Study of RPL DODAG Version Attacks

Anthéa Mayzaud
anthea.mayzaud@inria.fr

Anuj Sehgal
s.anuj@jacobs-university.de

Rémi Badonnel **Isabelle Chrisment**

Jürgen Schönwälder

IFIP AIMS 2014 – Brno, Czech Republik

Motivations

- **Currently, no study of the consequences of these attacks targeting Internet-of-Things (IoT) networks**
- **Existing security strategies based on cryptographic operations**
  - VeRa, Version Number and Rank Authentication in RPL [1]
  - TRAIL, Topology Authentication in RPL [2]
- **Supporting the creation of a baseline to better develop mitigation strategies**
- **Observing attack-related patterns in order to improve counter-measures**

What is the impact of such an attack in an IoT network and does it make sense to mitigate it ?

Outline

- Background
  - Internet of Things
  - RPL Protocol
- Analysis of Version Number Attacks
  - Attack Description
  - Experimental Setup
  - Analysis Metrics
- Impact Evaluation Results
  - Control Packet Overhead
  - Delivery Ratio
  - End-to-end Delay
  - Number of Loops and Inconsistencies
- Conclusions

Outline

- Background
  - Internet of Things
  - RPL Protocol
- Analysis of Version Number Attacks
  - Attack Description
  - Experimental Setup
  - Analysis Metrics
- Impact Evaluation Results
  - Control Packet Overhead
  - Delivery Ratio
  - End-to-end Delay
  - Number of Loops and Inconsistencies
- Conclusions

Internet of Things

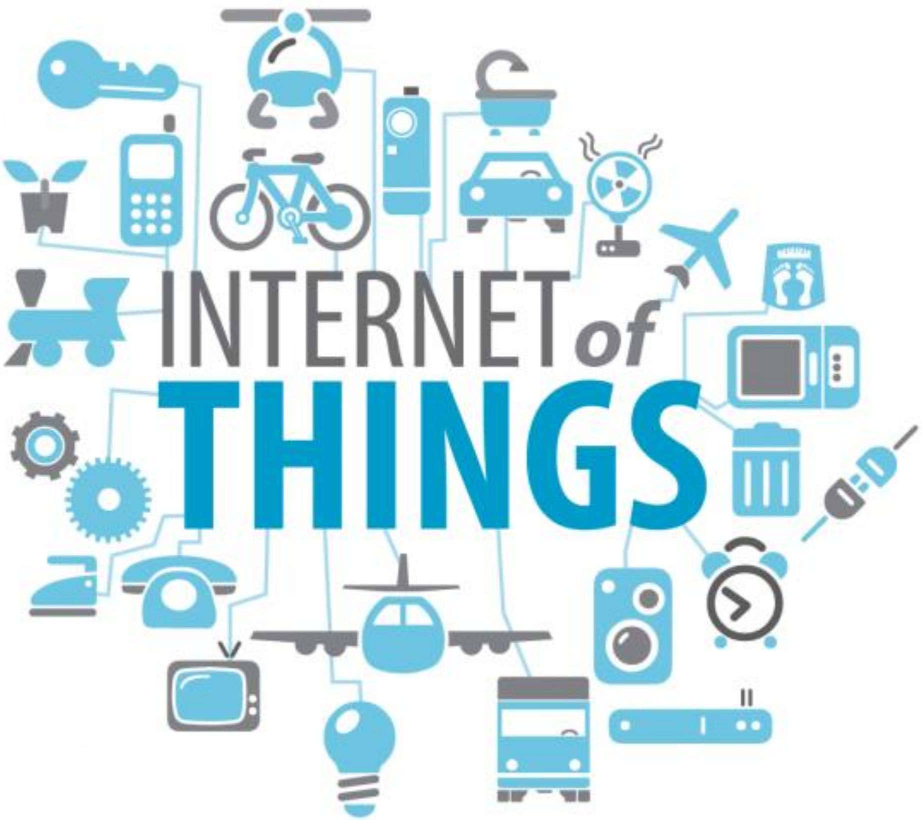


Illustration solarfeeds.com

- **Large-scale deployment of connected objects**
  - Sensors (wired or wireless)
  - RFID chips
  - Actuators…
- **Interactions and cooperations among objects**
- **Various application domains**
  - Logistics, transport
  - Smart environments
  - E-health…

LLN Networks and RPL

- **Nodes with strong constraints**
  - Energy
  - Memory
  - Processing
- **Lossy links**
- **Low throughputs**

- **Existing routing protocols are not appropriate**
- **Design of a dedicated stack**

