Zero-Watermarking Approach for Data Integrity and Secure Provenance in IoT Networks

Omair Faraj

Thesis Directors: Prof. Joaquin Garcia-Alfaro and Prof. David Megias

Samovar young researchers' day 2023

Motivation

1. IoT is integrating smart devices in almost every domain such as home automation, e-healthcare systems, vehicular networks, industrial control and military applications.
2. Sensory data, which is collected from multiple sources and managed through intermediate processing by multiple nodes, is used for the decision-making processes.
3. Ensuring data integrity and keeping track of data provenance is a core requirement in such a highly dynamic context (e.g., for the assurance of data trustworthiness).

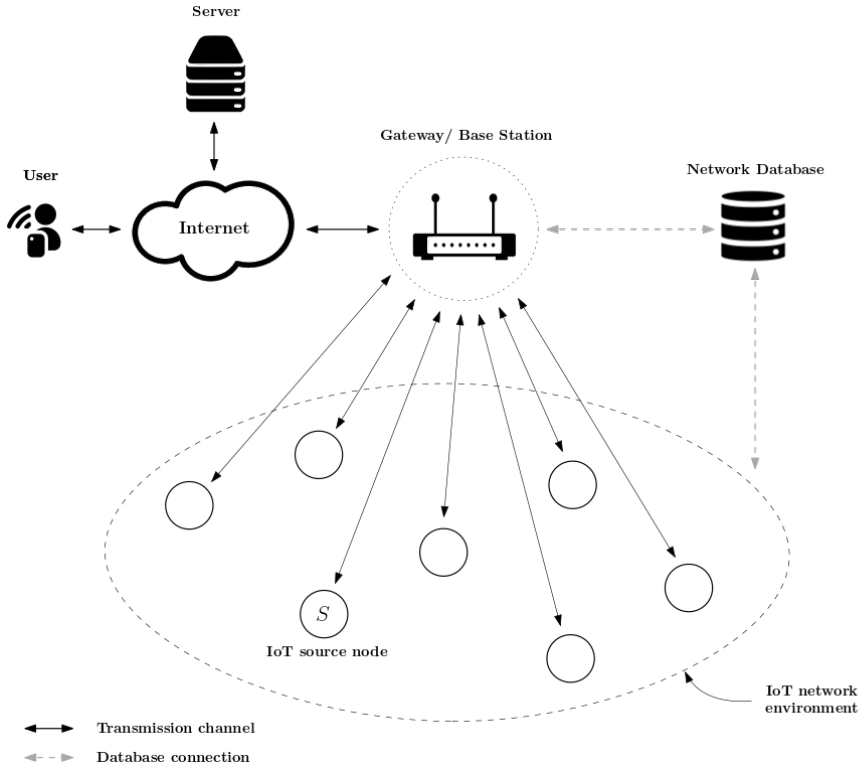
Data provenance allows tracing the source and forwarding the path of an individual data packet. Provenance data must be recorded for each packet, but essential challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes.

Objectives

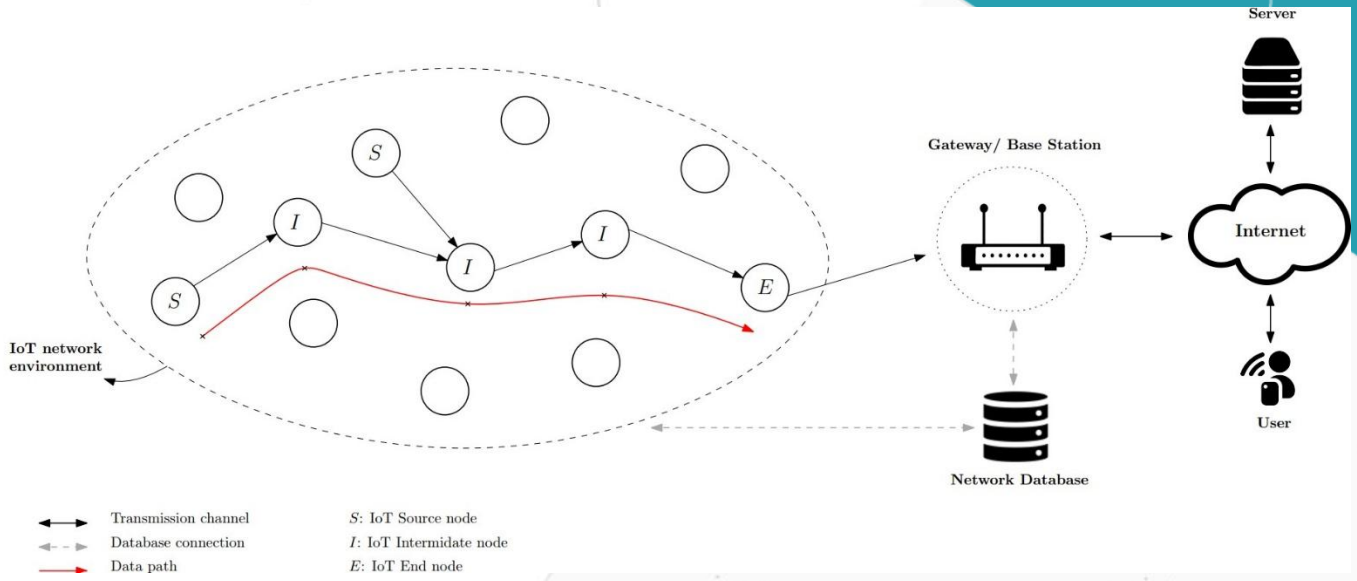
1. Propose a scheme for smart home IoT networks to ensure data integrity in single- and multi-hop scenarios.
2. Handle secure provenance transmission using a zero-watermarking approach with a tamper-proof network database.
3. Two main adversary models: passive and external adversaries.
4. Evaluate the performance of the final solution via simulation.

