µTesla-Based Authentication for Reliable and Secure Broadcast Communications in IoD Using Blockchain

J. C. P. García, A. Benslimane, A. Braeken and Z. Su

IEEE INTERNET OF THINGS JOURNAL, VOL. 10, NO. 20, 15 OCTOBER 2023

2025.02.05.

Summarized by, Sangwi Kang | swkang@mmlab.snu.ac.kr

Outline

- Introduction
- Drones and Broadcast Communication
- Secure Broadcast Communication
- µTesla-based Authentication Using Blockchain
- Security Analysis
- Performance Evaluation
- Conclusion

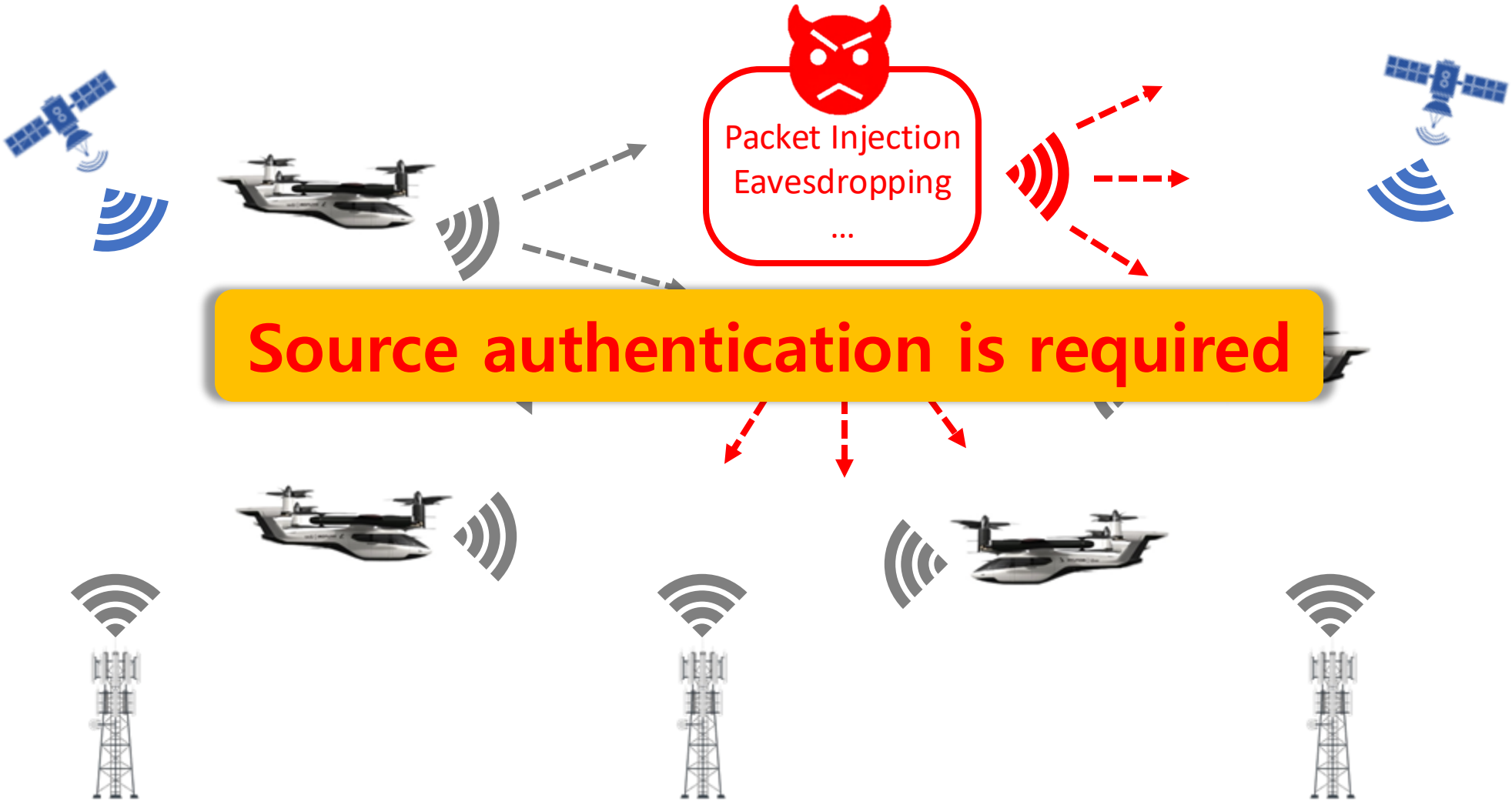
Introduction

Internet of Drones

- Most communications in IoD networks are conducted over a public channel in a broadcast fashion
- Due to the **high mobility of drones**, there is the potential for **packet loss**
- **Re-authentication** issues caused by **handover problems** are also a challenge
