et al.* [12] take a different approach to improve RPL. Firstly they proposed a new OF, named OF-FL (Objective Function based on Fuzzy Logic), which considers the link quality, number of hops, end-to-end delay, and ETX. They additionally proposed an extension on RPL named Co-RPL to support mobility by overcoming RPL's slow reaction to frequent network topology changes. According to the authors both OF-FL and Co-RPL improve performance concerning the packet loss ratio and average network latency. The work proposing EKF-MRPL [13] uses Received Signal Strength Indicator to

create a hand-off system between mobile nodes and their parents. The best parent for a mobile node is chosen by predicting its movements. EKF-MRPL is tested using Cooja, which shows that the proposal has better energy consumption and PDR than RPL.

In the paper of Lamaazi *et al.* [5] the authors analyze RPL's performance in static and mobile environments. They analyze in terms of control traffic overhead, EXT, hop count, packet delivery ratio, and node energy. For mobility performance, they use group and entity mobility models to characterize the movements of the mobile nodes. In their results, the authors note that RPL's performance degrades with an incrementing number of nodes and betters with more sink nodes. They also note that the entity model has better control traffic overhead and energy consumption, but the group model has a higher PDR.

3 Methodology

The research questions posed for this paper will be answered with findings from literature research. This paper discusses the performance of RPL in networks with mobile nodes compared to networks with static nodes by describing its behavior in different network configurations and analyzing the routing and security metrics. This will be done descriptively, so there will be no explicit data as a result of an experiment. Such an experiment is not necessary to analyze RPL's behavior in mobile networks as this paper will approach this in a general manner. This approach is based on RPL's behavior and not on a specific network configuration that can be tested.

The analysis will start by describing RPL's behavior when a mobile node joins, leaves, or moves around within a DODAG. The analysis will start with this because it will give the appropriate background for examining the routing and security metrics and the extended network configurations. Afterward, an extension will be made where several other network configurations (like a DODAG with multiple roots) will be discussed in the same manner to make the analysis more complete. Security metrics are discussed in the performance analysis as the security of RPL is closely related to its performance. If RPL is performing poorly, an attack is more easily established. As there is little research on RPL's security in mobile networks, it is imperative to look at the impact of mobile nodes on its performance in the security domain.

After the performance analysis, an attack on RPL and its mitigations will be analyzed, which are impacted by mobile nodes. This analysis starts with an explanation of the attack. Then the impact of mobility on this attack will be discussed. The analysis is concluded by discussing several mitigations and the impact of mobility on these. This analysis is also based on literature and will not be proven with any experiments. This analysis is a proposal for future research, as it is not the focus of this paper.

3.1 Overview performance metrics

Routing metrics

The performance analysis and comparison of RPL in static and mobile networks will be performed, considering several metrics chosen by their impact on the routing process.

- **Energy consumption**: Is the amount of energy consumed by a node. The energy consumption is an indication for a node's lifetime and is directly related to the number of messages transmitted to and received by the node, the processing time, and overhearing at idle state [2].
- **Packet delivery ratio (PDR)**: Represents the number of packets successfully delivered at the destination compared to the number of packets transmitted from the sender. A higher PDR presents a better RPL performance [5].
- **Expected transmission count (ETX)**: Exemplifies the maximum amount of re-transmission needed for a packet to successfully reach its destination [7] [8] [14]. It is an indication of RPL's performance. If RPL or link quality is under-performing, the ETX will grow as fewer packets successfully arrive more need to be retransmitted [7].
- **End-to-end delay**: Describes the time taken by a packet to travel from its source to its destination. End-to-end delay is an important metric to consider in delay-sensitive scenarios [15]. The end-to-end delay is also a good indication of the health of the network and links used. If the end-to-end delay is high, RPL is failing, or the used links have bad performance.
- **Control traffic overhead**: Expresses the amount of RPL control messages sent by nodes (DIO, DAO, and DIS messages). The amount of control messages sent is directly related to the energy consumption in a network, making it crucial to optimize the control process [2].

Security metrics

Next to routing metrics, several security metrics will be discussed in the performance analysis. These metrics are chosen by their impact on the security of RPL in mobile networks.