TCP/UDP

IPv6 RPL

6LoWPAN

802.15.4 MAC

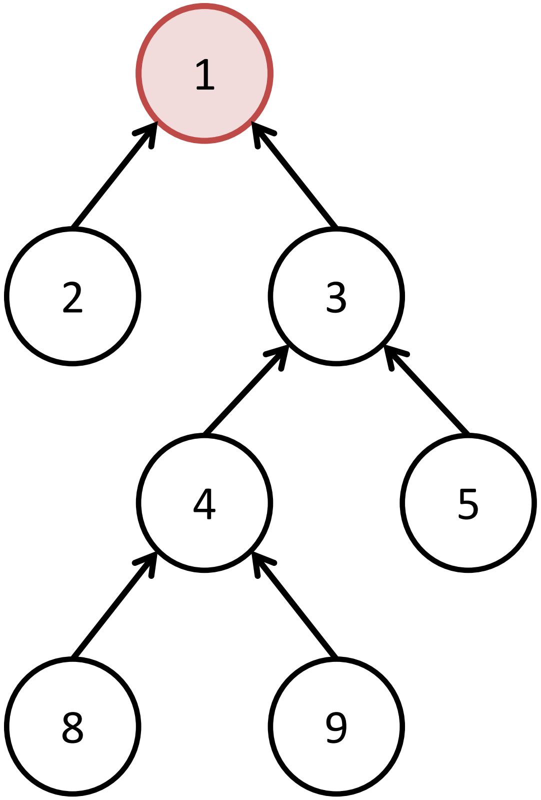
802.15.4 PHY

LLN : Low power and Lossy Network

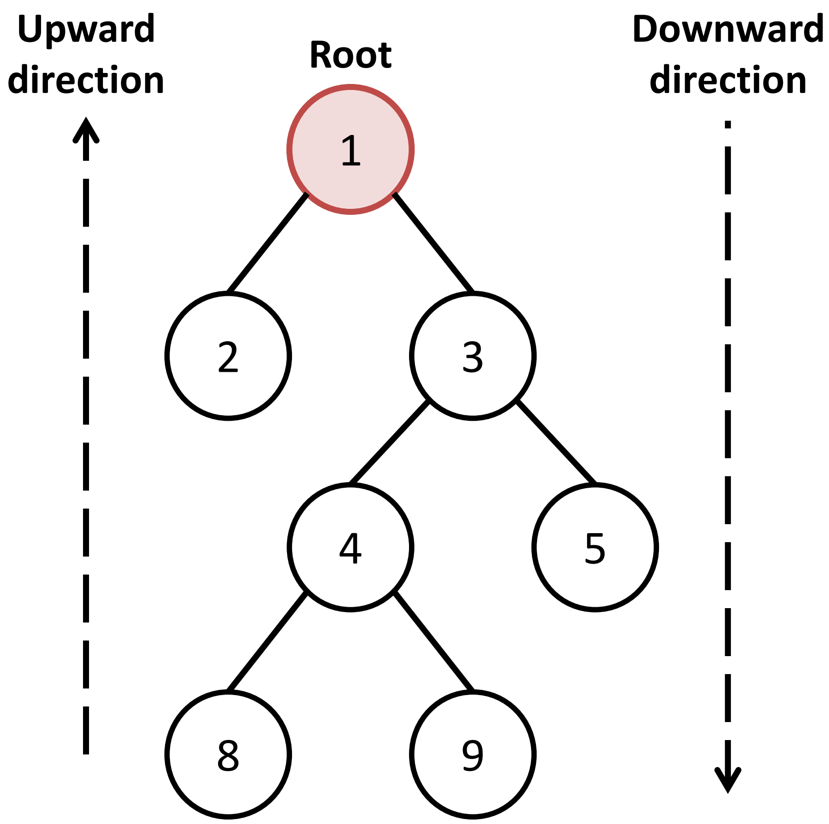
RPL : Routing Protocol for LLNs

The Routing Protocol for LLNs (RPL)

- **Protocol description**
  - RFC 6550 (March 2012) [3]
  - IPv6-based distance vector protocol
  - Building of specific graphs called **DODAG** **(**Destination Oriented Directed Acyclic Graph)
  - 3 ICMPv6 control messages (DIS, DIO, DAO)
- **Traffic patterns**
  - Multipoint-to-point (MP2P)
  - Point-to-multipoint (P2MP)
  - Point-to-point (P2P)
- **RPL instance**
  - Set of DODAGs
  - Optimized for a given routing objective based on metrics/constraints



RPL DODAG Principle



Root: destination node which manages the DODAG graph

Upward routes: built with DIO messages to reach the root

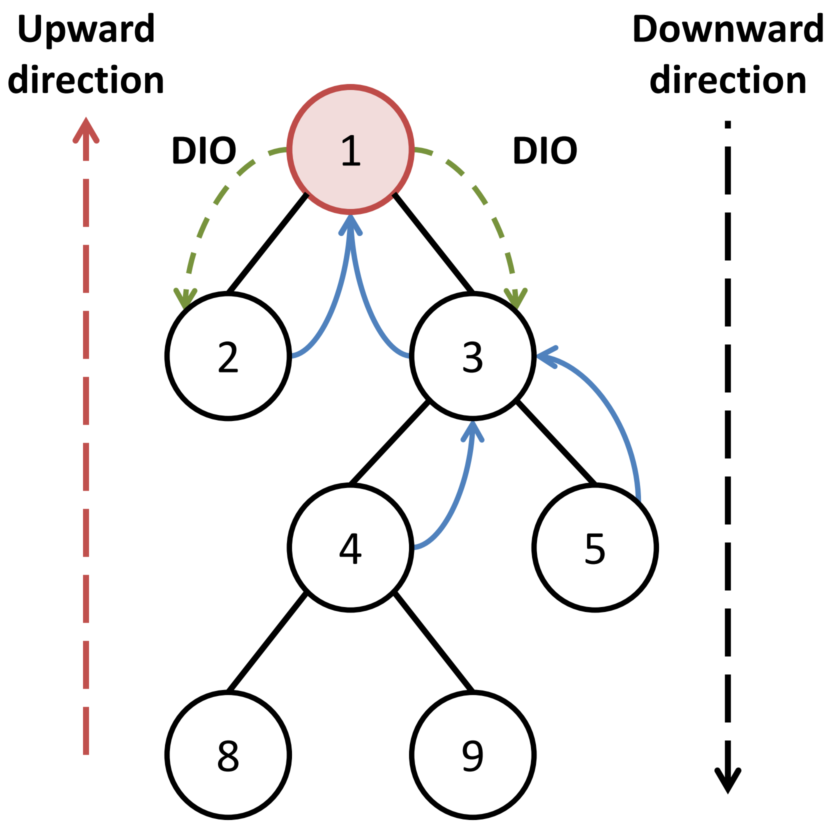
Trickle timer: used to define sending frequency of control messages

Downward routes: built with DAO messages to reach a node

Node rank value: used to indicate node's position with respect to the root ; always increasing in the downward direction

Metrics: used to characterize links and select the preferred parent

RPL DODAG Principle



Root: destination node which manages the DODAG graph

Upward routes: built with DIO messages to reach the root

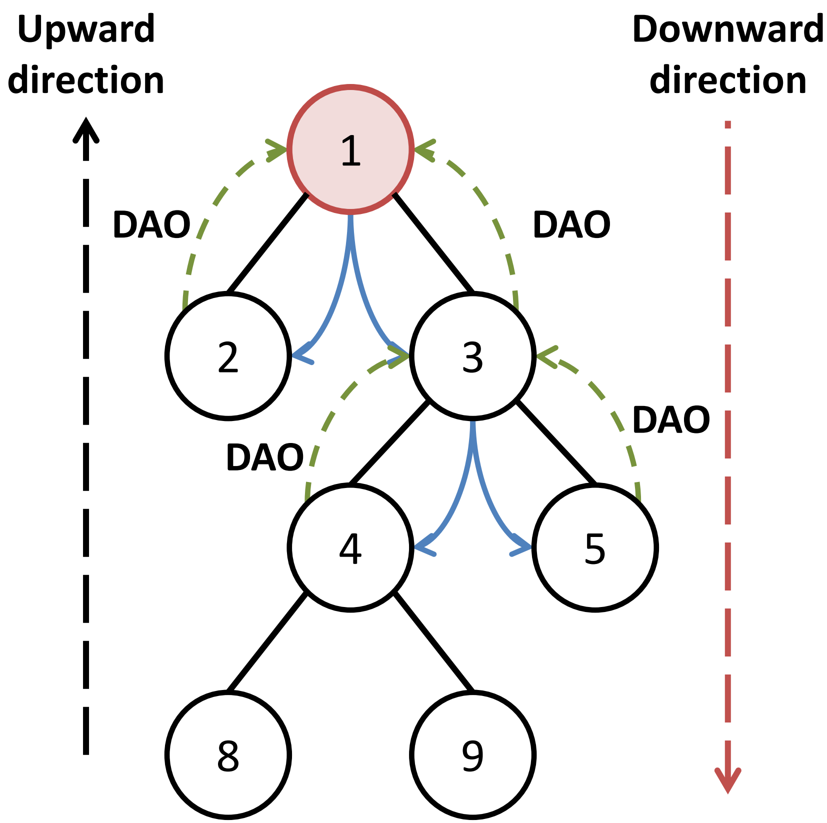
Trickle timer: used to define sending frequency of control messages