- The authentication protocol for the drones must consider the **handover** and packet loss
- There were some suggestions before, but they **do not** take into account **packet loss** and **handover**

- In this paper, the authors propose **a blockchain-based authentication** scheme inspired by **light-weight broadcast authentication protocol**

Drones and Broadcast Communication



Secure Broadcast Communication

> µTesla

- **The micro version** of the Tesla

✓ Designed for resource-constrained networks

✓ **Computationally expensive digital signatures have been removed**

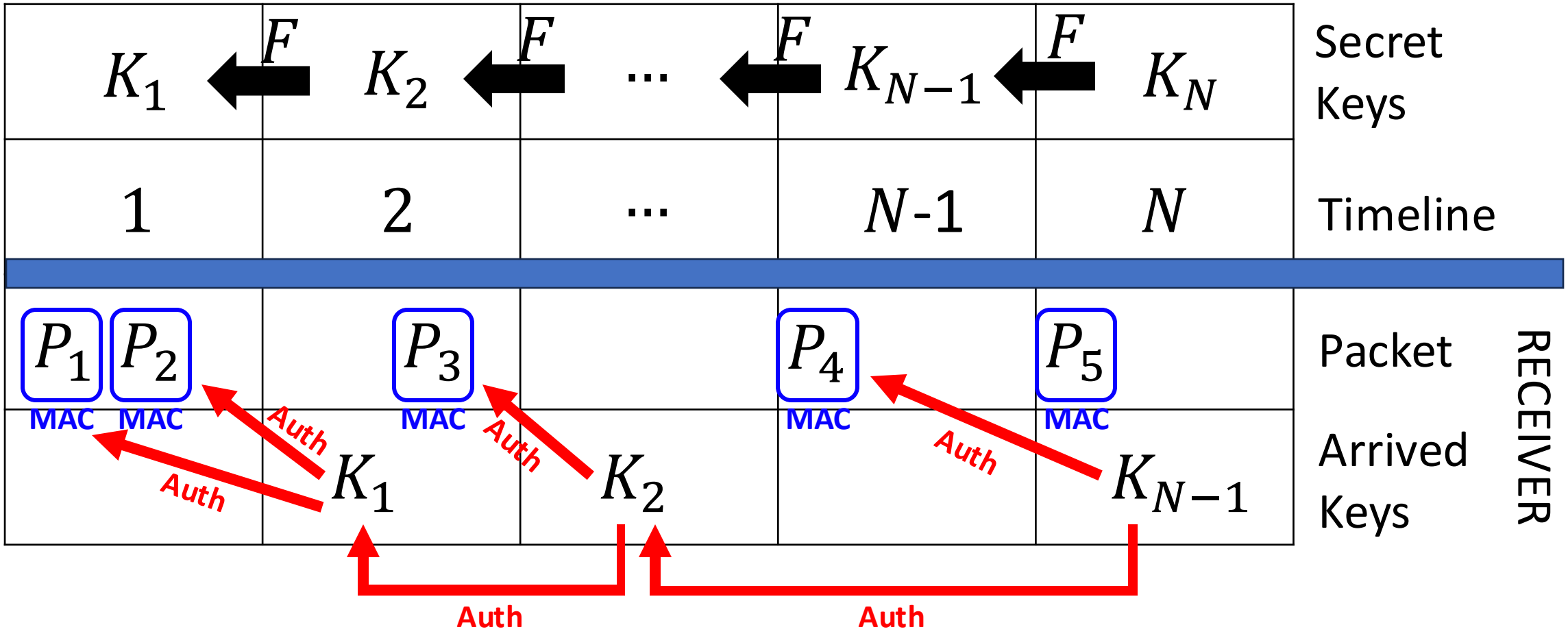
✓ Delivers the initial key in the key chain **by unicast** to all receivers, reducing the size of transmitted packets compared to the Tesla

