Law, Science and Technology
MSCA ITN EJD n. 814177

RIoE
Rights of Internet of Everything

Are Distributed Ledger Technologies Ready for Intelligent Transportation Systems?

Mirko Zichichi[1,2], Stefano Ferretti[3], Gabriele D'Angelo[2]

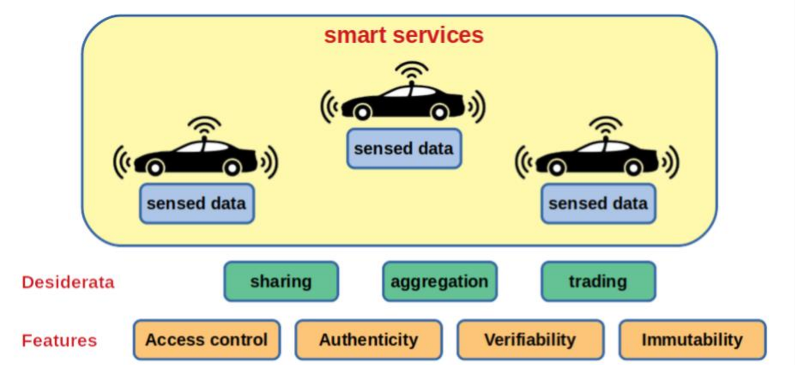
[1]Universidad Politécnica de Madrid
[2]University of Bologna
[3]University of Urbino "Carlo Bo"

Overview

1. Introduction
2. Architecture Design
3. Experimental Evaluation
4. Conclusion

Introduction

Intelligent Transportation Systems Crowd-sensed Data



Sensors → crowd-sensed data → next generation Internet **services**

Intelligent Transportation Systems (ITS) → services built on vehicles data

Trust the data

Distributed Ledger Technologies

Distributed Ledger Technologies (DLTs) are used in scenarios where:

1. **multiple actors** that concur in handling some shared data
2. there is **no complete trust** among these actors
3. and often they **compete to the access/ownership** of such data.

This is a typical scenario of a smart transportation service that exploit data sensed from multiple sources (vehicles).

Can DLTs be efficiently employed in ITS scenarios?

DLTs Limitations

The main **limitations** that are commonly attributed to DLTs (e.g. Bitcoin, Ethereum) are:

- lack of **scalability** and **sustainability**
- **transaction verification rate**

Some DLTs have been designed with the intent to support the **Internet of Things (IoT)** and to solve some of those limitations.

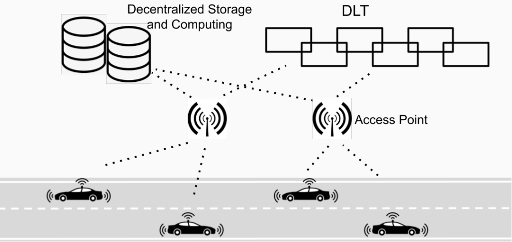
Our contribution

- propose a system architecture that exploits **DLTs for the support of ITS**
- present an **experimental evaluation** on DLTs

1. use of real data traces to emulate a **smart city traffic application**
2. performance of the **IOTA** DLT real-time scenarios

Architecture Design

The Use of DLTs for ITS



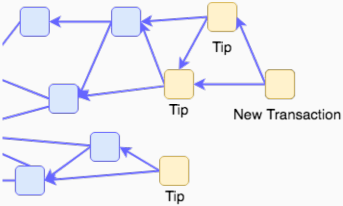
- **Vehicles equipped with sensors** that can generate data of some interest
- Sensed data can be **transmitted through a network to a DLT**
- Data can be stored and manipulated by a **(distributed) storage and computing platform** $\rightarrow$ and then **referenced in a DLT**

Communication Between Vehicles and DLT Nodes

- **Vehicle on board computing unit** (or user **smartphone**) is able to issue requests to a dedicated **DLT node**
- After authentication, these requests are converted to **DLT transactions (TXs)**
- System Requirements:
  1. TXs must be registered in the DLT in a **fast way**
  2. a good level of **scalability** must be guaranteed
  3. the DLT should offer **low fees** (or no costs at all)
  4. TXs must be easily treated as a **data-stream**, i.e. easy to retrieve.

