HCR: Detection and mitigation of the coordinated blackhole attack in RPL networks

RESEARCH QUESTION

Which limitations do existing solutions against collusion attacks exhibit? How can these limitations be addressed?

ALGORITHM

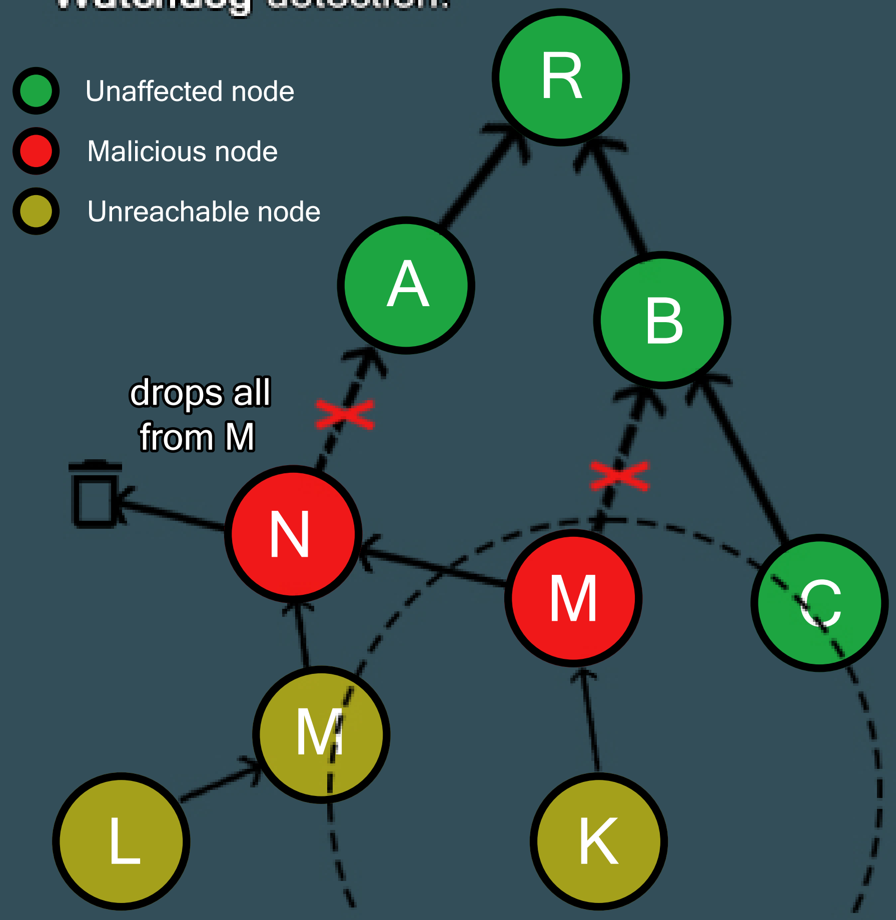
Leaf nodes periodically ping the root node with DAO messages. The root node responds with a DAO-ACK upon arrival.

The nodes performing HCR count the number of ACKs they receive.

If too many ACKs are lost within a predetermined timeframe, the node assumes the attack is happening in its chain of parents, and will attempt to switch parents.

HOW HCR WORKS - A SCENARIO

Multiple nodes are colluding to disrupt the network by performing an advanced blackhole attack. Malicious nodes appear to be properly behaving, thereby **avoiding Watchdog** detection.



PERFORMANCE ANALYSIS

HCR has **100% detection rate**. **Mitigation** rate **varies** depending on available unaffected parents. Mitigation **works** whenever affected nodes can **switch** to **(eventually) unaffected parents**. **Control packet overhead** increases between **1.6% and 25%** depending on **chosen parameters**.

CONCLUSION & FUTURE WORK

HCR **detects** and possibly **mitigates** CBA **in dynamic networks**. Performance comparison against other methods is **inconclusive**.

Future research is needed in:
- Other dynamic detection of the coordinated blackhole attack.
- Verification of HCR in simulations.
- Optimalisation of HCR parameters.
- Specialized data packets for pinging.

CHALLENGES

Resource constrained

Must support as low as **8-bit devices** with **128kB of memory**, while maintaining at least **5 years battery life**.

Huge demand & Horizontal integration

46 billion IoT devices in 2021. Applications in **many fields**, including industrial-, home-automation and medical care.

Security risk

Trade-off between **security** and **performance**.

TU Delft

By
David Essaadi - davidessaadi@gmail.com

Supervisors
Chhagan Lal, Mauro Conti