➢ The unicast can cause network overhead

➢ The number of keys is finite, so a mechanism for refreshing keys is required

Secure Broadcast Communication

> µTesla



µTesla-based Authentication Using Blockchain

> Overview

- µTesla achieves **light-weight computation** and can respond to **packet loss issue**

➢ **Centralization risks**

  - Single point of failure, scalability

- **Advantages of blockchain**
  - Publicly verifiable, tamper-proof, and distributed
  - Deals with re-authentication issues

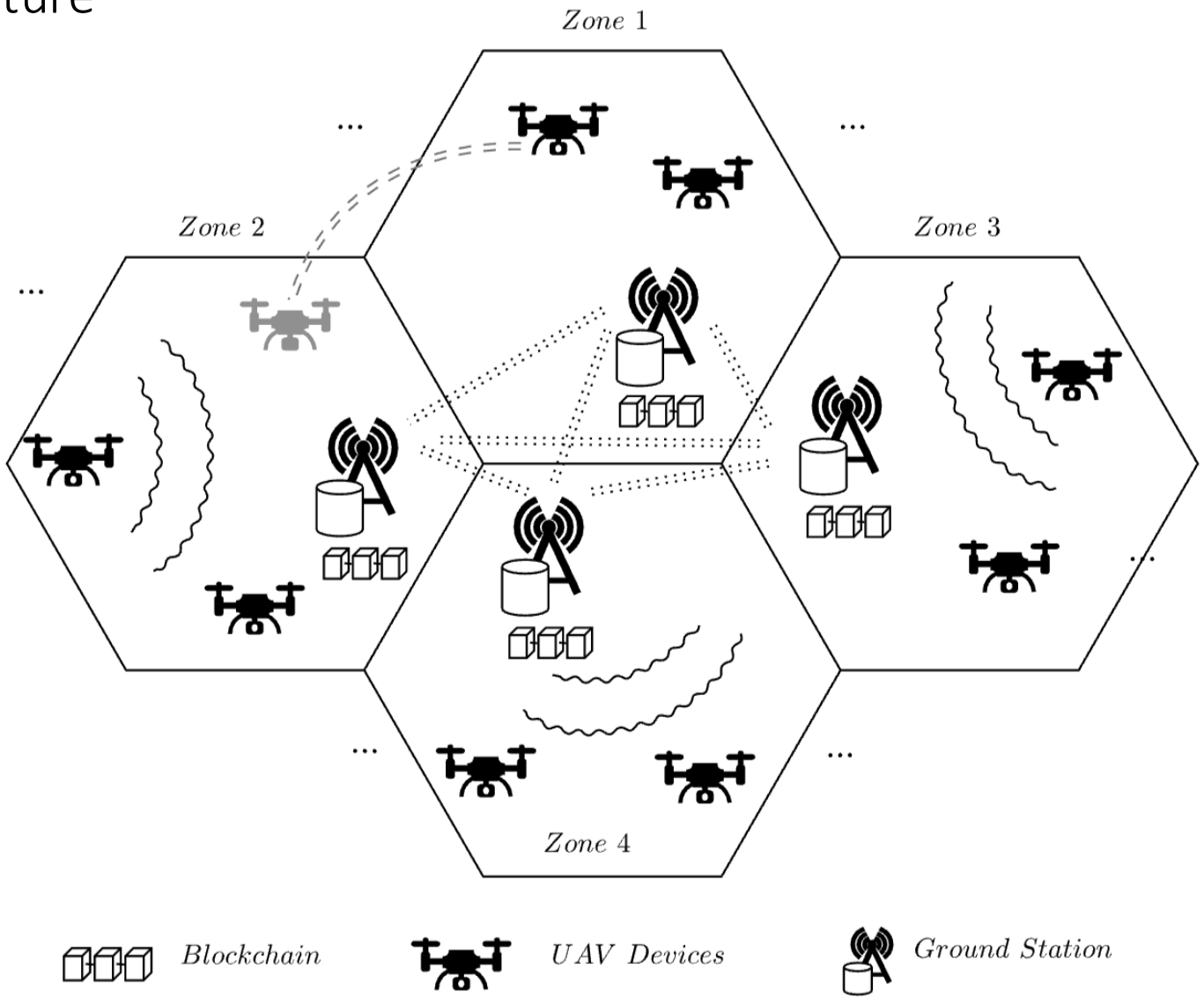
✓ Authentication protocol that combines **µTesla** and **blockchain**

