lasaris LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
Masaryk University

Trust-based Detection Strategy against Replication Attacks in IoT

Bacem Mbarek, Ph.D.
Masaryk University, Czech Republic
Lasaris Lab (Lab of Software Architectures and Information Systems)

Published in AINA 2021 (B conference) and selected and published as an extended version in the IoT Elsevier Journal.

PLAN

What is 6LoWPAN?

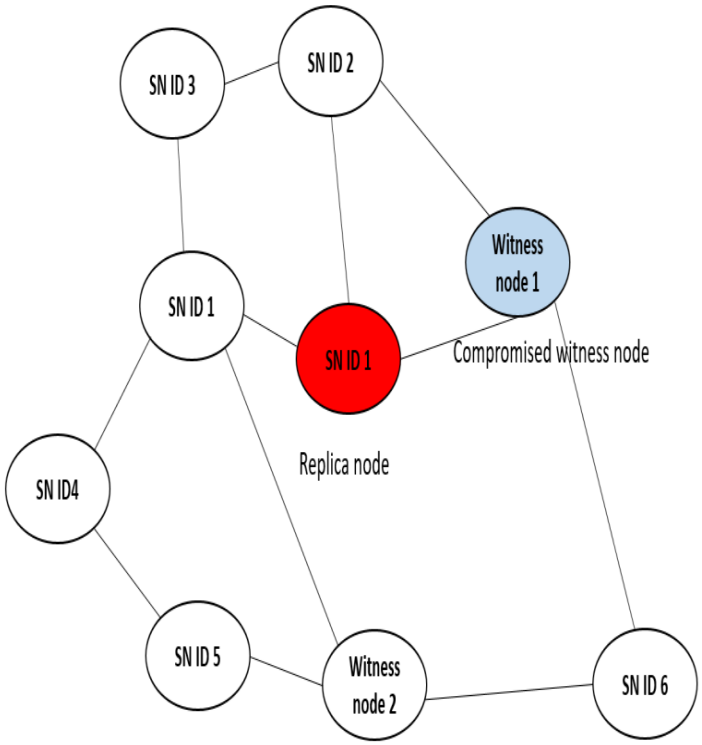
FACULTY OF INFORMATICS
Masaryk University

6LoWPAN is one of the most successful standards that defines the approach for routing IPv6 over low-power wireless networks. Thus, 6LoWPANis considered as a promising IoT technology, and can be applied even to the smallest IoT devices.

In 6LoWPAN, routing functionalities have been investigated under a dedicated routing protocol, namely RPL (Routing Protocol for Low Power and Losy Networks).

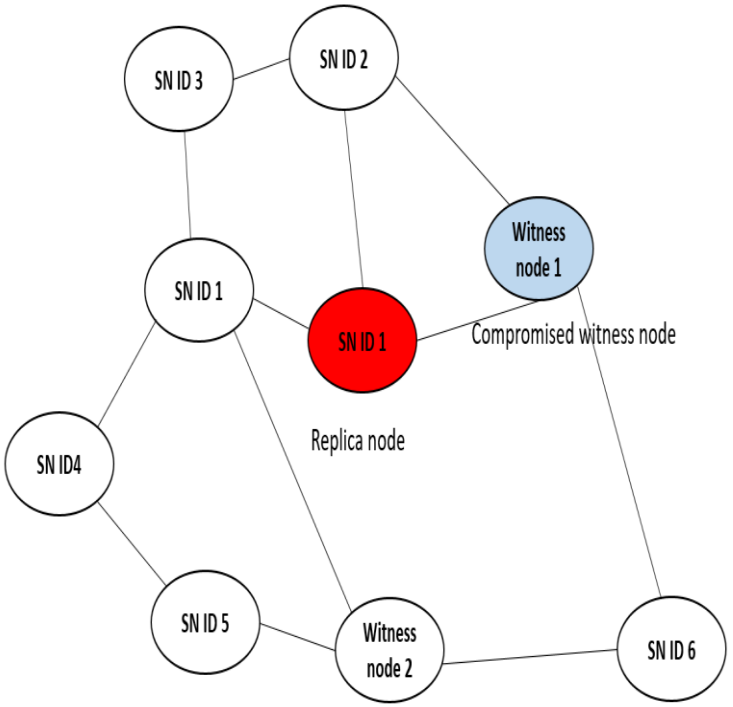
Problematic

- 6LoWPAN is vulnerable to a variety of attacks, among others, replication attack can be launched to consume the node's resources and degrade the network's performance.
- RPL-based 6LoWPAN network is usually vulnerable to various attacks given the resource constrained of IoT devices.
- One of the most severe cyber attacks is replication attack, where it creates replicated nodes in the IoT network.
- Once the replication attack compromises witness nodes, the adversary will make all the replicated nodes hidden as 6Mapper provides node ID and rank of each node.