Downward routes: built with DAO messages to reach a node

Node rank value: used to indicate node's position with respect to the root ; always increasing in the downward direction

Metrics: used to characterize links and select the preferred parent

RPL DODAG Principle



Root: destination node which manages the DODAG graph

Upward routes: built with DIO messages to reach the root

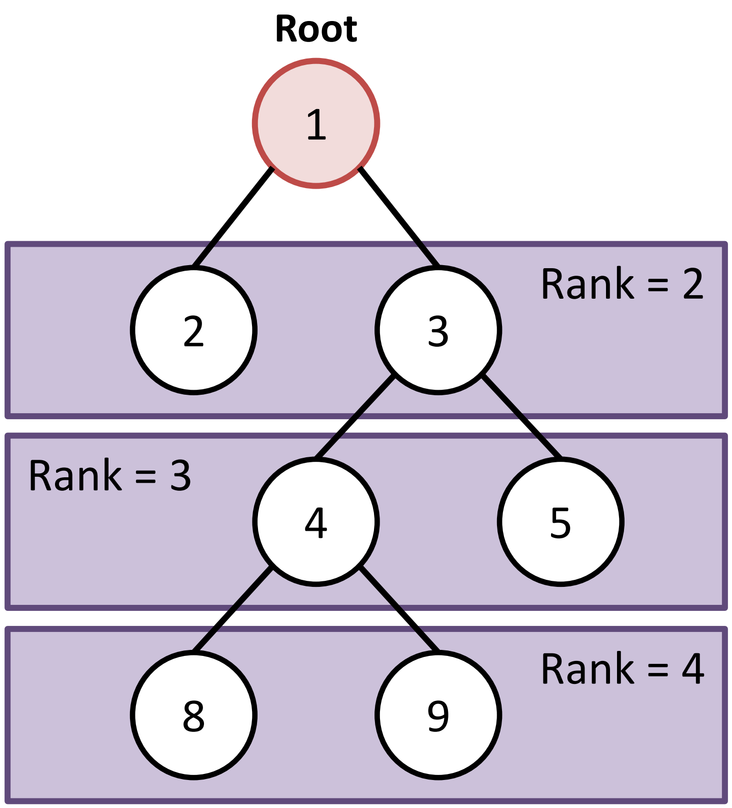
Trickle timer: used to define sending frequency of control messages

Downward routes: built with DAO messages to reach a node

Node rank value: used to indicate node's position with respect to the root ; always increasing in the downward direction

Metrics: used to characterize links and select the preferred parent

RPL DODAG Principle



Root: destination node which manages the DODAG graph

Upward routes: built with DIO messages to reach the root

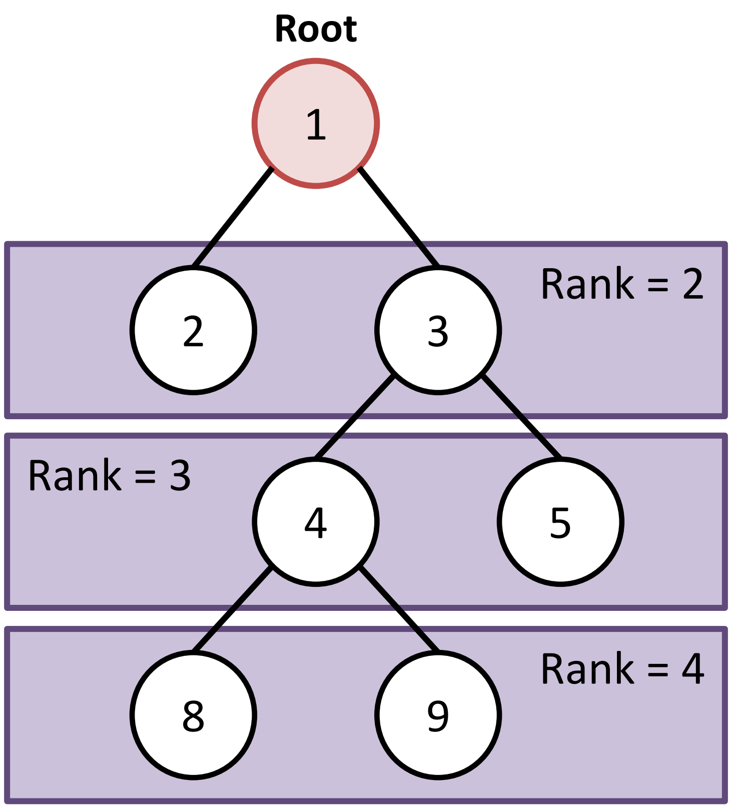
Trickle timer: used to define sending frequency of control messages

Downward routes: built with DAO messages to reach a node

Node rank value: used to indicate node's position with respect to the root ; always increasing in the downward direction

Metrics: used to characterize links and select the preferred parent

RPL DODAG Principle



Root: destination node which manages the DODAG graph

Upward routes: built with DIO messages to reach the root

Trickle timer: used to define sending frequency of control messages

Downward routes: built with DAO messages to reach a node

Node rank value: used to indicate node's position with respect to the root ; always increasing in the downward direction

Metrics: used to characterize links and select the preferred parent

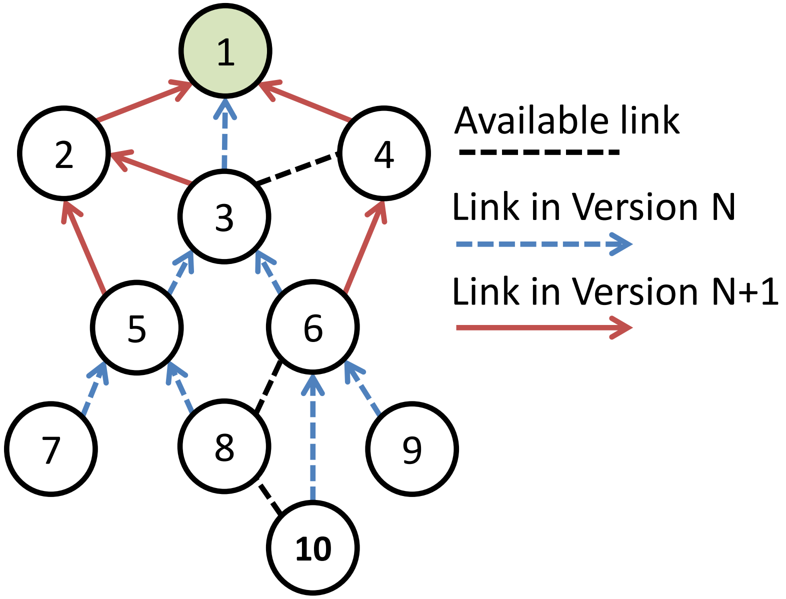
Other RPL Mechanisms

Datapath Validation [4]