Light-weight
Packet Loss Tolerant

Distributed
Tamper-proof
Re-authenticapable

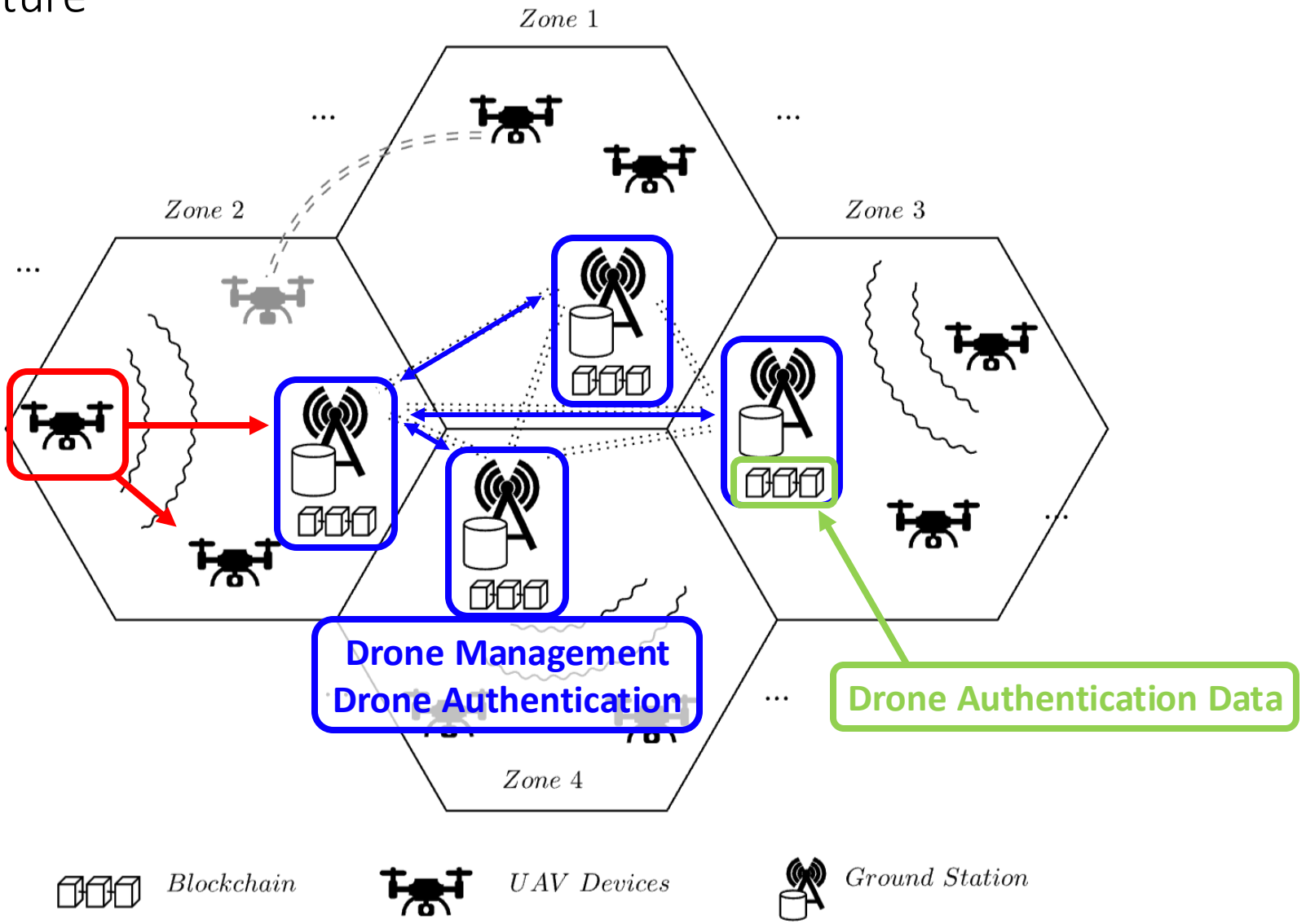
μTesla-based Authentication Using Blockchain

