CPS: Small: Collaborative Research: A Secure Communication Framework with Verifiable Authenticity for Immutable Services in Industrial IoT Systems

Song Han (University of Connecticut); Chen Qian (UC Santa Cruz)

2021 NSF Cyber-Physical Systems Principal Investigators Meeting

Project Overview and Objectives

- IIoT systems are deployed in harsh and complex environments, and have stringent dependability, timing performance, and especially security requirements to optimize production efficiency.
- The objectives of this project are to design: 1) efficient signature schemes to support verifiable authenticity, integrity, and uniformity for intra-plant communications and 2) hierarchical and scalable blockchain protocols to support inter-plant immutable services.

Secure Communication Framework

Thrust 1: Verifiable and Efficient Management of Real-time Sensing Data for IIoT

- Holistic Design of the VERID Data Management System
- Authenticity and Integrity for Uniform and Prioritized Sampling
- Real-time and Online Sensing Data Verification
- Privacy protection when devices communicate with cloud servers

Thrust 2: Efficient IoT Authentication and Data Protection

- Efficient on-device IoT certificate verification and revocation checking
- Low-cost packet header protection for IoT devices to defend against passive adversaries
- Hybrid Verification Mechanism with Gateway Protection

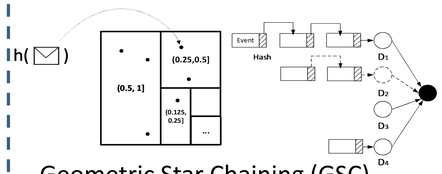
Thrust 3: Immutable Cross-plant Data Ledger

- Hierarchical Blockchain Structure Design
- Cloud-based Hierarchical Storage Design
- Scalable BFT Consensus Design with Detection Mechanism

Thrust 4: IIoT-enabled Advanced manufacturing System Testbed

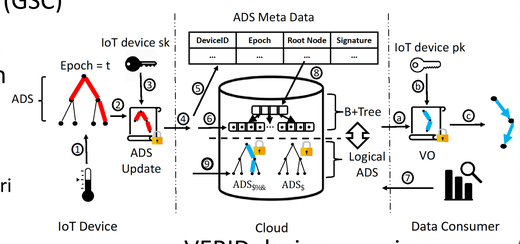
- Implementation of the Security Protocols on 6TiSCH Testbed
- Deployment of the Testbed in P&W Additive Manufacturing Center
- Integration with a Cloud-based Real-Time Data Analytics Platform

Thrust 1 Verifying Sensing Data



Geometric Star Chaining (GSC)

- GSC is a signature scheme to verify data authenticity and data integrity
  - Computation efficient.
  - Support partial data retrieval.
  - Constant space cost.
  - Sampling **uniformity**.
- VERID data management system is a holistic design for IoT.
  - Computation and memory efficient.
  - Support **verifiable** range queri and aggregate queries.



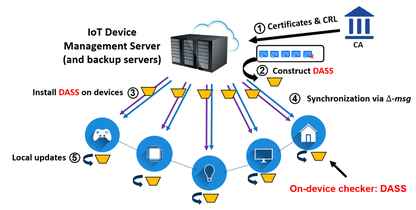
VERID design overview

Thrust 2 Efficient IoT Authentication and Data Protection

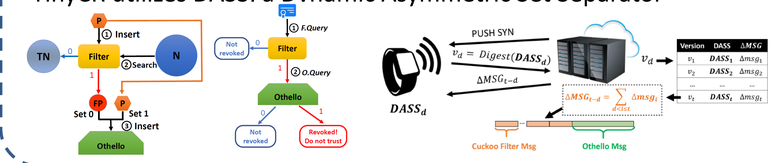
- TinyCR: On-device IoT Certificate Revocation Checking with Small Memory and Low Latency.

TinyCR is a protocol for IoT CR checking with the following features:

- 100% accuracy
- Query efficiency: < 1 us/query
- Small memory: 1.7 MB for 100M certs
- Low synchronization latency: incremental update

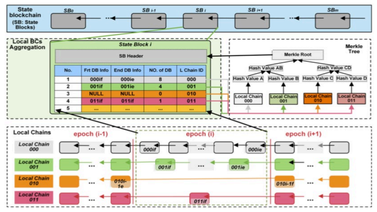


- TinyCR utilizes DASS. a Dynamic Asymmetric Set Separator

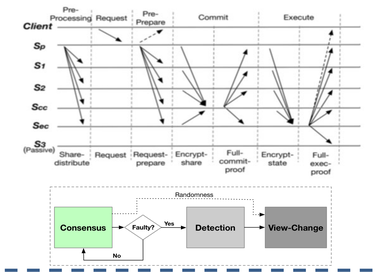


Thrust 3 Immutable Distributed Ledger

- SMChain: two-layer blockchain design for inter-plant services
  - Local chain and state chain
  - Each plant constructs its local chain
  - Hierarchical storage with the majority of chain on the cloud



- DetBFT: Efficient BFT consensus protocol with a detection phase
  - Reduces communication complexity via threshold crypto-primitives
  - Adds detection phase to BFT protocol



Thrust 4 IIoT Testbed Design and Deployment

- The developed solutions will be implemented on a 120-node 6TiSCH industrial wireless testbed and deployed in P&W Additive Manufacturing Innovation Center.

Scientific Impacts

- Ensuring authenticity, integrity, and uniformity of sensing data in IIoT networks by designing novel signature schemes.
- Enabling PKC-based fast control message authentication by extending the control border of IIoT networks to the cloud/Internet.
- Providing inter-plant immutable services by developing a hierarchical blockchain structure and scalable lightweight consensus protocol.
- Developing a unique IIoT-enabled advanced manufacturing system testbed to cover the whole sensing-analysis-control-actuation life cycle of IIoT systems.

Broader Impacts

- Provide unique opportunities for students to apply learnt cybersecurity technologies into IIoT systems design and development.
- Have the potential to completely reshape the security architecture in future IIoT network protocol design, and vastly advance the adoption of IIoT network infrastructure.
- The collaboration of the research team will lead to a publicly available IIoT-enabled advanced manufacturing testbed, effective dissemination of research results among practitioners, and initiation of technology transfer.

UCONN UNIVERSITY OF CONNECTICUT

UNIVERSITY OF CALIFORNIA SANTA CRUZ

Industry Collaborator: EMERSON Process Management

UConn PI: Song Han (song.han@uconn.edu)

UCSC PI: Chen Qian (cqian12@ucsc.edu)

Award ID#: 1932480 and 1932447