- Data control mechanism used to detect loops
- Flags in the Hop-by-Hop option header
- ‘O’ flag used to track packet direction
- ‘R’ flag used to track rank error (mismatch between ‘O’ flag and current direction of a packet)

Version Number

- Version of a DODAG graph
- DIO field supposed to remain unchanged by the other nodes
- Only incremented by the root
- Used to rebuild the DODAG (global repair)

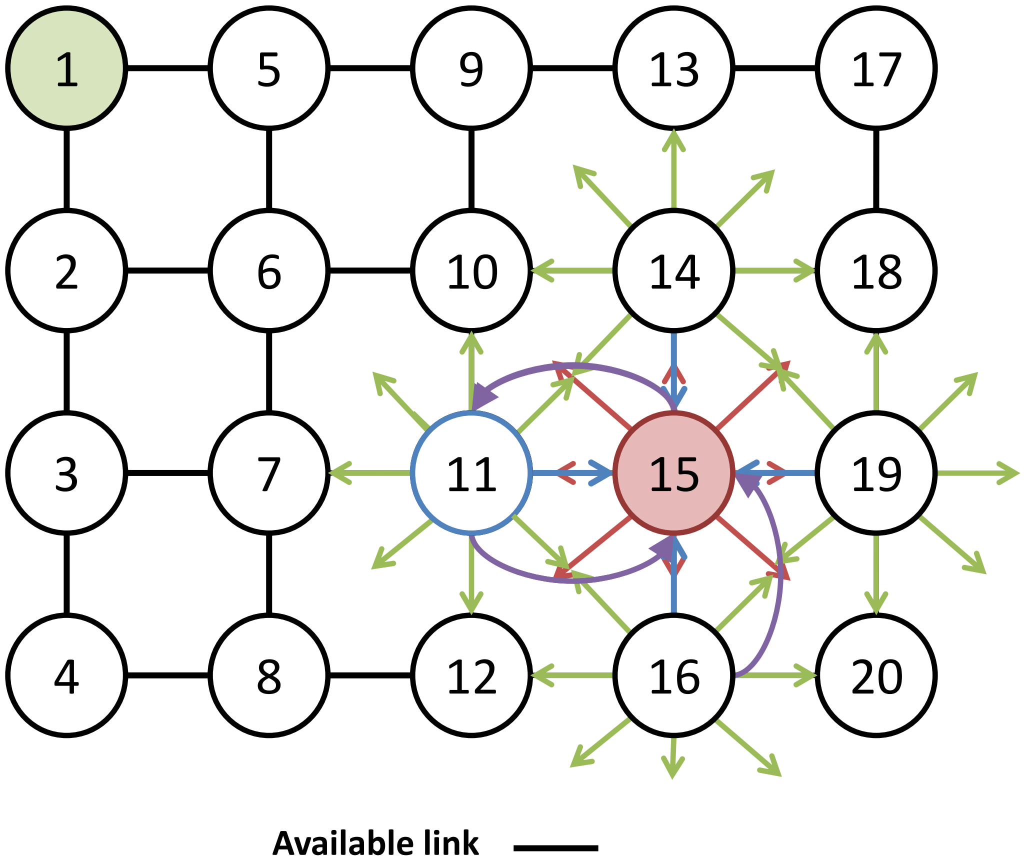


Outline

- Background
  - Internet of Things
  - RPL Protocol
- Analysis of Version Number Attacks
  - Attack Description
  - Experimental Setup
  - Analysis Metrics
- Impact Evaluation Results
  - Control Packet Overhead
  - Delivery Ratio
  - End-to-end Delay
  - Number of Loops and Inconsistencies
- Conclusions

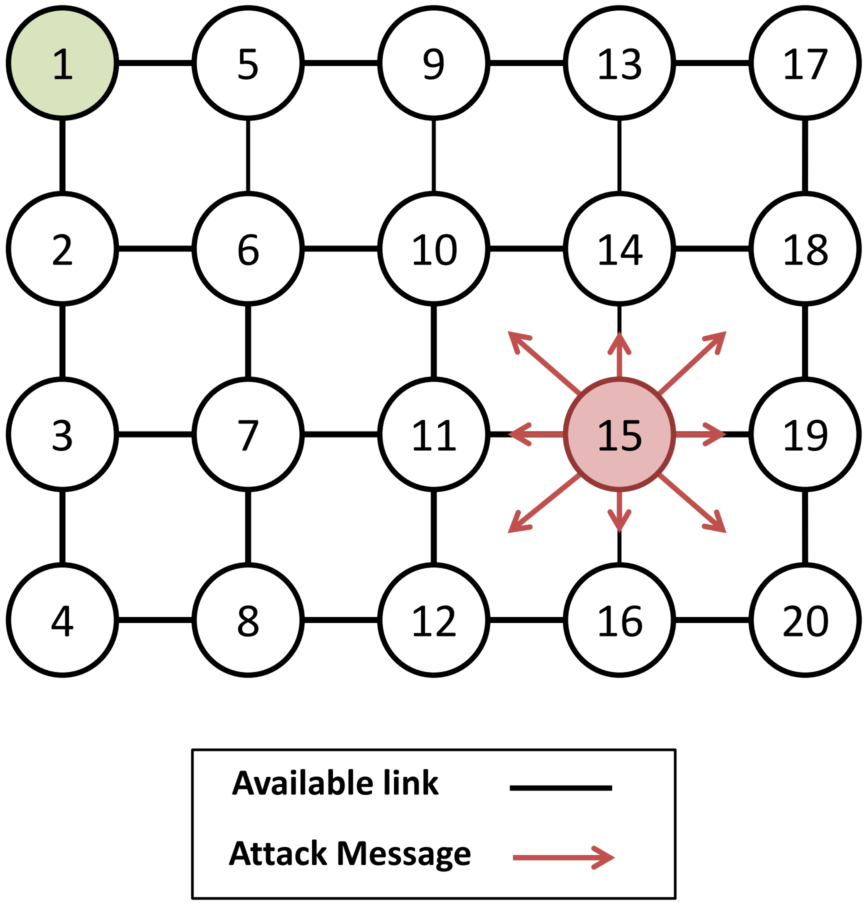
Attack Description

- **Increment of the version number by an attacker**
- **Propagation of the malicious version number**
- **Direct consequences**
  - Unnecessary rebuilding
  - Control message overhead
  - Loops generation
- **Indirect consequences**
  - Impact on energy reserves
  - Data packets loss
  - Channel availability



Experimental Setup

- **Grid topology of 20 nodes**
  - Node 1 is the DODAG root
  - Relocation of the attacker to multiple positions
- **Simulations based on Cooja (Contiki 2.6)**
  - 1 simulation without attacker as a baseline
  - Duration of 50 min.
  - 5 times each scenario
  - Attacks start after 5 min.