Goals

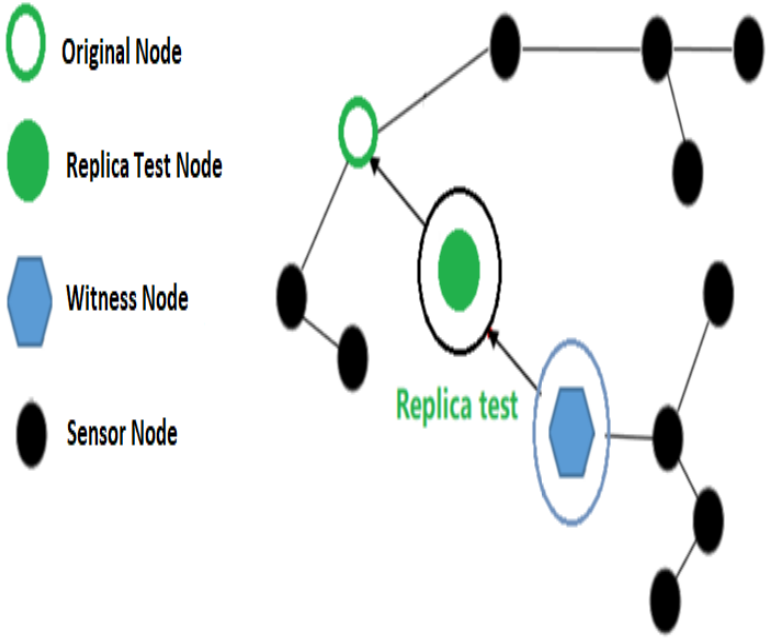
- This paper therefore proposes a trust-based detection strategy against replication attacks in IoT, where a number of replica nodes are intentionally inserted into the network to test the reliability and response of witness nodes.
- Those testing replica nodes is deployed intentionally to the witness node and uses the reaction of the tested witness node to consolidate the detection of compromised witness nodes.
- We compare the proposed trust-based strategy with two baselines strategies, which are brute-force strategy and first visited strategy.



Contributions: Overview

FACULTY OF INFORMATICS
Masaryk University

- We intentionally insert an arbitrary number of replica test nodes into the network to test the response of witness nodes.
- If the witness nodes do not detect these replica test nodes, the network will be considered as the case that there are compromised witness nodes used by the adversary who protects replicas from being detected.
- In this way, the deployed replica would be able to verify the compromised witness node. The replica node is inserted next to the witness node. Our new solution can test the reaction of the witness node to detect if it is compromised.



Contributions : Description (1)

FACULTY OF INFORMATICS
Masaryk University

- We intentionally insert an arbitrary number of replica test nodes into the network to test the response of witness nodes.

- The trust score depends on three factors: (1) Energy used to transmit a packet (ε),(2) Transmission delay (DT) and (3) Packet delivery ratio (PDR).

- TrustScore can be for example scaled into a rating from 1 to 10. Each node in the network start with a score equal to 10. All three factors serve as important functions in determining if a node has the possibility to be hacked, loaded with malware, or with other cyber-attacks.

- For example, a node can be considered as possible malfunctions or under attack if it expends abnormal energy in the transmission of a packet or a large delay in the submission of a packet or a low propagation speed.

Contributions : Description (2)

FACULTY OF INFORMATICS
Masaryk University

- In a predefined interval, the base station should analyze the behavior of each node by comparing their trust factors (ε, DT, and PDR) with the average score of each factor.

