Energy Efficient Decentralized Authentication in Internet of Underwater Things using Blockchain

Abbas Yazdinejad, Ali Dehghantanha (University of Guelph, Canada)
Reza M. Parizi (Kennesaw State University, USA)
Gautam Srivastava (Brandon University, Canada)
Kim-Kwang Raymond Choo (University of Texas at San Antonio, USA)

Decentralized Science Lab (dSL)

https://www.blockchaincyberlab.com/

DECENTRALIZED SCIENCE LAB

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking

Abbas Yazdinejad[a], Reza M. Parizi[b], Ali Dehghantanha[a], Kim-Kwang Raymond Choo[c,*]

[a] Cyber Science Lab, School of Computer Science, University of Guelph, Ontario, Canada
[b] Department of Software Engineering and Game Development, Kennesaw State University, GA 30060, United States
[c] Department of Information Systems and Cyber Security, University of Texas at San Antonio, Texas, United States

Blockchain-enabled Authentication Handover with Efficient Privacy Protection in SDN-based 5G Networks

Abbas Yazdinejad, Reza M. Parizi, *Senior Member, IEEE,* Ali Dehghantanha, *Senior Member, IEEE,* and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

2019 IEEE International Conference on Blockchain (Blockchain)

BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability

Emmanuel Nyaletey
College of Computing and Software Engineering
Kennesaw State University
GA, USA
enyalete@students.kennesaw.edu

Reza M. Parizi
College of Computing and Software Engineering
Kennesaw State University
GA, USA
rparizi1@kennesaw.edu

Qi Zhang
IBM Thomas J. Watson Research
Yorktown Heights NY, USA
q.zhang@ibm.com

Kim-Kwang Raymond Choo
Department of Information Systems and Cyber Security
The University of Texas at San Antonio, TX, USA
raymond.choo@fulbrightmail.org

Internet of Things (IoT)

- Wearable devices (e.g. smart uniforms with motion sensors and monitoring for threat awareness)
- Portable (but not wearable) devices and apps
- Less portable / stationary devices

- Many applications (medical – IoMT, battlefields – IoBT, industry – IIoT, etc.)
- *Security and privacy are two of many ongoing research and operational challenges*

Most (IoT) systems are not designed with security in mind!

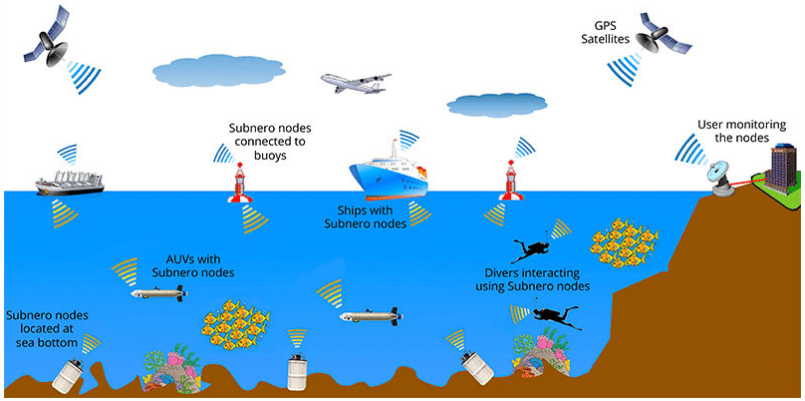
KENNESAW STATE UNIVERSITY

Internet of Underwater Things (IoUT)

- Nearly 70% of the Earth's surface is covered by water and a large proportion of underwater environments are still unknown and have not been explored
- With the increasing growth of IoT and its entry into all areas of urban life including water environments
- IoUT can be defined as a network of smart devices interconnected in an underwater environment

IoUT applications

- It made of unmanned vehicles that scour the sea while communicating with underwater sensors and sending the information to networks atop the surface.
- Environmental monitoring
- Underwater exploration

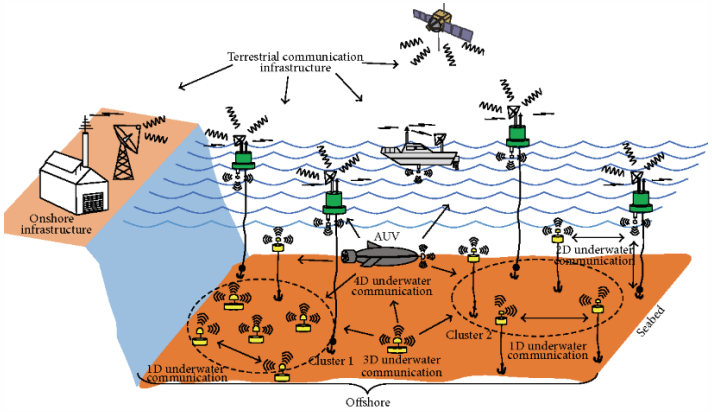


Felemban, Emad, et al. "Underwater sensor network applications: A comprehensive survey." *International Journal of Distributed Sensor Networks* 11.11 (2015): 896832