IOTA DLT

IOTA is designed to address those requirements and with the aim to support **IoT scenarios**.



- The **IOTA** ledger is structured as a Direct Acyclical Graph (DAG) $\rightarrow$ the **Tangle**
- Vertices $\rightarrow$ **TXs** , edges $\rightarrow$ **approvals**

To issue a new TX it is necessary to $\rightarrow$ **approve two previous tips** and **compute PoW**:

1. **Tips selection** - selecting from the Tangle two random **Tip TXs**, i.e. that do not have a successor yet
2. **Proof of Work (PoW)** - the purpose of PoW is to deter denial of service attacks and other service abuses, since IOTA is **feeless**

IOTA MAM Channels

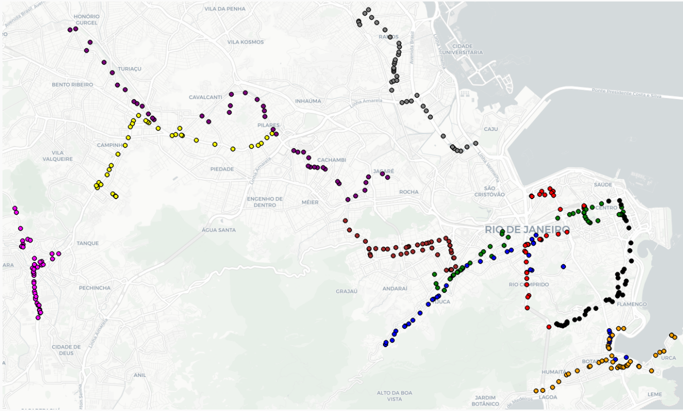
- **Masked Authenticated Messaging (MAM)** is a second layer data communication protocol
- It is used to emit and access an **encrypted data stream** over the Tangle
- It takes the form of a **linked list** of transactions, chronologically ordered

- Only the **owner** can publish encrypted messages
- Whoever holds the **MAM channel encryption key** can decode the messages in the stream
- Access to new messages may be **revoked** simply by using a new encryption key

Experimental Evaluation

ITS Real Mobility Traces

Dataset of **real mobility traces** of buses in Rio de Janeiro (Brasil)



We simulated up to **240 buses** that issue (geolocation) data to MAM Channels

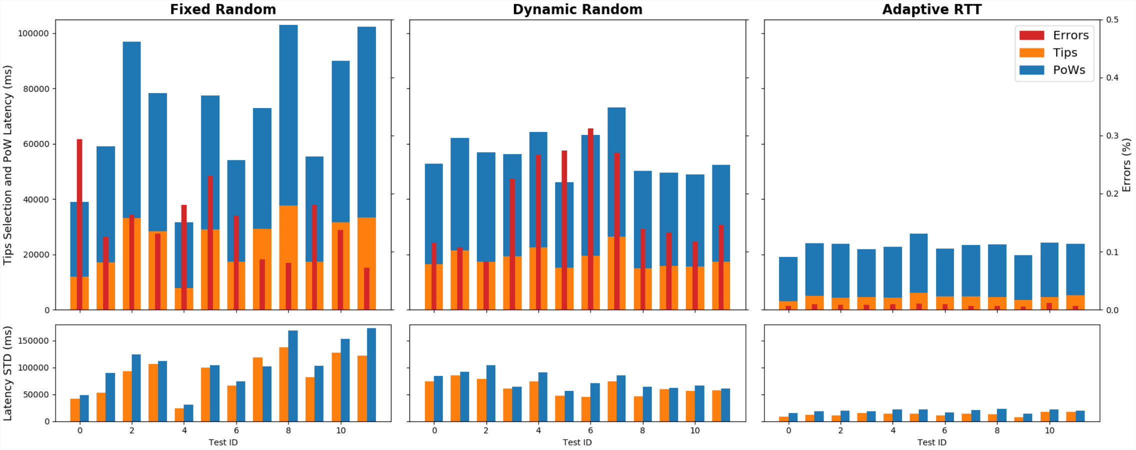
Test configuration

- **one hour** of trace data for each bus.
- 1 bus $\rightarrow$ generates $\sim$**45 message/hour** (1 message every 80 sec), a reasonable time interval to sense data in an urban scenario.
- we recorded the outcome of each message published into the MAM channel:
  1. **successful** or **unsuccessful** (due to errors or timeouts)
  2. **latency** between the transmission of the message and its insertion into the channel (i.e. the TX **Tips selection** and **PoW**)
- we queried **60 public IOTA full nodes**