- **Authentication**: The verification that the sender of the packet received is the node that it claims to be [16] [17] [18] [19]. Failure to authenticate can cause spoofing of routing messages by adversaries to change the routing operations in the network to their advantage.
- **Access control**: Granting resource access to authorized nodes, preventing unauthorized nodes from accessing resources, and preventing unauthorized uses of resources [16] [18] [19]. Without Access control unauthorized nodes can access network critical information.
- **Availability**: Being accessible and operational upon demand of an authorized node, conforming the systems performance specifications [16] [17] [18] [19]. This entails maintaining correct and efficient routing, which can be threatened by interference or by disruption [19] [20].
- **Data integrity**: Data is not altered, destroyed or lost in a manner that is unauthorized or accidental [16] [17] [18] [19]. Making sure that when data is sent it is in the same state as when it is received independent of whether the data is authentic [17]. When data is not integral, adversaries can spread inconsistent information that can

cause network suboptimality and fragmentation of the network [20].

- **Confidentiality**: Data is not disclosed to unauthorized nodes [16] [17] [18] [19]. This includes data like routing information, neighbor maintenance and information stored within the node [19] [20]. Losing confidentiality can impact the performance of the network or can cause loss of privacy for the transmitters [20].

4 RPL performance in mobile scenarios

In this section, the performance of RPL in mobile networks compared to static networks will be analyzed. If not noted otherwise, a network with a single root and random node movements will be assumed. Firstly RPL's behavior will be explained when a mobile node joins, leaves, or moves around within a DODAG. Secondly, the overall picture of RPL's behavior with mobile nodes is depicted, followed by the analysis of its performance through routing and security metrics. Finally, its behavior is analyzed in other scenarios than for a network with a single root and random node movements.

4.1 Nodes joining a DODAG

When a node wants to joins a DODAG, the node broadcasts a DIS to all its neighbors. Any neighbors that receive this DIS will respond with a DIO message to supply the soliciting node with sufficient information to join the DODAG. But when a node is physically moving, it might not be able to receive the DIO response, and it will have to rebroadcast the DIS message. Therefore joining a DODAG is more challenging for a mobile node on top of that, more control messages are needed [5].

When mobile nodes have to rebroadcast DIS messages, they have to stay active, as the nodes broadcast DIS messages and listen for DIO responses. Therefore more energy is consumed by mobile nodes when joining a DODAG. Fig. 2 shows a mobile node joining a simple DODAG but missing the DIO response because the mobile node moved out of its range.

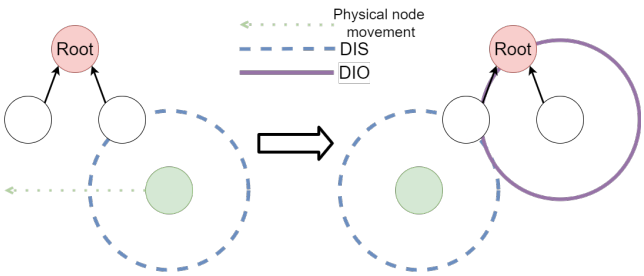

Figure 2: An example of a mobile node joining a DODAG

4.2 Nodes leaving a DODAG

When a node leaves a DODAG, it takes about a long trickle timer interval for its neighbors to notice this [2]. The parents and children of the node that left need to find new routing paths as their data cannot be forwarded through the disconnected node. Nodes in a DODAG broadcast DIO messages to its children according to the TrickleTimer to keep its children updated. The children send DAO messages in response. When a node receives no more DAO or DIO messages, it assumes that the node from which it should receive these messages has left its range and removes this node from its routing table, list of neighbors, and list of parents [2].

The parents and children of the disconnected node do exactly this they remove the node from its routing table, list of neighbors, and list of parents [2]. Luckily RPL allows nodes to chose multiple parents to decrease the risk of failure as part of its self-healing strategy [21]. Choosing multiple parents might resolve the issue by providing the nodes with another usable routing path, but if the nodes still need a new route, they will wait for control messages from other nodes to update their information and ensure connectivity [2]. Fig. 3 shows an example of a mobile node leaving a simple DODAG.

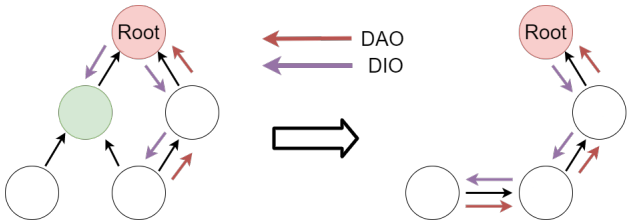

Figure 3: An example of a mobile node leaving a DODAG

4.3 Nodes moving within a DODAG

One of the causes for inconsistency in RPL is when a node physically moves a distance that results in a change of topology [2]. This can happen in RPL because it allows for routing paths with mobile nodes, which frequently disconnect, disrupting the routing path [2]. When this inconsistency happens for a node, it becomes isolated from its parent and children and loses its ability to send data [2]. This node needs to reconnect to the DODAG to be able to regain its abilities. RPL tries to resolve this issue with local or global repairs. The local repair entails that the parent and children nodes will look for new routing paths to avoid data loss and for the inconsistent node to receive a DIO message to reconnect. If this local repair fails to resolve the issue, a global repair is issued, which increments the DODAG version allowing nodes to join the new version and reestablish paths and rank.