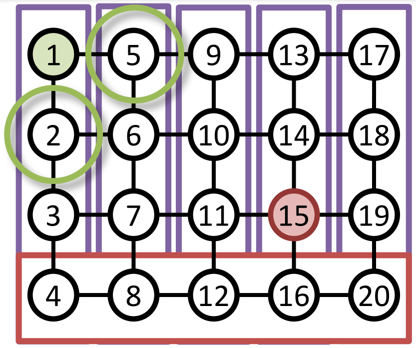
Analysis Metrics

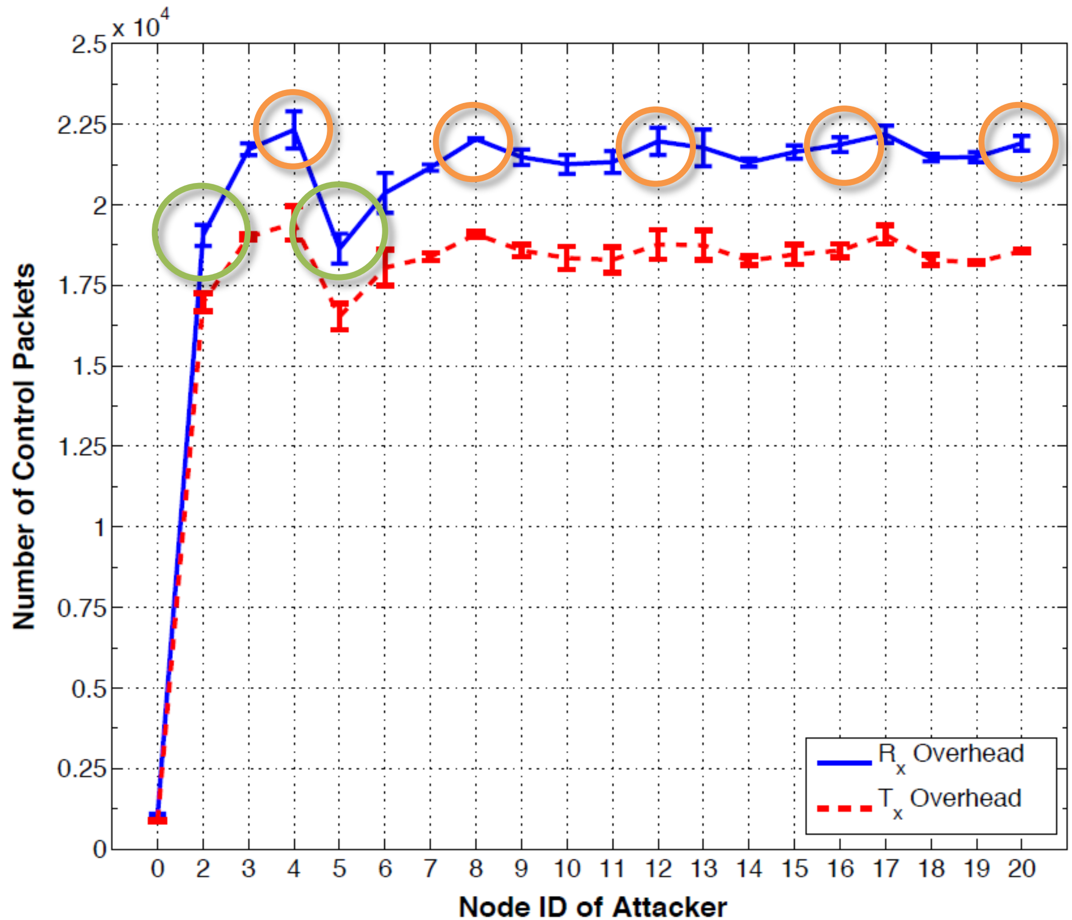
- **Control packet overhead**
  Total number of RPL control packets (DIS, DIO, DAO) transmitted and received
- **Delivery ratio**
  Number of data packets successfully delivered to the sink compared to the number of data packets generated by all nodes
- **Average end-to-end delay**
  Average time spent for all packets from all nodes to be successfully delivered
- **Number of inconsistencies**
  Number of packets when a mismatch between the 'O' flag and the actual direction is detected
- **Number of loops**
  Number of packets when an inconsistency is detected with the 'R' flag

Outline

- Background
  - Internet of Things
  - RPL Protocol
- Analysis of Version Number Attacks
  - Attack description
  - Experimental Setup
  - Analysis Metrics
- Impact Evaluation Results
  - Control Packet Overhead
  - Delivery Ratio
  - End-to-end Delay
  - Number of Loops and Inconsistencies
- Conclusions