> Network Structure



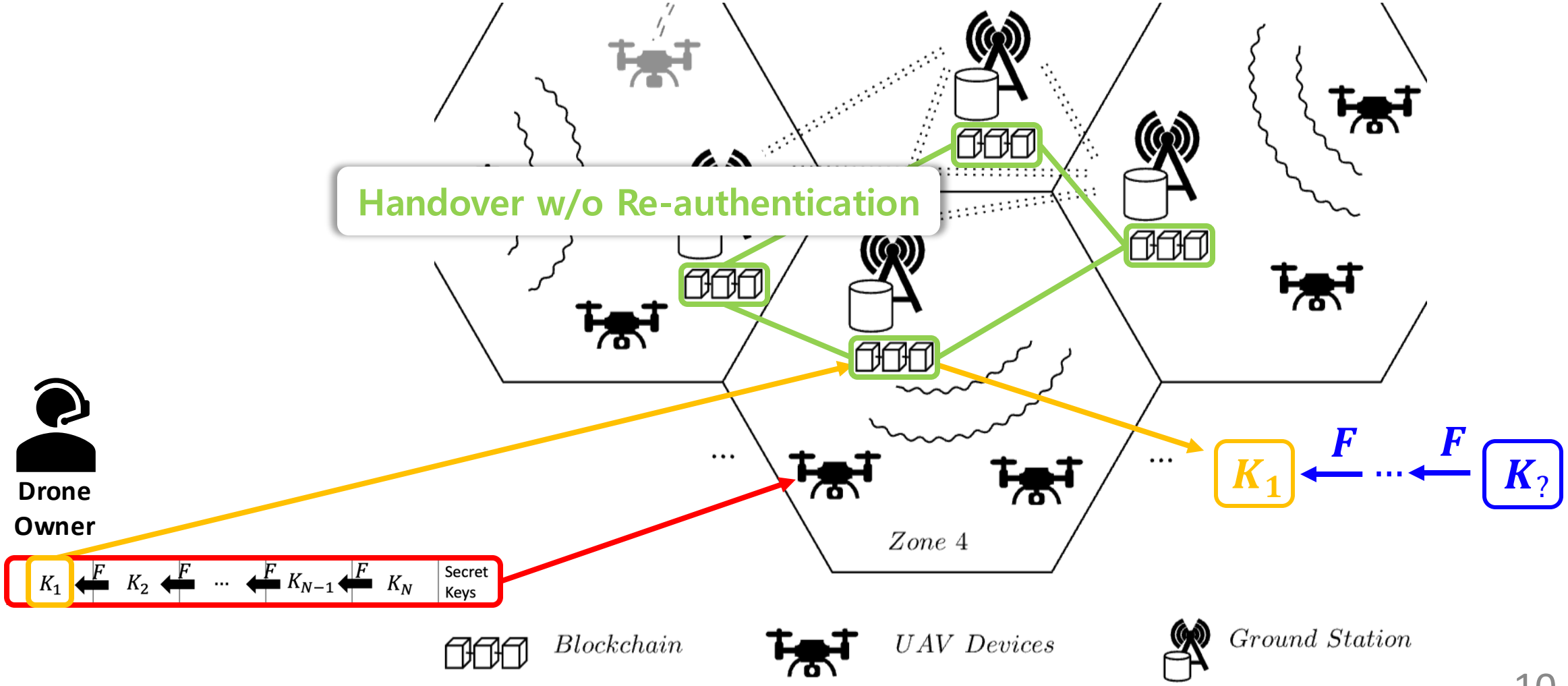
μTesla-based Authentication Using Blockchain