The mobile node that caused the inconsistency rejoins the DODAG in one of two ways. The mobile node receives a DIO message send according to the TrickleTimer, giving the node the ability to update its necessary information. Oppositely, it broadcasts a DIS message to its neighbors. When the mobile node receives a DIO message it:

- Firstly uses the information from the DIO message to update its neighbor list, parent list, preferred parent list, rank, and routing table. Then using the information, the node selects one or more parents to create an upwards routing path [2].
- Secondly, it sends a DAO message to its parents to create a downwards routing path [2].

- Finally, it broadcasts DIO messages with its updated information according to the TrickleTimer, potentially to enlist new children [2].

The parents and children of the inconsistent node will find a new routing path by acting as if the moved node has disconnected, which the previous subsection named 'Nodes moving within a DODAG' describes. Fig. 4 shows an example of a mobile node moving within a simple DODAG, giving both the outcomes where the node receives a DIO message in the upper outcome graph and where the node does not receive a DIO message, so it broadcasts a DIS message in the lower outcome graph.

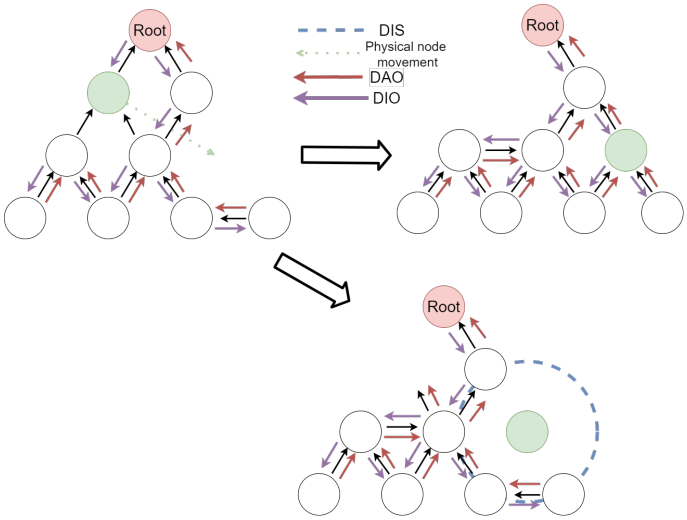

Figure 4: An example of a mobile node moving within a DODAG

4.4 Performance analysis

When nodes are static, topology repairs only occur when a node fails or disconnects. When nodes are mobile, they also occur when nodes physically move out of the range of their parents. Observing that dynamic nodes instigate more repairs already displays that the performance of RPL will be worse when they are in the network. How often these repairs occur, and so its impact on RPL's performance depends on the manner and frequency of the node's moves. When nodes in the network move frequently and far, considering the transmission range of nodes, the impact will be the most prominent.

Aside from the repairs, mobile nodes often lose data when sending or receiving because nodes are far apart. Nodes can be far apart because RPL has no system to immediately switch to a more suitable node when the connection with its current parent set is degrading. In RPL, a node has to move out of the transmission range of the current parents to reconnect to the DODAG and find a new parent with a stable connection for the node's current position. If mobile nodes are constantly moving, this data loss happens frequently.

Signal quality is defined by its power, noise, and interference at the receiver input [22]. Data loss happens more often when communicating nodes are far apart because the signal quality changes over time. Data signals are transmitted with a predefined power, which several physical phenomena degrade [22]. These power degrading phenomena are constantly occurring, causing the signal to degrade more the further it has to travel. Others physical phenomena strengthen the noise power, which increases signal interference [22]. This interference means the sent signal is harder to read.