Control Packet Overhead

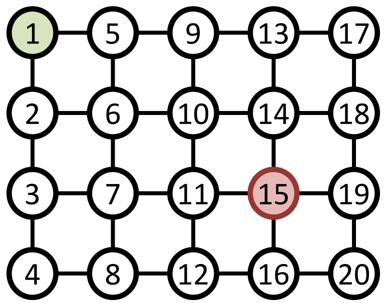


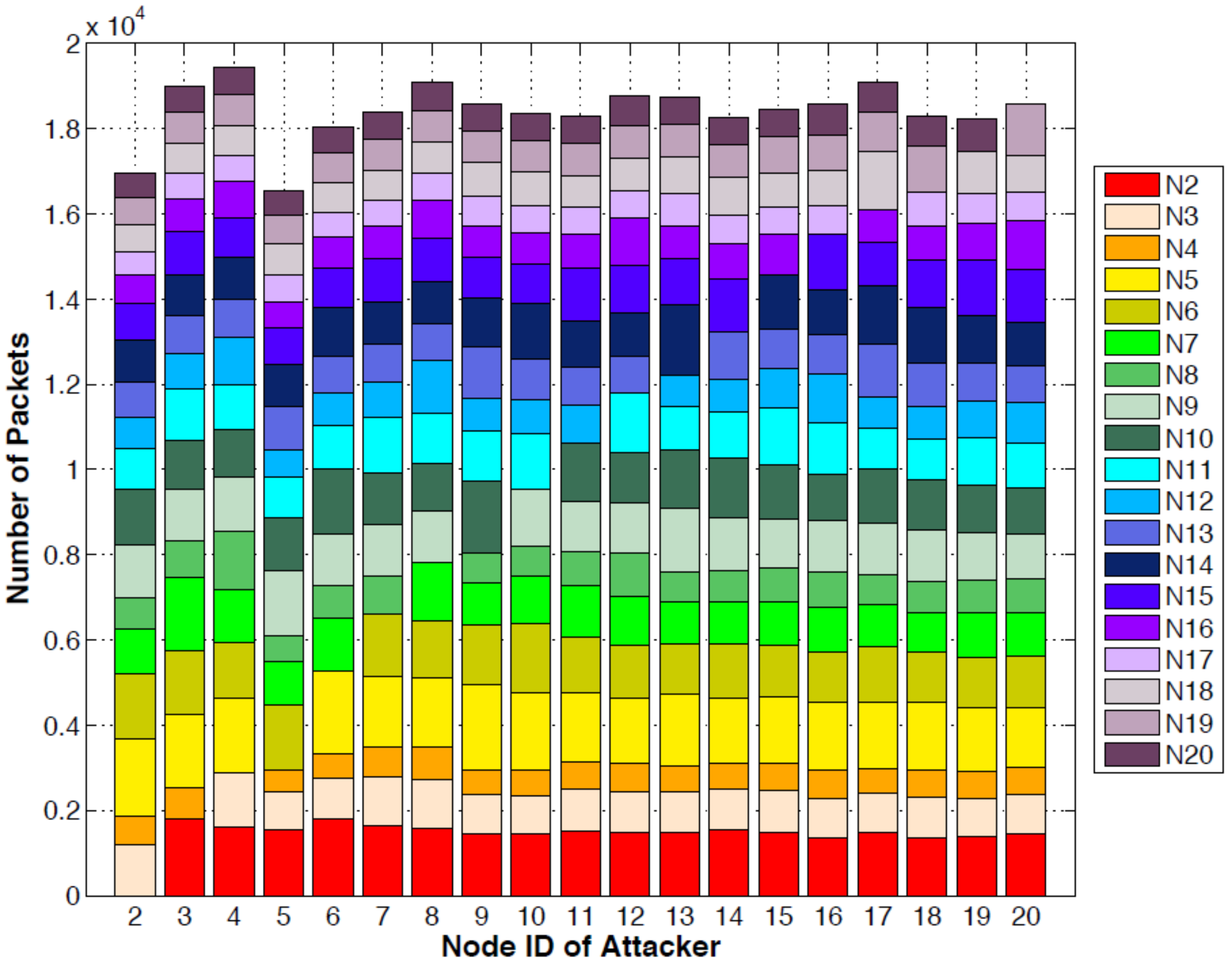


- Overhead for every node
- 1250 control pkts without attacker
- Up to 18 times in the worst case
- Per column: maximum for the nodes in the bottom row (4, 8, 12, 16, 20)
- Similar results for positions 2 and 5 which are minimums

Not only the number of neighbors, but also the distance from the root impacts the overhead.

Per Node Outgoing Packet Overhead

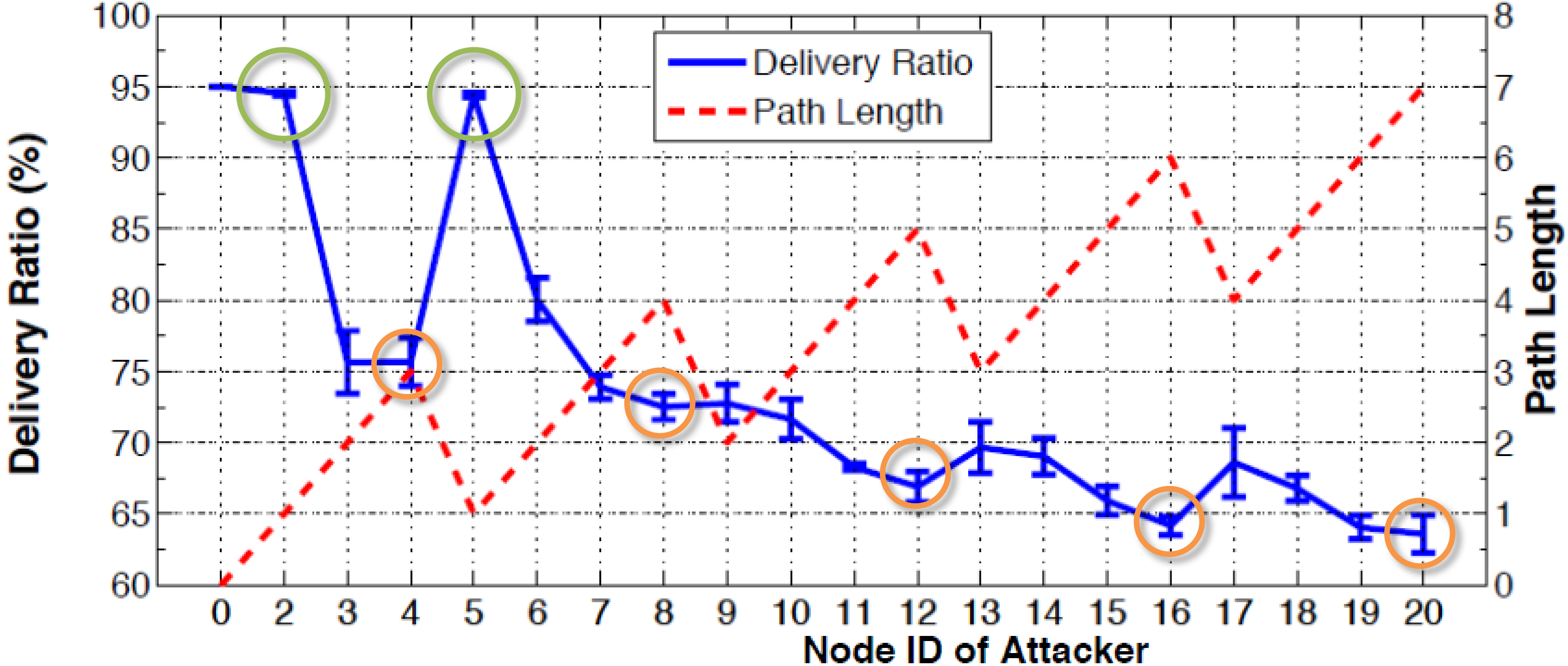




Overhead not only localized at the neighborhood of the attacker

Not only the attacker neighborhood is impacted, but also the entire network.