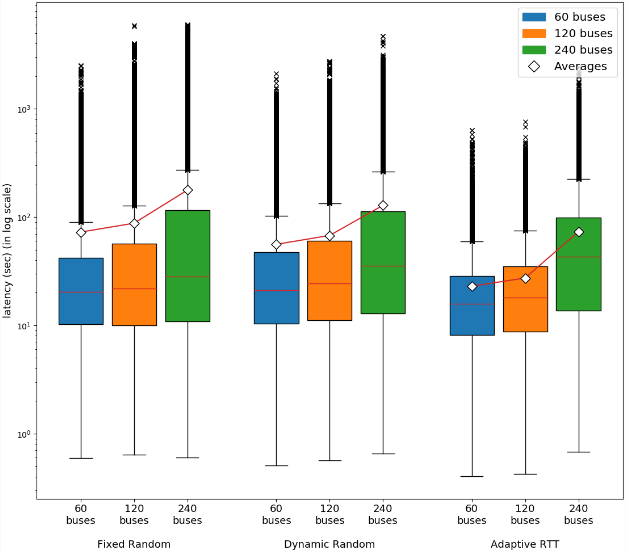
Selecting IOTA nodes for Requests

1. **Fixed Random**: Each bus is assigned to a **random public IOTA full node** and keeps it for **the whole duration** of the test.
2. **Dynamic Random**: A random node from the pool of random full nodes is selected **every time a message has to be published** by a bus.
3. **Adaptive RTT**: Each bus b holds a list of *known_nodes(b)*, ordered through the **experienced Round Trip Time (RTT)** of past interactions.
   - for each b
   - **if** waiting(***curr_assigned(b)***, m^b_{t-1}) **then** **curr_assigned(b)** = first_not_waiting(*known_nodes(b)*);
   - publish(***curr_assigned(b)***, m^b_t);
   - if each node $\in$ *known_nodes*(b) is in the process of publishing a b's previous message, a new full node is picked randomly from the list of public nodes

60 bus tests: average latencies, standard deviation and errors



Boxplots for tests with 60, 120, 240 buses (y-axis in log-scale)



Results Table

# buses	Heuristic	Avg Latency	Conf. Int. (95%)	Errors
60	Fixed Random	72.68 sec	[70.43, 74.94] sec	15.37%
	Dynamic Random	56.0 sec	[54.51, 57.5] sec	18.26%
	Adaptive RTT	**22.99 sec**	[22.69, 23.29] sec	**0.81%**
120	Fixed Random	87.75 sec	[85.38, 90.12] sec	29.49%
	Dynamic Random	67.6 sec	[66.29, 68.9] sec	18.99%
	Adaptive RTT	27.35 sec	[27.11, 27.58] sec	1.1%
240	Fixed Random	**177.62 sec**	[174.25, 181.0] sec	**42.81%**
	Dynamic Random	128.2 sec	[126.28, 130.12] sec	**44.85%**
	Adaptive RTT	73.26 sec	[72.68, 73.85] sec	7.55%

Results Discussion

- through a **proper selection** of full nodes it is possible to achieve **reliable ledger updates** (low errors)
- however, the **measured latencies are relevant**
- a possible solution =
  edge computing system model → PoW executed by a gateway + Tip selection accomplished by a full node (complete copy of the Tangle)

Conclusion

Conclusion

- Architectural solution **resorting to DLTs to support ITS**, allowing to safely and securely store sensed data
- **Experimental evaluation** on a DLT that presents features that are needed for ITS scenarios $\rightarrow$ IOTA
- Measured **latencies resulted higher than 20 sec** $\rightarrow$ high for real-time applications, reasonable for less time demanding services
- Could be reduced by a **targeted selection** or by improving ITS and DLT **infrastructures**.
- **Future Work**
    - Further experiments with IOTA **delegating PoW to gateways**
    - Employing new DLTs solutions, e.g. **sharding**