Routing metrics

- **Energy consumption** The reasons for higher energy consumption in dynamic networks can be found in Table 1. For these reasons, mobile nodes experience more failures as their resources are quickly diminished [2]. Table 1 mentions unawareness of node movements, which can happen because nodes need to wait for a DIO message sent following a TrickleTimer to detect movements [10] [13]. While waiting, all nodes keep sending data while they could be out of transmission range of each other [23].
- **PDR** As indicated in Table 1, topology repairs decrease PDR, and these occur more often in mobile networks [8] [13] [23]. In such repairs, new routing paths will need to be established for data to flow again and be successfully delivered. The PDR also lowers when a connection degrades because a node travels away from its parents.
- **ETX** Table 1 notes that mobile nodes lose more data. This loss is due to numerous disconnections that the network is unaware of and deteriorating connections caused by node movements.
- **End-to-end delay** As Table 1 mentions, the end-to-end delay is closely connected with the PDR and ETX as more messages sent for a successful reception means more time spent.
- **Control traffic overhead** The reasons for TrickleTimer resets, which rapidly increase the exchange of control messages [8] [23], are named in Table 1. This rapid increase also degrades all other routing metrics as the network is flooded. In inconsistent networks, these resets frequently occur, keeping the network unstable as RPL needs a while of stability for establishing routing paths [8] [24].

Security metrics

- **Authentication** The secure modes of RPL only allow nodes to join with a preinstalled key [9]. In Authenticated mode, the node needs another key from an authority to connect as a router [9]. Key exchanges are impacted by mobility, as described in Table 1. The longer end-to-end delays and instability of dynamic networks are the reason for this impact. Table 1 also notes that sessions are more often interrupted, caused by the disruption of routing paths. These interruptions require nodes to reconnect and make a new session, again needing to exchange keys.
- **Access control** The only form of access control in an RPL network is in its secure modes, where a key is needed to join. But as mentioned in Table 1, the internal access control of a dynamic node might fail due to its higher energy consumption. The failure of a node's

internal access control might allow adversaries to access sensitive data, which can hurt the network and the node's owner.

- **Availability** The availability of a network is the most heavily impacted security metric. As Table 1 indicates, mobile nodes deteriorate a network's availability. This deterioration makes networks more vulnerable to attacks on availability, and their mitigations might not work in dynamic networks, of which an example is given in Section 5. Additionally, Intrusion Detection Systems (IDS) might not work as they strain the network, which can overload it in mobile cases.
- **Data integrity** As mentioned in Table 1, session keys are needed for creating signatures, which RPL can use to verify data integrity [9]. Table 1 also describes that signature schemes might be too costly for a mobile node because they are already drained of resources, incrementing error chances. When a node's integrity fails, an attacker can take advantage by altering messages, which allows for several attacks on the network.
- **Confidentiality** Session keys are also used to encrypt messages, which can be used in RPL [9]. Furthermore, Table 1 declares that encrypting data might be too heavy for mobile nodes to calculate. It drains energy that mobile nodes are already lacking, increasing error chances which can incur a loss of confidentiality.

4.5 Extended scenarios

Larger scale networks

The performance of RPL degrades as more nodes join the network making it denser. There are multiple causes for this degradation:

- One of the causes is that there is more interference between the transmitted packets [2]. The interference causes nodes to increase the number of packets sent to enlarge the packet's chances of successfully being received. With increased interference between packets, nodes can also choose to send their data down multiple paths, using several or all of its parents. If more nodes do this, it can cause congestion at the parent nodes. The congested parents will respond by dropping these packets, which further increases the problem [2].
- In a denser network, nodes multicast more DAO and DIO messages to create routing paths and spread the routing information [2]. The increase in multicast DAO and DIO messages sent increases the control traffic overhead, which impacts network stability [2].
- Lastly, the dense network increases the transmission delays [2]. This delay causes increased congestion and packet interference in the network. This also increases the control messages send by nodes to check the availability of neighboring nodes. Which again increases overhead but also drains resources.

The scale of degradation depends on how many nodes in the network are mobile, as they also degrade RPL performance on top of the denser network. When many nodes in a dense network are mobile, the network is highly probable to fail as the combination intensifies each other. As mentioned in the analysis, mobile nodes increase the control traffic overhead and congestion in the network, which is also the main impact of a denser network.

Performance metrics	
Routing metrics	
Energy consumption	Mobile nodes signal more frequently. Unawareness of node movements can cause loss of packets which need to be resent.
PDR	New routing paths need to be established after a topology repair causing packet loss. Mobile nodes lose data by degrading connections with their parents.
ETX	Mobile nodes lose more data, so these packets have to be re-transmitted before a successful delivery
End-to-end delay	With a lower PDR and ETX, it takes longer for a message to successfully reach its destination [13] [23].
Control traffic overhead	A global repair caused by mobility resets all TrickleTimers. A DIS message broadcasted by a disconnected node resets the TrickleTimers of its receivers.
Security metrics	
Authentication	The key exchanges for router privileges and message authentication are protracted. Key sessions are more often interrupted.
Access control	Mobile nodes are more prone to errors and failures, indicating that its internal access control might fail
Availability	Nodes in the network are harder to reach as mobility increases delays, congestion and failure rates. Attacks on availability are enhanced
Data integrity	Session keys for signatures have the same issues as with authentication keys. The signature scheme might be too costly for a mobile node to calculate for each message.
Confidentiality	Session keys for encryption experience similar problems as authentication keys. Encrypting messages can be too heavy for dynamic nodes.

