RPL Attack Analysis: Evaluation of a Cryptography-based Sybil Defence in IEEE 802.15.4

Ruben Stenhuis **2-7-2021**
R.Stenhuis@student.tudelft.nl

Supervisors
M. Conti
C. Lal

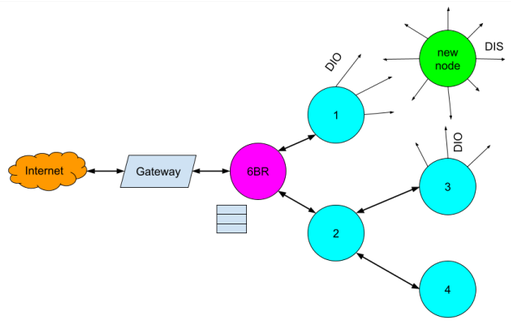
Problem (1)

- Broad application and market potential of IoT [1], but:
  - **inefficient** key management.
  - **Security, privacy** and **interoperability** Issues.
- **incoherent security** research for **RPL**.

Research Question:

"What generic attacks to IoT remain an imminent threat in RPL-based networks and what mitigation can be employed against this threat in IEEE 802.15.4"

RPL (2)



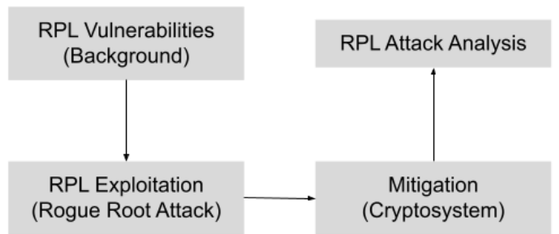
Security Measures of RPL:

Preinstalled: An key is preinstalled for **AES-128** in **CBC-HMAC** or **RSA** operations.

Authenticated: Use of session key from a authentication authority, nodes that promote to routers need to solicit this key.

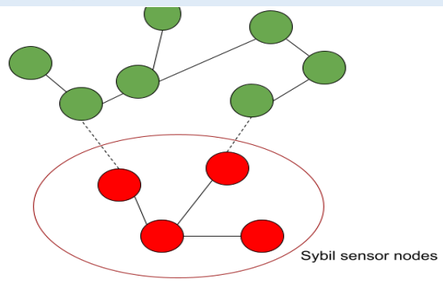
Approach (3)

1) Document the vulnerabilities and IoT generic attacks for RPL.
2) Demonstrate the severity of an attack type.
3) Evaluate the mitigation with the new adversarial perspective.

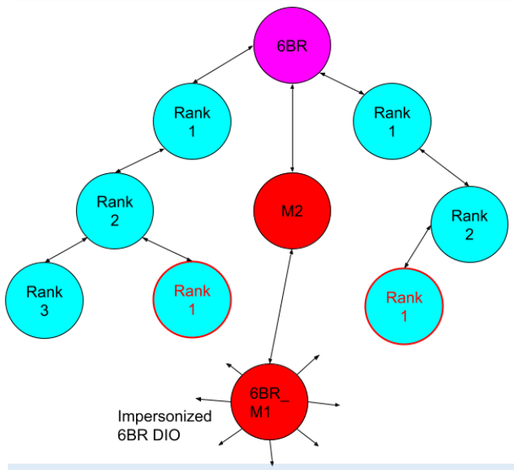


Sybil Attacks (4)

- Adversary creates **fabricated** or **stolen identities**.
- The adversary advertises the identity and captures the traffic and privileges of the address, with the **6LoWPAN Fragment duplication exploit** for RPL.
- For instance, sensor data can now be manipulated as shown below.



Privilege Elevation (5)

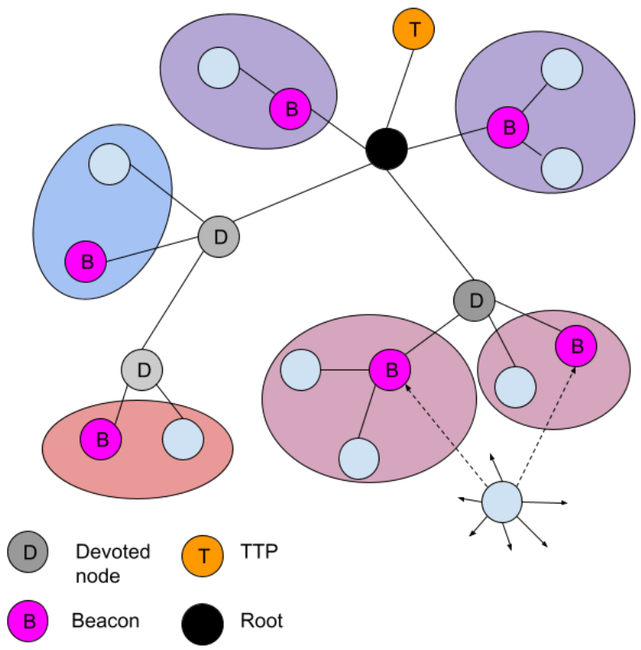


Resources:

- One node for **6BR** impersonalization.
- One sybil leaf node.
- out-of-range of the **6BR**.

Impact: DoS, eavesdropping, Isolation.

Solution (6)



- **Devoted nodes** regulate an authentication key exchange**.**
  - This isolates nodes in a security domain, called clusters.
  - **Key derivation functions** create and retrieve **cluster keys** for **devoted nodes**.
- **Beacons** measure the **link quality** on joining nodes. **Devoted nodes** assign the node to a cluster based on this.

Effect:

- Sybil attacks and eavesdropping are limited to within the cluster.
- Adversaries may find a collision by (offline) **brute force** or spoofing (mitigated by **beacons**).
- Less communication with the **TTP**, lightweight crypto, and no storage of **cluster keys**.

Future Work (7)

- **Performance analysis** of an implementation.
- **Efficient handoffs** for MANETs.
- **Perfect Forward Secrecy** (PFS) on the key derivation master key during global repair.
- **RPL operational attack analysis** for RPL specific attacks.

references

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015, doi: 10.1109/COMST.2015.2444095.