- If the value of the trust factor $Ti > Ti_{average}$, then a malfunction is detected and TSV will be−1, otherwise it is 0.

$$TSV = \begin{cases} -1, & \text{if } T_i > Ti_{average} \\ 0, & \text{otherwise} \end{cases}$$

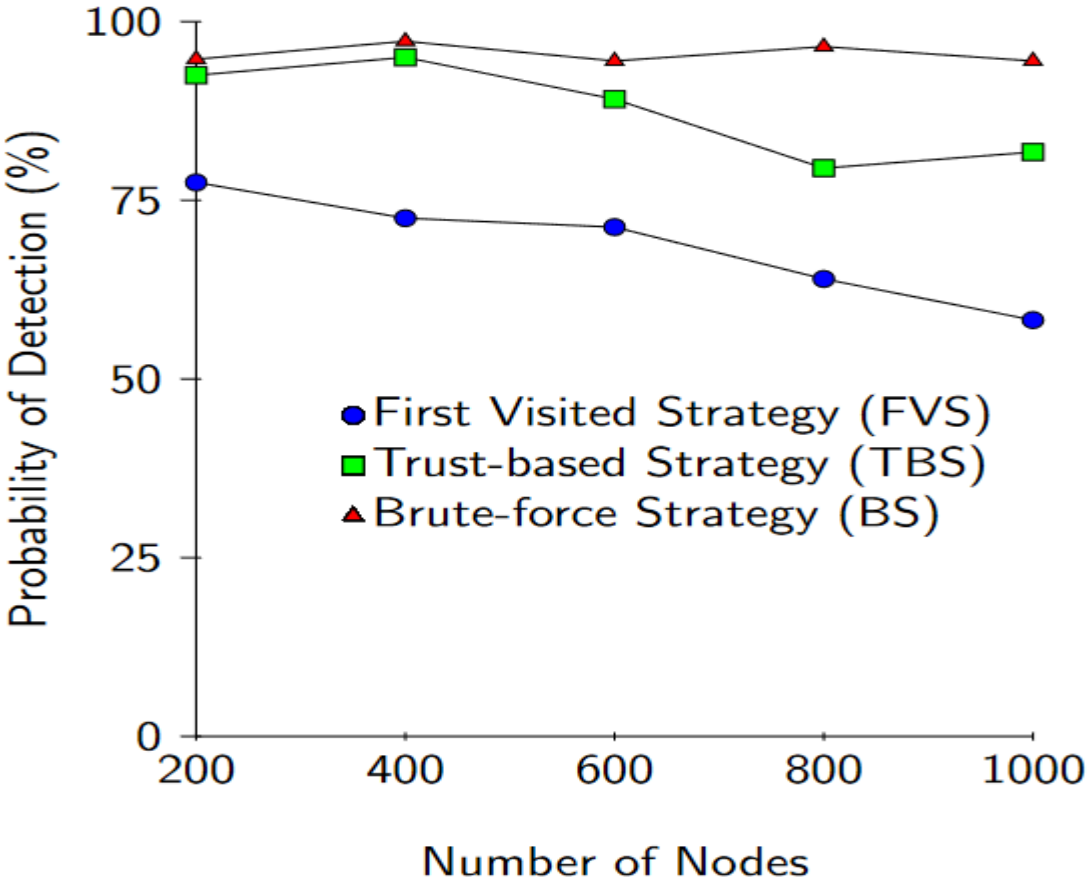
Evaluation

- We used the Contiki network simulator COOJA to analyze the performance of the trust-based strategy in terms of probability of detection of replication attacks and in terms of the runtime of detection.

- This embedded operating system, using the COOJA network simulator, allows a comprehensive of the new security scheme. It is written in the C language, and enables an easy deployment of the 6LoWPAN security extension.