Table 1: An overview of the impacts of mobility on RPL's performance metrics

Multiple roots

The performance of RPL is positively impacted by the incremental presence of roots in the network. The length of routing paths decreases considerably with more roots in the network. The paths' length decrease even more if the roots are evenly distributed over the network [2]. This can be explained by

nodes' behavior to send their data to the nearest root. When the roots are evenly distributed throughout the network, each root will roughly handle the same amount of nodes. This decreases congestion, interference, and packet loss. Which, in turn, will positively impact all previously discussed routing metrics.

With more roots in the network, nodes will have more freedom to choose shorter and less congested paths. Roots do not consume much energy as they only receive and handle data from nodes and do not send control messages to check availability or find neighbors. Roots also broadcast less frequently when the network is more stable, and fewer nodes join the network [2]. Therefore, an increment in roots does not increase energy consumption.

The presence of more roots is beneficial for mobile nodes for two reasons:

1. Firstly, because the network is incrementally more stable with increasing roots. Meaning that the congestion, overhead, and delays caused by mobile nodes have less impact on the network.
2. Secondly, because the impact of topology repairs caused by the movement of nodes is abated. This is because nodes now have more choices in routing paths. Children of the mobile node that caused the topology repair normally would be cut off from the root, but with more roots, they have more choice. Therefore, the node might find a better path to another root instead of the path to the old root it was sending data towards. Furthermore, a node can also send a message to multiple roots. This increases the probability that the message sent is still received by a root, despite the node losing its parent.

Mobile roots

When a DODAG contains a single root, all the upwards routing paths are oriented towards that root. When the root would move out of the transmission range of its children, all upwards paths would be interrupted, and if RPL is running in non-storing mode, the downwards paths would also be disrupted. This means that momentarily no data can reach the root, causing packet drops at the children of the root. When the root sends out a DIO message according to the TrickleTimer, the nodes receiving the DIO will update their routing information and send out DIO messages themselves, propagating the new routing information throughout the network. A mobile root is catastrophic for RPL's performance if the root is frequently moving with distances that are large compared to the nodes' transmission ranges.

Incrementing the number of roots in the network is beneficial for RPL's performance. A network with two mobile nodes outperforms a network with one mobile node for the same reasons mentioned for static roots in the Multiple roots section.

5 DIS flooding in mobile networks

A flooding attack is an attack where the network is inundated with messages to deteriorate its availability. It increases control traffic overhead and subsequently increases energy consumption and delays in the network. DIS flooding is a kind of flooding attack that periodically sends DIS control messages to draw out DIO responses of non attacker nodes. There are two possible DIS flooding attacks, namely multicast and unicast [25]. Flooding by multicast DIS messages is the most impactful version as a DIS message requests a multicast DIO as a response and resets the TrickleTimer for all receivers of the DIS. The frequent resets of TrickleTimers will cause an unstable local network as control message overhead is increased [25]. Two examples of a broadcast DIS flooding attack are given in Fig. 5. Unicast DIS flooding is less effective as a unicast DIS requests a unicast DIO response and does not reset TrickleTimers. For initiating a DIS flooding attack, control of one or several nodes in the range of the network is needed. These nodes need to be able to send DIS messages in an attacker-defined interval to neighboring nodes.

The impact of mobile nodes in an RPL network is similar to attacks on availability like DIS flooding. Both cause congestion, delays, and an increase in energy consumption, which decrease the availability of the network and lead to more node failures. The increased failure rate is caused by having to react to every DIS message inundating the network on top of mobile impacts, which drain energy.

When a DIS flooding attack would (partially) be executed from a mobile node, the attacker needs to verify that the node is capable of sending DIS messages at an interval defined by the attacker. Such an attacking mobile node would have a lower energy consumption than a non-attacker mobile node as the attacker never has to join the network. When an attack is performed from a moving node, the DIS broadcasts can have changing recipients, as depicted in Fig. 5. Meaning that the control overhead and energy consumption are distributed over the path of the mobile node, thus decreasing the impact on some nodes (the leaf nodes in Fig. 5). The impact of a DIS flooding attack, when executed from a mobile node, depends on its path. Fig. 5 shows a mobile node that moves to a position where it affects more nodes than from its previous location. A DIS flooding attack has more impact with more attacker nodes depending on their distribution. They will be most impactful when the attacker nodes are evenly distributed over the network. Using a mobile node as an attacking node might improve this distribution.