> Network Structure



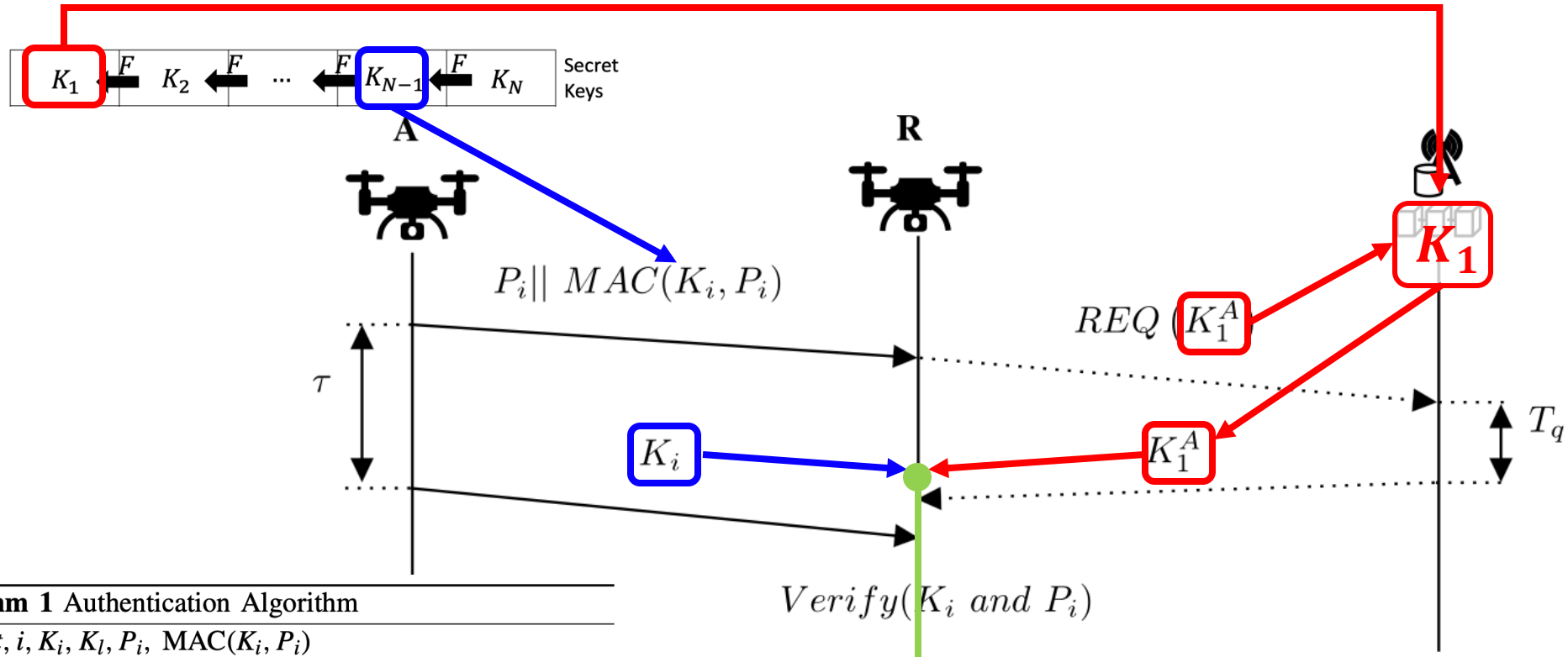
μTesla-based Authentication Using Blockchain