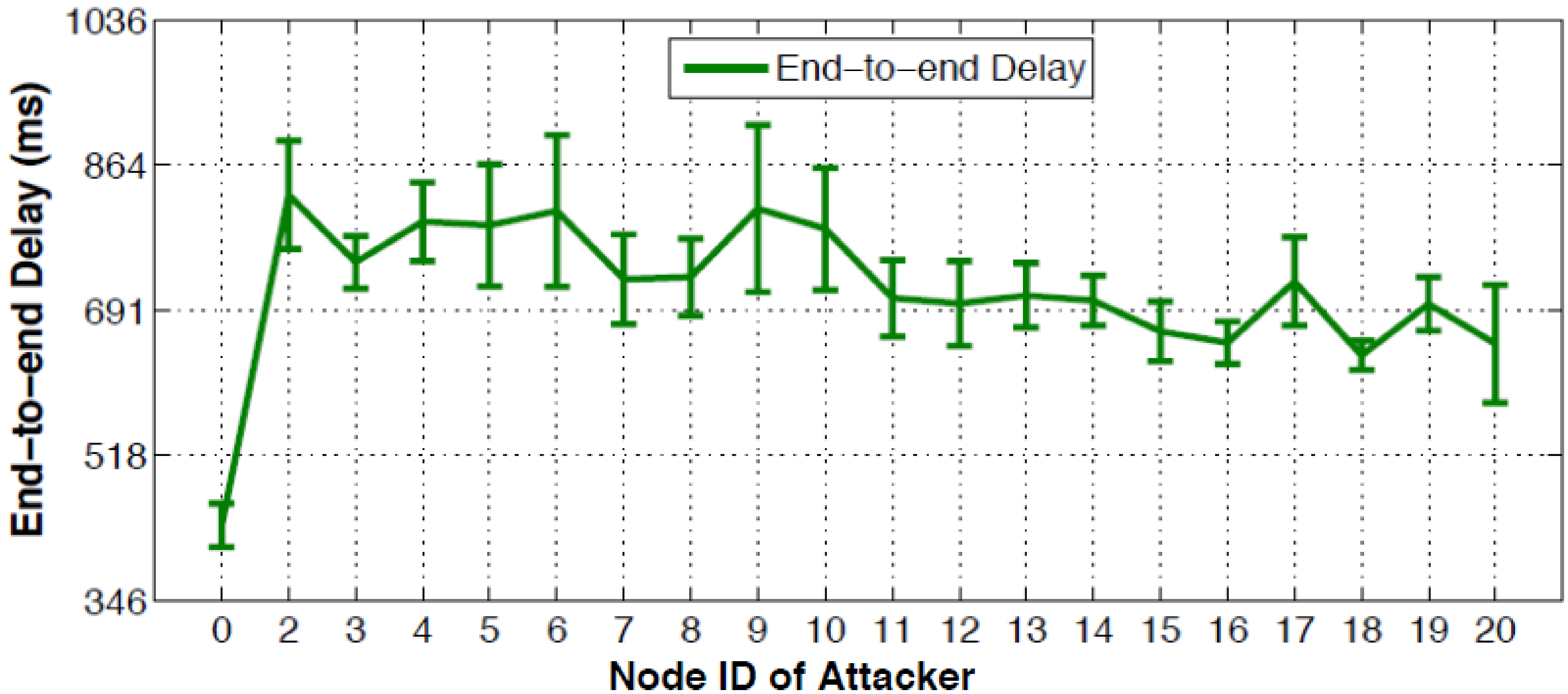
Delivery Ratio



- Reduced by up to 30%
- Similar pattern than packets overhead
- Strong correlation between path length and effects on the DR

The farther the attacker from the root, the worse the delivery ratio.

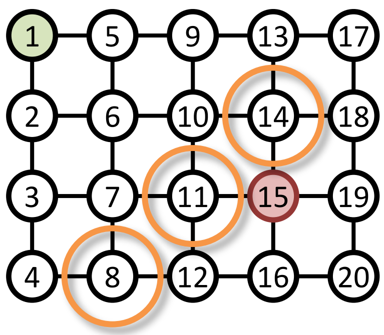
Average end-to-end delay

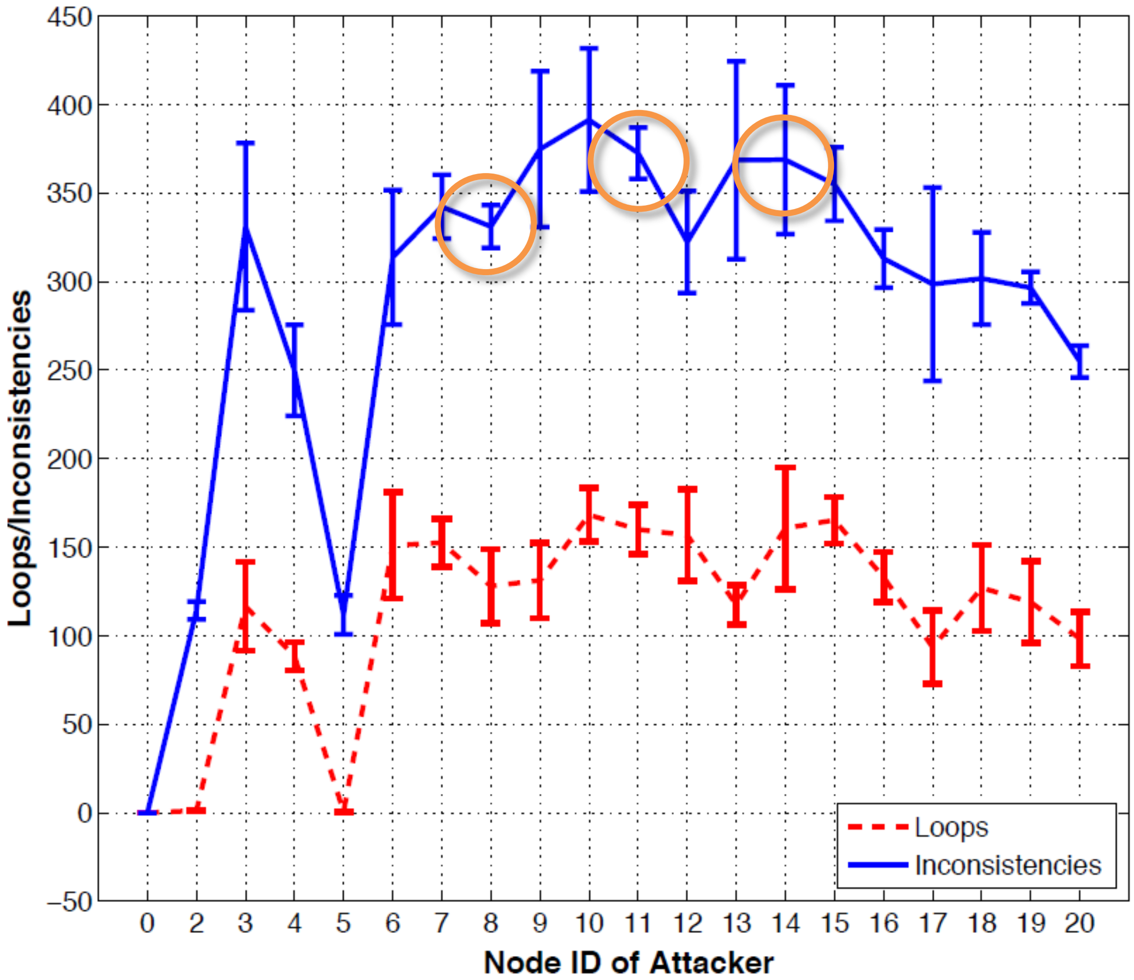


- Almost doubled
- High variation in the results

No strong correlation between location of the attacker and the delay.

