RPL's performance in mobile networks compared to static networks

Fimme Neeleman - Chhagan Lal - Mauro Conti

CSE3000 Research Project

2 July 2021

1. Research question

- How is RPL's performance impacted (concerning routing and security metrics) by mobile nodes in networks?
- How does mobility impact the DIS flooding attack and its mitigations?

2. Methodology

- Mobile nodes will be defined as one of the following:
  1. A node that **joins** a DODAG.
  2. A node that **leaves** a DODAG.
  3. A node that **moves within** a DODAG.
- This paper is constructed with a literature review and includes no experiments.

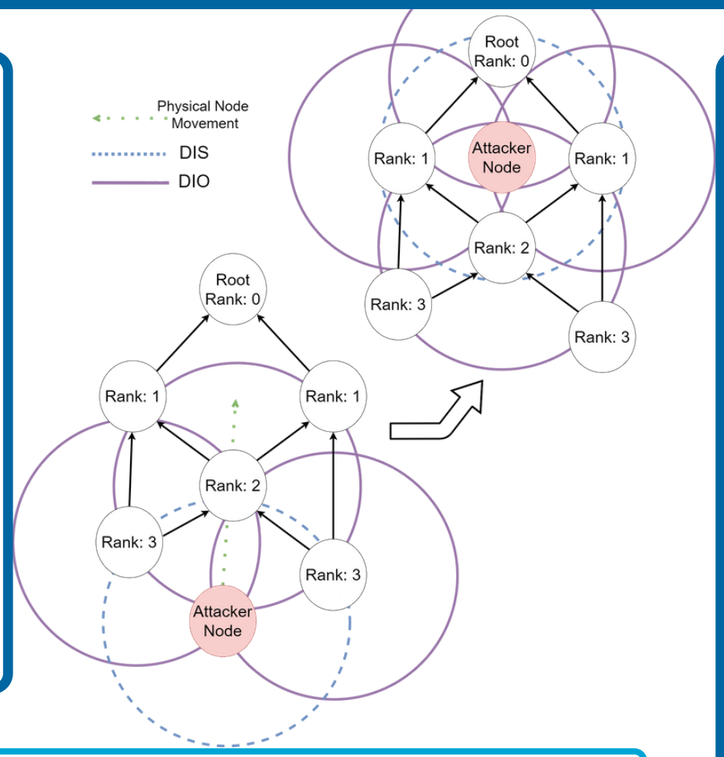
3. Background

- The devices used in IoT are usually constrained (limited processing power, memory, energy) and network links are often lossy.
- RPL is a IPv6 routing protocol that is standardized for LLN's in the IoT.
- RPL does not support mobility while this is in growing demand.
- RPL's security is insufficient especially in mobile situations.

4. RPL's performance

1. **No hand-off system.**
   - Degrading connections through movement.
2. **Frequent disconnects** causing topology repairs.

- **A denser network** deteriorates performance, which is aggravated by higher ratios of mobile nodes.
- **More roots** improve performance as it offers more routing path diversity.
- **Mobile roots** are catastrophic for performance, as all routing is aimed towards this root.



Mobile impacts on performance metrics

Energy consumption
Packets need to be resent.

Packet delivery ratio
Frequent interruptions of routing paths.

Expected transmission count
More data loss.

End-to-end delay
With a lower PDR and higher ETX, delays are increased [1] [4].

Control traffic overhead
TrickleTimer resets increase control traffic in the network.

Authentication
Key exchanges are protracted and sessions interrupted.

Access control
Nodes are more prone to errors and failures.

Availability
Increased delays and failures.

Data integrity
Signature schemes can be too burdensome.

Confidentiality
Encryption algorithms might be too costly.

5. DIS flooding attack

- Both mobile impact and DIS flooding attacks deteriorate the availability of a network.
- A DIS flooding attack performed from a moving node can have changing recipients.

Mitigations

- Secure-RPL [2] uses thresholds to limit the number of DIS messages per node.
  - This constraints the receivers of the DIS messages and delays reconnections.
- µTESLA [3] requires nodes to:
  - Generate keys
  - Authenticate packets
  - Maintain a steady connection with the base station.

6. Future work

- Research into other attacks and their mitigations in mobile situations is vital for RPL's security.
- Performance analyses tested in a physical mobile network will be interesting.
- Finally, research into updating the standard by combining extensions and protocols.

Abbreviations

- **IoT** = Internet of Things.
- **RPL** = Routing Protocol for Low-power and Lossy Networks.

References

[1] 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.
[2] 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
[3] 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
[4] M. Bouaziz, A. Rachedi, and A. Belghith, "Ekfmrpl: 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