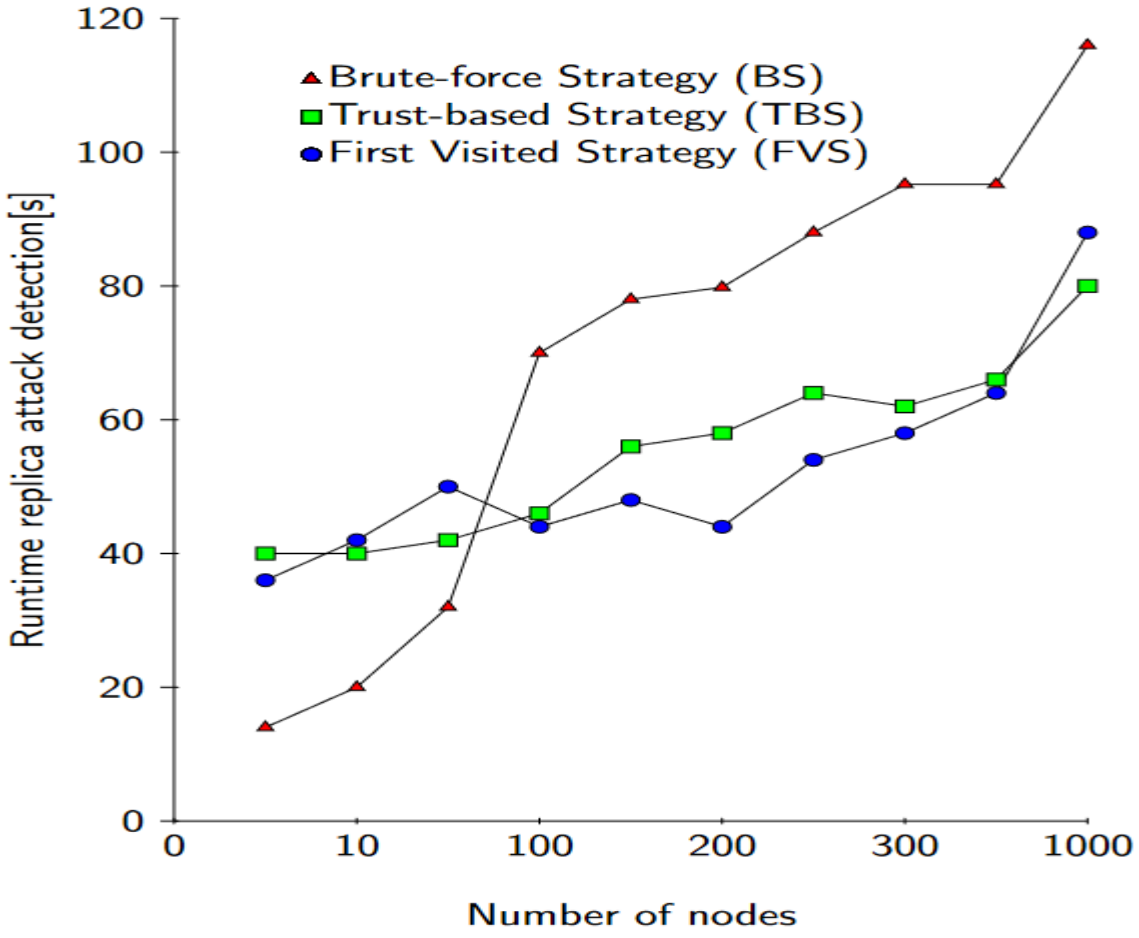
- During replication attacks in RPL-based 6LoWPAN networks, the attacker can use compromised nodes to send wrong information about their rank or one of their rank of neighbors to the intrusion detection modules

Probability of detection



Replica detection runtime

FACULTY OF INFORMATICS
Masaryk University



Conclusion

FACULTY OF INFORMATICS
Masaryk University

- In this paper, we have proposed a new trust-based detection strategy and algorithm against replication attacks in IoT network.
- This strategy has been used to detect the replication attacks in the presence of compromised witness node against the RPL-based 6LoWPAN network.
- The simulation results have shown that the trust-based strategy can significantly improve the effectiveness of detection probability of replication attacks while being comparable to brute-force strategy and first visited strategy when the number of nodes is larger.
- We found that the proposed trust-based detection strategy has a significantly lower delay than the other two strategies in the presence of higher number of nodes,

Perspectives

FACULTY OF INFORMATICS
Masaryk University

- In the future, we plan to generate a dynamic strategy for replica detection according to different network factors, such as number of nodes, network status, nodes' behavior, etc.

- In addition, we plan to apply different evaluation metrics to further investigate the robustness of the trust based detection strategy in various business domains such as connected transport and smart home,

FACULTY OF INFORMATICS
Masaryk University

Thank you for your attention

QUESTIONS AND DISCUSSION

email:
bacem.mbarek@mail.muni.cz