> Drone Setup and Registration



μTesla-based Authentication Using Blockchain

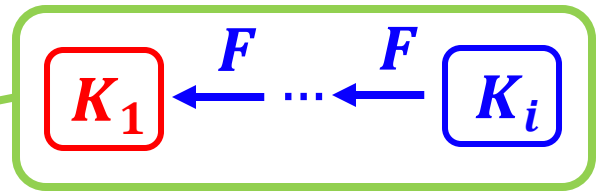
> Broadcast Authentication Flow



Algorithm 1 Authentication Algorithm

Input: $t, i, K_i, K_l, P_i,$ MAC(K_i, P_i)
Output: **bool** A

1: **if:** $t < i * \tau$ % *Check security condition*
2: Verify MAC(K_i, P_i)
3: **if:** $K_l == F^{(i-l)}(K_i)$ % *Key verification*
4: $A = True$ % *Successfully authentication*
5: Store K_i % $K_l = K_i$
6: **else:** $A = False$
7: **return** A



Security Analysis

- Assumptions
  - The private blockchain is jointly maintained by the authorized GS(Ground Station)s
  - Attackers can impersonate drones or GSs
  - Dolev-Yao (DY) Model : Shows what happen when communication occurs on insecure channel

- Eavesdropping Attack
- Drone Identity Impersonation

Time Delayed Key Disclosure
One-way Hash Function

- Drone Identity Forgery
- Drone Cloning Attack
- Ephemeral Secret Leakage Attack

Hash Key Chain

- MITM (Man-in-the-Middle)
- **DoS (Denial of Services) → Buffer flooding attacks can occur**

Performance Evaluation

> Experiment Setting

- Drone
  - Raspberry Pi 3B Quad-core Cortex-A72 @1.5GHz 8G 64G ROM
  - Python *pycrypto* library
  - AES128 for symmetric encryption, SHA256 for hash function

- Blockchain
  - Hyperledger Fabric v2.2 / Docker v20.10.6
  - PBFT (Practical Byzantine Fault Tolerance)
  - Intel Core i7-7700 CPU 3.60GHz x 8 16G RAM

Performance Evaluation

> Computation and Communication Cost

Schemes	Time Complexity	$Time$(ms)	Comm.($bits$)
[6]	$12T_{hm}$	118.788	1280
[7]	$23T_H + 2T_S$	2.548	2304
[9]	*	12799.200	16912
[12]	$2T_H + 5T_S$	4.927	7168
Ours	$T_H + T_{MAC} + T_S$	1.054	1024

* $14T_H + 14T_m + T_e + 3T_{bp} + 3T_S$

(The average of 1,000 executions of the cryptographic operations)