Proposed Approach

Single hop Scenario

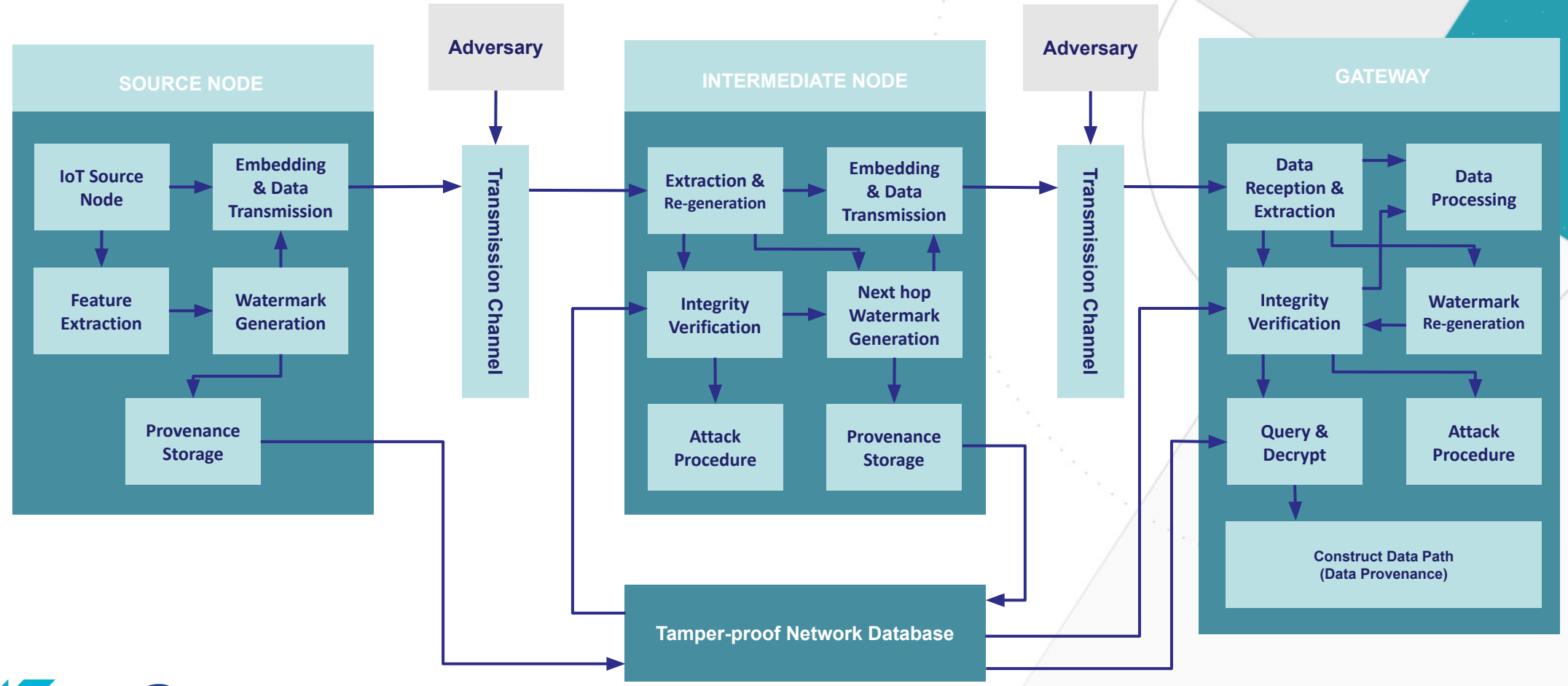


Multi hop Scenario



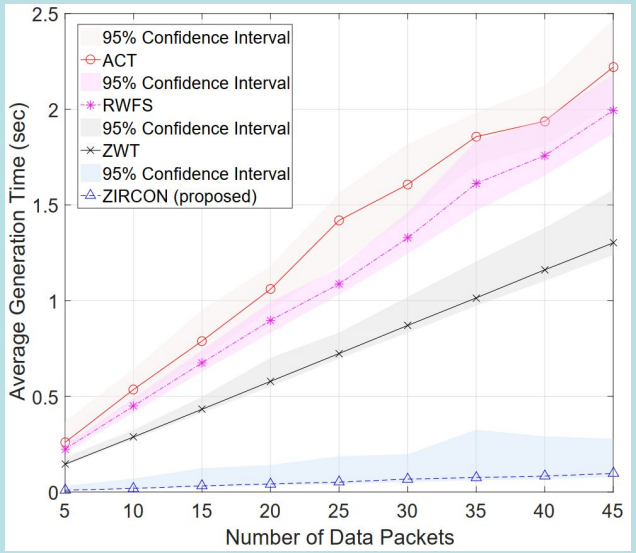
Proposed Approach

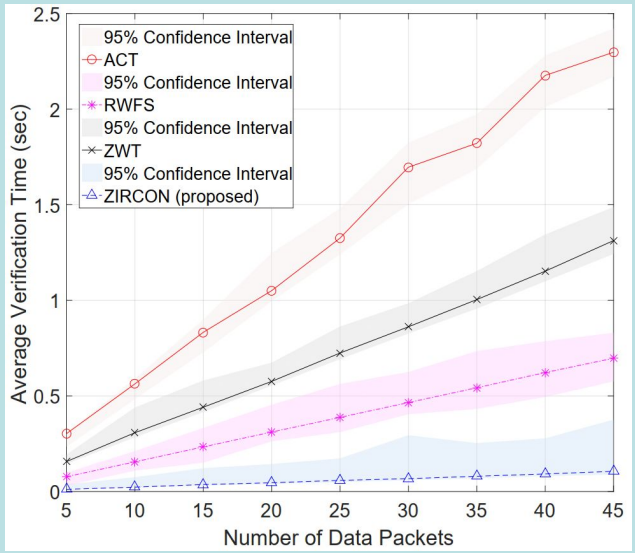
ZIRCON – **Z**ero-watermark**I**ng based data p**R**ovenan**C**e for i**O**t **N**etworks



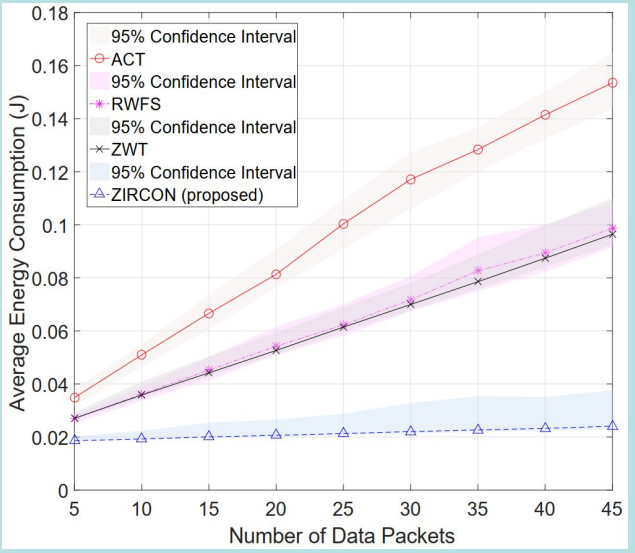
Performance Results

Watermark Generation and Verification Time





Energy Consumption



- **RWFS:** uses homomorphic encryption which requires complex computational operations
- **ACT:** uses asymmetric cryptography and group hashing which creates additional overhead.
- **ZWT:** uses DES for data and watermark encryption.
- **ZIRCON:** uses AES for sub-watermark encryption which is secure, reliable, efficient and fast choice for encryption and decryption.

Thanks for your attention!

Samovar young researchers' day 2023