Secure Asset Tracking in Manufacturing through Employing IOTA Distributed Ledger Technology

Svoronos Leivadaros, George Kornaros and Marcello Coppola

Intelligent Systems & Computer Architecture Lab (ISCA-Lab)
Hellenic Mediterranean University, GR

May 10th, 2021
Agenda

- Industrial IoT revolution for predictive maintenance, asset analytics, etc.
- Challenges in convergence of IIoT, Cloud, LPWAN, DLT technologies
- IOTA DLT enabling trusted IoT – cloud automation
- STM32M7-based implementation and evaluation
- Conclusions
## IoT Key Factor in Smart Industry

<table>
<thead>
<tr>
<th>Layer</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Layer</strong></td>
<td>Optimization of Manufacturing Load, Spare Part Inventory Management, Maintenance Scheduling</td>
</tr>
<tr>
<td><strong>Cognition Layer</strong></td>
<td>Performance Evaluation, Risk Assessment</td>
</tr>
<tr>
<td><strong>Cyber Layer</strong></td>
<td>Knowledge Discovery, Time Machine Snapshot Collection, Degradation Progress Mode Feedback, Dynamic Fleet-sourced Prognostics</td>
</tr>
<tr>
<td><strong>Conversion Layer</strong></td>
<td>Individual Information, Smart Analytics</td>
</tr>
<tr>
<td><strong>Perception - Connection Layer</strong></td>
<td>Factory A Sensors Network, Factory B Data Acquisition</td>
</tr>
</tbody>
</table>
IoT End-to-End Organization
**IIoT and Blockchain Convergence**

Blockchain features
- Decentralization (identity management, access control)
- Tamper-proof data (immutable, traceable, signed-timestamps)
- Information security (confidentiality, integrity)
- Privacy (disassociate public keys hashes from user IDs)

Challenges:
- relative volatility of blockchain implementations involving protocol changes vs long-lived IIoT devices
- scale to the transaction rates that can be generated by large numbers of connected devices

IoT ↔ Blockchain: trusted multi-party processes to bridge physical world things to industry process computing environments
Use Cases

- Automation Monitoring and Maintenance in Manufacturing
  - Access and manage IoT devices/data in an industrial environment (IIoT)
    - Trusted monitoring of IoT device data (e.g., sensor values) at the ledger
  - Management of IIoT device lifecycle by using firmware updates
    - Record update information metadata at the ledger that can be used to manage the firmware update procedure of IoT devices
Industrial Monitoring

LoRaWAN

Cloud
Influx DB

Chronograph Visualization
FOTA Updating

- **Director Server**
  - Send FW metadata
  - Receive FW metadata

- **OEM Gateway**
  - Git push

- **GIT Server**
  - Git pull
  - Git push

- **Gateway**
  - FW IMG
  - FW Metadata

- **Island Gateway**
  - EndPoints 1 (ECU1)
  - EndPoints N (ECU N)

- **Block Chain**
  - FW Metadata

- **Database**

---

ISCALab/HMU, CCGRID-SIoTEC2021, May 10-13, 2021, Melbourne
Tfusting IoT LoRaWAN Devices

- Devices
  - Dx
  - Dx
  - Dx
  - Dx
- Gateways
- Network Servers
- Application Servers
- Long-range Sub-GHz LoRa®
- 3G / 4G / Ethernet (IP)
- Ethernet (IP)
- All transactions bundled in a Directed Acyclic Graph (DAG)
- Each new transaction must approve two previous transactions
- PoW for preventing spam
- Flexibility in “confirming” transactions
- No transaction fees
- Support for offline transactions (partitioning)
Light Node Transaction Flow

1. Boot Device
2. Initialize Peripherals
3. Read CPU Temperature and device UUID
4. Generate 64-bit random nonce using TRNG and append it to temperature and UUID
5. Calculate SHA256 Digest of message
6. Generate Random Initialization vector using TRNG peripheral and encrypt with AES256-CBC
7. Create Transaction. Generate Address and set message and tag field values
8. Request 2 transactions to approve
9. Return hash of 2 transactions to approve
10. Create a bundle with a single zero-value transaction
11. Send attachToTangle API call to do PoW on Full Node Provider
12. Return valid nonce
13. Compute transaction hash
14. Send broadcastTransaction API call to broadcast transaction to Tangle

IOTA Light Node
STM32F746G-Disco Board

IOTA Full Node Provider
Linux PC, i7 3770K CPU

Network Time Protocol Server

5. Request timestamp
6. Return timestamp value
7. Compute valid nonce for received Transaction

12-May-21
ISCALab/HMU, CCGRID-SIoTEC2021, May 10-13, 2021, Melbourne
Latency Breakdown

IOTA Light Node Application with MAC running on STM32F746G-Disco - Remote Proof of Work with MWM = 14

- Other Functions
- Broadcast
- Curl Hash
- PoW
- MakeBundle
- TSA
- All 2-ary/3-ary Conversions
- gen_address
- MAC

Execution time in milliseconds

IOTA Light Node Application with MAC running on STM32F746G-Disco - Remote Proof of Work with MWM = 9

- Other Functions
- Broadcast
- Curl Hash
- PoW
- MakeBundle
- TSA
- All 2-ary/3-ary Conversions
- gen_address
- MAC

Execution time in milliseconds

IOTA Light Node Application with MAC running on STM32F746G-Disco - Local Proof of Work with MWM = 14

- Other Functions
- Broadcast
- Curl Hash
- PoW
- MakeBundle
- TSA
- All 2-ary/3-ary Conversions
- gen_address
- MAC

Execution time in milliseconds

IOTA Light Node Application with MAC running on STM32F746G-Disco - Local Proof of Work with MWM = 9

- Other Functions
- Broadcast
- Curl Hash
- PoW
- MakeBundle
- TSA
- All 2-ary/3-ary Conversions
- gen_address
- MAC

Execution time in milliseconds
Scalability Evaluation on Docker-based IOTA Nodes

- Physical Host 1
  - Light Node
  - Full Node 1

- Physical Host 2
  - Light Node
  - Full Node 2

- Physical Host 3
  - Light Node
  - Full Node 3

- Physical Host 4
  - Light Node
  - Full Node 4

- Physical Host 5
  - Light Node
  - Light Node
  - Light Node
  - Light Node

- Coordinator

- Physical Host 1
  - Physical Host 2
  - Physical Host 3
  - Physical Host 4

- Light Node and Full Node Provider Link

- Neighboring Full Nodes Link

- Mean TPS

- 1 LN
- 2 LN
- 4 LNs
- 8 LNs

- Full Node 1
- Full Node 2
- Full Node 3
- Full Node 4

- Physical Host 5

- IoT Device/Sensor
- IoT Device/Sensor
- IoT Device/Sensor

- Sensor Data

- DLT Light Node

ISCALab/HMU, CCGRID-SIoTEC2021, May 10-13, 2021, Melbourne
Summary

- STM-based IoT devices authentication through decentralized integrity assurance framework enabled by IOTA
- Investigation on performance and scalability when partitioning Full Node Ledgers

Promising days, with potential for DLT technologies for next generation decentralized industrial networks and applications is clear
Thank you for your attention!

EU-H2020 AVANGARD

Intelligent Systems and Computer Architecture Lab
https://isca.hmu.gr

George Kornaros
[kornaros@hmu.gr]