Loops and Inconsistencies

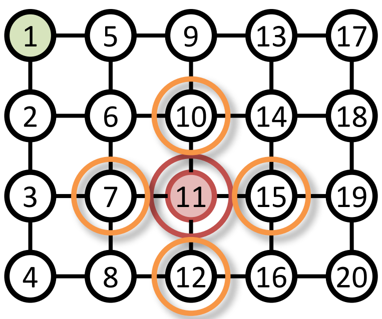




- Same pattern
- Greater distance from root, lesser inconsistencies
- Proximity to the root and most number of neighbors, highest number of loops

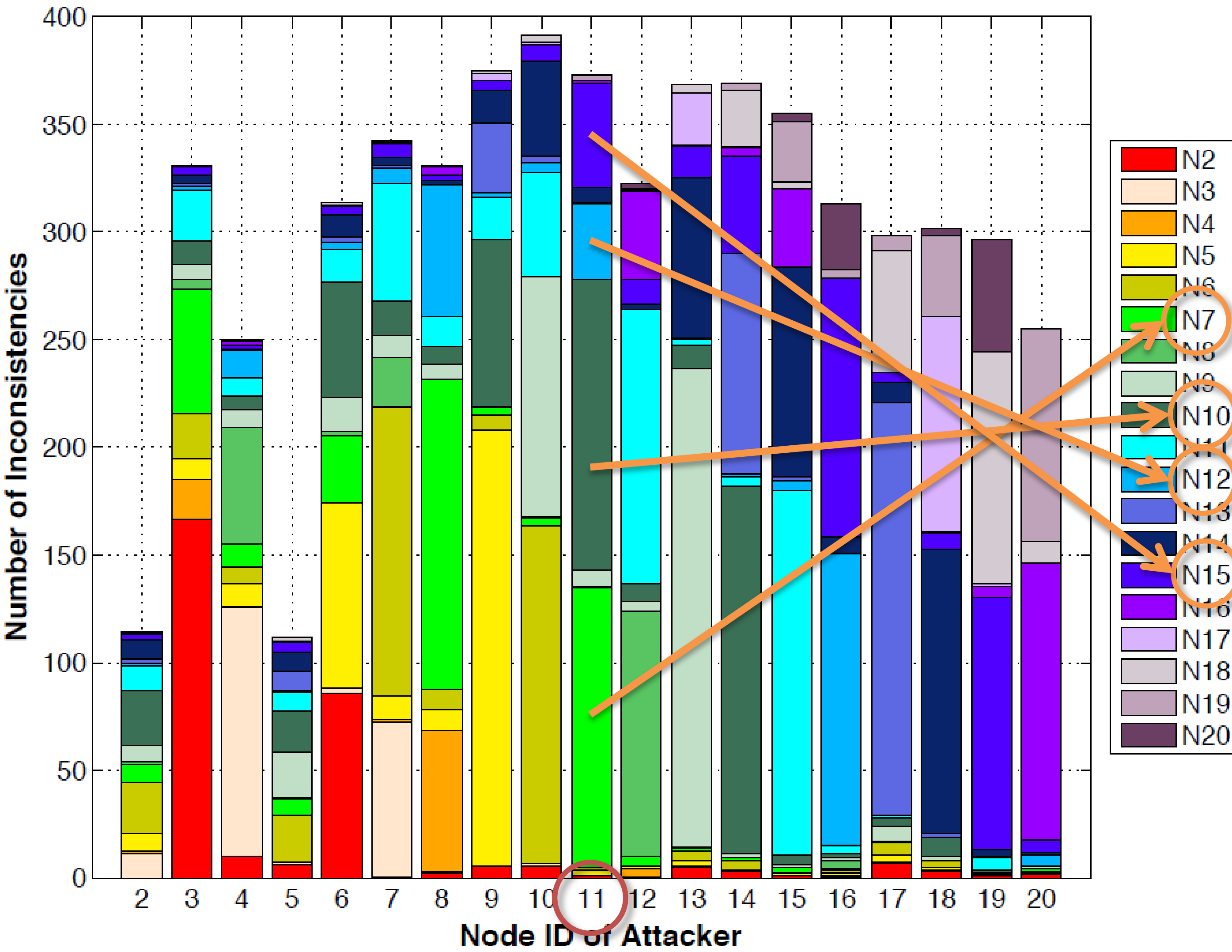
Larger number of neighbors and attacker proximity to root lead to higher number of loops and inconsistencies.

Inconsistencies per Node



Inconsistencies mostly located around the attacker

Majority of inconsistencies is detected by parents of the attacker and also by its children.



Outline

- Background
  - Internet of Things
  - RPL Protocol
- Analysis of Version Number Attacks
  - Attack Description
  - Experimental Setup
  - Analysis Metrics
- Impact Evaluation Results
  - Control Packet Overhead
  - Delivery Ratio
  - End-to-end Delay
  - Number of Loops and Inconsistencies
- Conclusions

Conclusions and Future Work

- **Study of the impact of version number attacks within RPL networks**
  - Increase of control packets overhead by up to 18 times
  - Decrease of delivery ratio by up to 30%
  - End-to-end delay nearly doubled
  - Strong correlation between the position of the attacker and the observed effects
  - RPL network lifetime can be drastically shorten

- **Perspectives**
  - Extension to more complex topologies
  - Evaluation of existing solutions based on observed baseline
  - Development of lightweight mitigation strategies based on identified attack patterns

References

[1] Dvir et al., *VeRa – Version Number and Rank Authentication in RPL*, in Proc. of the IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS), 2011, Hangzou, China.

[2] Perrey, H. et al., *TRAIL: Topology Authentication in RPL*, in CoRR, 2011 .

[3] Winter, T. et al., *RPL, IPv6 Routing Protocol for Low-Power and Lossy Networks*. IETF RFC 6550 (March 2012).

[4] Hui, J. and Vasseur, J., *The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams.* IETF RFC 6553 (March 2012).

[5] Contiki project: http://www.contiki-os.org

[6] Tsao, T. et al., *A Security Threat Analysis for Routing Protocol for Low-power and Lossy Networks (RPL).* IETF Internet Draft (December 2013).

Thank you for your attention!
Questions?