Secure-RPL is a security mechanism proposed by Verma A. and Ranga V. [25] which aims to address DIS flooding attacks on RPL. The mechanism does this by using RPL parameters to set two thresholds for receiving DIS messages, namely γ and μ. γ is the safe DIS transmission interval, and μ is the allowed maximum number of DIS messages send by a certain node [25]. It also uses a blacklist and an array for storing node information like the amount of DIS messages sent by a node. γ is for detecting DIS flooding attacks with a small sending interval and μ for large intervals. Each time a DIS message is received by a node, Secure-RPL will check if the node is on a blacklist, if so it discards the DIS. If the node is not in the list, it will check if thresholds γ and μ are exceeded, if so it discards the DIS. If the thresholds are not exceeded, the DIS message is handled as normal.

Secure-RPL has more overhead when a node joins the network, which might be problematic in dynamic scenarios with frequent topology repairs. It adds the constrain to the nodes

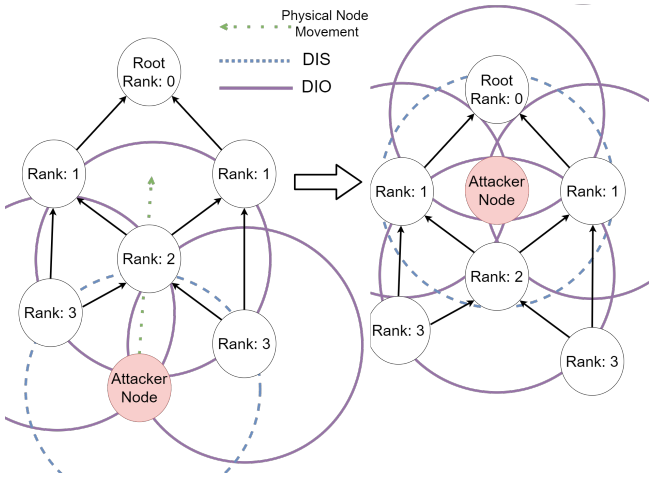

Figure 5: An example of mobile DIS flooding attack

receiving the DIS, which checks the blacklist and thresholds. These checks also add a delay to the reconnection of mobile nodes depending on the implementation of the DIS processing algorithm of Secure-RPL. Defining μ is also a challenge as a small μ detects slow DIS flooding attacks, but nodes might be isolated due to sending too many DIS messages. A high μ will not detect slow DIS flooding attacks. The authors of Secure-RPL showed that their implementation imposes little overhead on resource-constrained nodes by simulating with Cooja [25]. This might not be enough for dynamic nodes as they are more constrained than static nodes. Secure-RPL can therefore work in moderately mobile networks, but another solution would be needed for highly mobile networks.

A protocol aimed to mitigate flooding attacks, in general, is μTESLA which is part of the SPINS protocol set proposed by Perrig *et al.* [26]. The protocol tries to mitigate flooding attacks with authenticated broadcasts by using symmetric key cryptography [27]. μTESLA was an improvement of TESLA, intending to work in constrained sensory networks. μTESLA should therefore work in static RPL networks. It requires nodes to generate keys and authenticate packets, which can be too straining for mobile nodes. Moreover, the protocol uses a base station to relieve limited nodes of strain. Nodes, therefore, need a steady connection with the base station, which cannot be guaranteed in dynamic scenarios. μTESLA is, therefore, not a great candidate for mitigating flooding attacks in mobile networks.

6 Responsible Research

The reproducibility of research is a critical aspect as researchers (the authors and others) should have the ability to verify its results. Therefore, a descriptive methodology should be present that allows for reproducing the research. This reproduction should justify the conclusions of the authors and indicate whether or not their results are trustworthy.

This paper is literature research that is arguably easy to reproduce as the steps to attain the results are implicit. Furthermore, all the resources used to obtain the results are the references used in the paper and a further reading list provided at github.com/FNTuDelft/Reading-list-excluding-references. Therefore, a researcher wanting to verify this paper could read the literature in the reference and reading list and scrutinize the paper's explanation and argumentation.