T_H: Cost of calculating hash

T_{MAC}: Cost of calculating MAC

T_S: Cost of encryption and decryption

Performance Evaluation

> Blockchain Operations Latencies

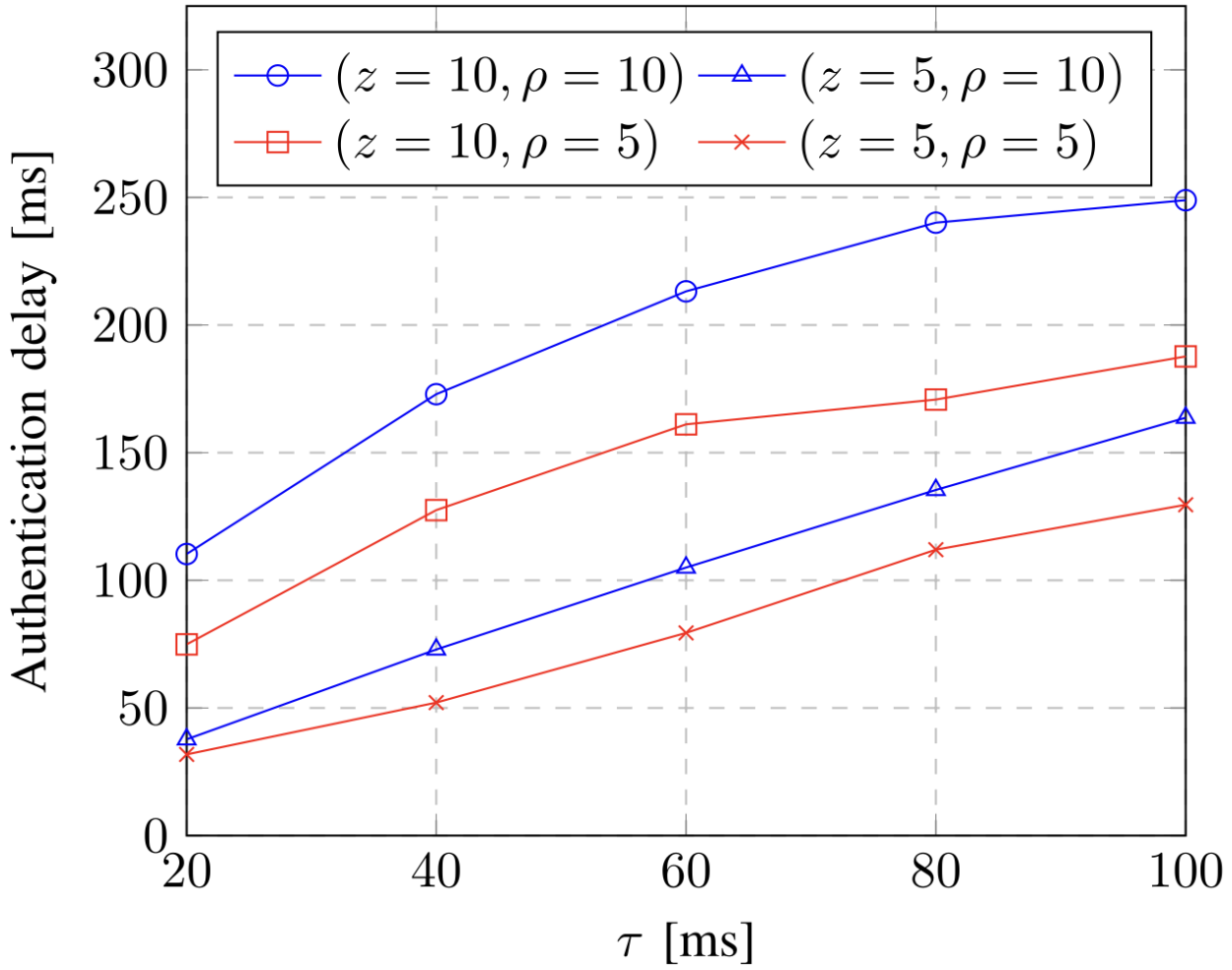
(*sec*)

Operation	Min	Max	Average
Invoke RegisterUAV	1.342	1.721	1.418
Invoke RevokeUAV	1.541	1.726	1.692
Query for White List	0.364	0.621	0.481
Query for UAV	0.127	0.182	0.150

(300 independent invocations to the smart contract i.e., Hyperledger chaincode)
(The average block generation time setting : 2sec level)

Performance Evaluation

> Average Authentication Delay



(Key Disclosure Time)

10 zones x 10 drones

10 zones x 5 drones

5 zones x 10 drones

5 zones x 5 drones

Conclusion

- Secure communication is challenging due to high mobility in a restricted environment.
- By applying blockchain and µTesla, the author proposed a authentication protocol that is **packet loss tolerant, lightweight, tamper-proof, and re-authenticapable.**

- Detailed and realistic parameters for various situations
- PKI concept authentication system w/o PKI
- Loss tolerant for the keys, but not for the message itself
- Unknown whether it can be applied to a real drone environment

Appendix

> Time Cost of Different Cryptographic Operations

Notation	Description	$Time$(ms)
T_{hm}	Hyper-elliptic curve multiplication	9.899
T_H	SHA256 Hash function	0.026
T_S	AES128 encryption and decryption	1.975
T_m	Scalar Multiplication in $\mathbb{G}_1$	0.031
T_e	Exponentiation in $\mathbb{G}_T$	7.682
T_{bp}	Bilinear pairing in $\mathbb{G}_T$	8.128
T_{MAC}	MAC Code	0.053

Appendix

> Simulation Setup

Parameter	Value
Simulation time	30 minutes
Zones (GS)	$[5, 10]$
Drones/Zone (ρ)	$[5, 10]$
Mobility model	Random
Average Block time	2 seconds
Transaction size	64kB
Packet size	512 Bytes
Data Rate (802.11b)	11 MBps