The literature used for this paper was found with the IEEE Xplore Digital Library, Scopus, and DBLP databases. Therefore, literature that can be found in databases excluding the mentioned three is not used for this paper, which can induce an unintentional, unwanted bias. Furthermore, Mostly peer-reviewed literature and requests for comments were used for this research. The used works were picked based on their subject, being RPL in mobile situations. Even within this subsection of literature, only a few works were selected for use in this paper, meaning that any results other than the previously mentioned works are not included in this paper. With this subsection of used literature, the results have been constructed as unbiased and extensive as within the author's abilities.

Ethically speaking, this paper is more interesting as the weaknesses of RPL in mobile situations can be scrutinized by adversaries to create or enhance attacks on RPL networks. Furthermore, the information on the DIS flooding attack, Secure-RPL, and μTesla in mobile situations can be used to enhance attacks. Delivering knowledge to malicious users is by no means the purpose of this paper. This study is intended by the authors for researchers to strengthen the security and acknowledge the vulnerabilities of RPL and related works. Finally, this article is not funded. It is part of a Bachelor thesis project meant to show the capabilities of its authors within eight pages.

7 Discussion and Future Work

This paper contains literature research that analyzes RPL's performance in mobile situations. In contrary to the work of Lamaazi *et al.* [5], no simulations or experiments are used for this analysis. The analysis is based on RPL's behavior as described in its standard [9]. Such a study was missing for RPL in mobile networks, as other papers either shortly discuss RPL's performance to base amelioration's on or use simulations for their analysis. This article gives researchers the ability to easily obtain information and find research directions. Contrarily, this analysis is not specific as it is not tested in a physical RPL network, and no concrete metric data is given, which is needed for physical implementations.

Research on attacks on RPL in mobile situations is lacking. The authors of Secure-RPL [25] shortly discuss the mobility support of implementation. Most mitigations and preventions do not consider and support mobile networks. This study quickly discusses one attack and two of its mitigations because these are heavily impacted by mobility. Many more attacks and mitigations exist that have no mobility supporting solutions, making RPL insecure, especially in mobile networks.

Future research into other attacks and their mitigations in mobile situations is vital for RPL's security. Investigation into rank attacks and their mitigations in mobile networks might be interesting. Further performance analyses for RPL tested in a physical mobile network will be interesting, especially

when several ameliorations are analyzed. Finally, research into updating the standard by combining extensions and protocols will be interesting for both static and mobile situations.

8 Conclusions

In this study, RPL's performance in mobile networks is compared to its performance in static networks. RPL is not capable of treating mobile nodes efficiently. In many papers, RPL's deficiencies in mobile situations are discussed, but none of these have done this in an extensive and general manner as posed in this paper.

The analysis starts with the description of RPL's behavior when a mobile node joins, leaves, or moves within a DODAG. Afterward, the performance of the behavior is described by stating that the frequent topology repairs are the main cause for the deteriorated performance of RPL under mobility. The frequent topology repairs cause decreased PDR and increased ETX, end-to-end delays, energy consumption, and control traffic overhead in the network because of routing path interruptions and packet drops. Packet drops are also caused by RPL missing a hand-off system. A mobile node has to move out of the transmission range of its parents before it can connect to new parents in its range. As for the aforementioned reasons, the availability of the network is catastrophically impacted by mobile nodes. Subsequently, the analysis is extended by noting the following:

- Incrementing the scale of the network deteriorates RPL's performance, which is aggravated by higher ratios of mobile nodes.
- Having more roots in the network improves performance as it offers more routing path diversity.
- Mobile roots are catastrophic for RPL's performance, as all routing is aimed towards this root.

Finally, DIS flooding is discussed, and the impact of mobility on this attack and its mitigations. DIS flooding is enhanced by mobility in the network as both attacks its availability. Furthermore, mitigations are needed that can run in highly mobile networks.

References

[1] B. Safaei, A. Mohammadsalehi, K. T. Khoosani, S. Zarbaf, A. M. H. Monazzah, F. Samie, L. Bauer, J. Henkel, and A. Ejlali, "Impacts of mobility models on rpl-based mobile iot infrastructures: An evaluative comparison and survey," *IEEE Access*, vol. 8, pp. 167 779–167 829, 2020.

[2] M. Bouaziz, A. Rachedi, A. Belghith, M. Berbineau, and S. Al-Ahmadi, "Ema-rpl: Energy and mobility aware routing for the internet of mobile things," *Future Generation Computer Systems*, vol. 97, pp. 247–258, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18302541

[3] H.-S. Kim, J. Ko, D. E. Culler, and J. Paek, "Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2502–2525, 2017.

[4] R. K. Yadav and N. Awasthi, "A survey on enhanced rpl: Addressing the mobility in rpl," in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2020, pp. 1189–1195.

[5] H. Lamaazi, N. Benamar, and A. J. Jara, "Rpl-based networks in static and mobile environment: A performance assessment analysis," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 320–333, 2018.

[6] A. Oliveira and T. Vazão, "Low-power and lossy networks under mobility: A survey," *Computer Networks*, vol. 107, pp. 339–352, 2016, mobile Wireless Networks. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128616300895

[7] X. Liu, Z. Sheng, C. Yin, F. Ali, and D. Roggen, "Performance analysis of routing protocol for low power and lossy networks (rpl) in large scale networks," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2172–2185, 2017.

[8] S. Murali and A. Jamalipour, "Mobility-aware energy-efficient parent selection algorithm for low power and lossy networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2593–2601, 2019.

[9] R. Alexander, A. Brandt, J. Vasseur, J. Huii, K. Pister, P. Thubert, P. Levis, R. Struik, R. Kelsey, and T. Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, Mar. 2012. [Online]. Available: https://rfc-editor.org/rfc/rfc6550.txt

[10] P. Levis, T. H. Clausen, O. Gnawali, J. Huii, and J. Ko, "The Trickle Algorithm," RFC 6206, Mar. 2011. [Online]. Available: https://rfc-editor.org/rfc/rfc6206.txt

[11] I. E. Korbi, M. Ben Brahim, C. Adjih, and L. A. Saidane, "Mobility enhanced rpl for wireless sensor networks," in *2012 Third International Conference on The Network of the Future (NOF)*, 2012, pp. 1–8.

[12] O. Gaddour, A. Koubâa, and M. Abid, "Quality-of-service aware routing for static and mobile ipv6-based low-power and lossy sensor networks using rpl," *Ad Hoc Networks*, vol. 33, pp. 233–256, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870515000992

[13] M. Bouaziz, A. Rachedi, and A. Belghith, "Ekf-mrpl: Advanced mobility support routing protocol for internet of mobile things: Movement prediction approach," *Future Generation Computer Systems*, vol. 93, pp. 822–832, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17306805

[14] O. Gnawali and P. Levis, "The Minimum Rank with Hysteresis Objective Function," RFC 6719, Sep. 2012. [Online]. Available: https://rfc-editor.org/rfc/rfc6719.txt

[15] J. Tripathi, J. C. de Oliveira, and J. Vasseur, "Performance Evaluation of the Routing Protocol for

Low-Power and Lossy Networks (RPL)," RFC 6687, Oct. 2012. [Online]. Available: https://rfc-editor.org/rfc/rfc6687.txt

[16] "Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture," International Organization for Standardization, Geneva, CH, Standard, Feb. 1989.

[17] D. B. Parker, "Restating the foundation of information security," *Computer Audit Update*, vol. 1991, no. 10, pp. 2–15, 1991. [Online]. Available: https://www.sciencedirect.com/science/article/pii/096025939190013Y

[18] R. W. Shirey, "Internet Security Glossary, Version 2," RFC 4949, Aug. 2007. [Online]. Available: https://rfc-editor.org/rfc/rfc4949.txt

[19] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)," RFC 7416, Jan. 2015. [Online]. Available: https://rfc-editor.org/rfc/rfc7416.txt

[20] S. Mangelkar, S. N. Dhage, and A. V. Nimkar, "A comparative study on rpl attacks and security solutions," in *2017 International Conference on Intelligent Computing and Control (I2C2)*, 2017, pp. 1–6.

[21] O. Gaddour and A. Koubâa, "Rpl in a nutshell: A survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128612002423

[22] L. W. Couch, *Digital and Analog Communication Systems*. Harlow: Pearson, 2013.

[23] C. Cobarzan, J. Montavont, and T. Noìl, "Mt-rpl: a cross-layer approach for mobility support in rpl," *EAI Endorsed Transactions on Internet of Things*, vol. 2, no. 5, 12 2016.

[24] M. Vučinić, M. Król, B. Jonglez, T. Coladon, and B. Tourancheau, "Trickle-d: High fairness and low transmission load with dynamic redundancy," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1477–1488, 2017.

[25] A. Verma and V. Ranga, "Mitigation of dis flooding attacks in rpl-based 6lowpan networks," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, p. e3802, 2020, e3802 ett.3802. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3802

[26] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "Spins: Security protocols for sensor networks," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '01. New York, NY, USA: Association for Computing Machinery, 2001, p. 189–199. [Online]. Available: https://doi.org/10.1145/381677.381696

[27] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.