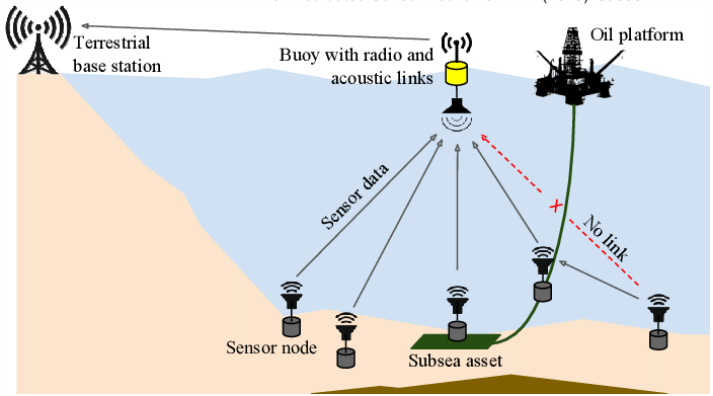
KENNESAW STATE UNIVERSITY

IoUT applications

- Disaster prevention
- Monitoring the health of animals
- Oil and Gas



Felemban, Emad, et al. "Underwater sensor network applications: A comprehensive survey." *International Journal of Distributed Sensor Networks* 11.11 (2015): 896832

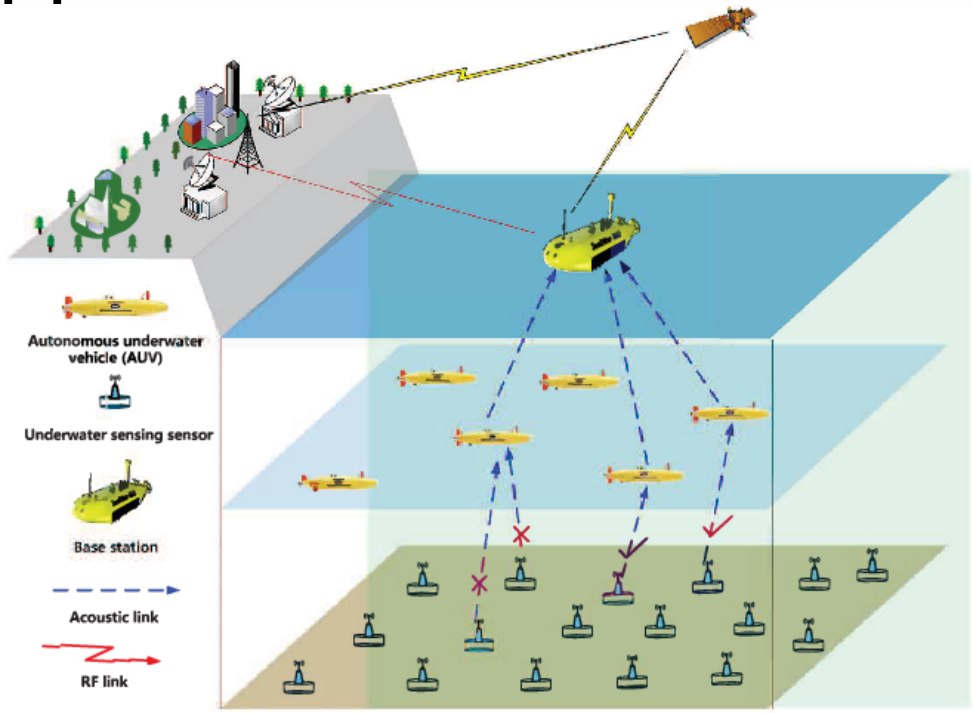


Morozs, Nils. "Unsynchronized dual-hop scheduling for practical data gathering in underwater sensor networks." *2018 Fourth Underwater Communications and Networking Conference (UComms)*. IEEE, 2018.

KENNESAW STATE UNIVERSITY

IoUT applications

- Military



Li, Xinbin, et al. "Relay selection for underwater acoustic sensor networks: A multi-user multi-armed bandit formulation." *IEEE Access* 6 (2018): 7839-7853

KENNESAW STATE UNIVERSITY

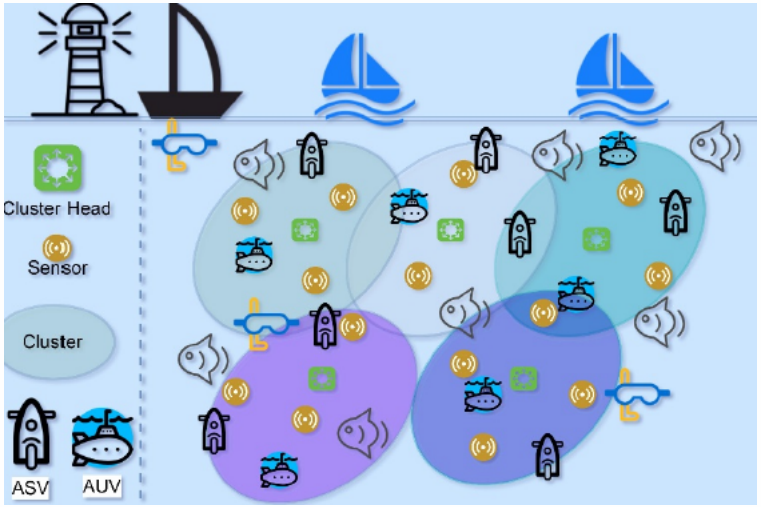
IoUT-specific issues

- Long-term isolated environments…
- Most of the classic authentication methods and centralized security mechanisms require a trusted third-party
- The lack of security in design, inability to defend against attacks, resource constraints…
- The *mobility* of IoUT devices and the frequent switching between clusters, there is a need for frequent authentication to identify and authenticate devices which can require high energy use, unacceptable for IoUT

Proposed approach (Preliminary work)

- Our solution is based on a cluster-based network of objects that uses distributed ledger technology (DLT) to allow secure exchange of data underwater (decentralized authentication).

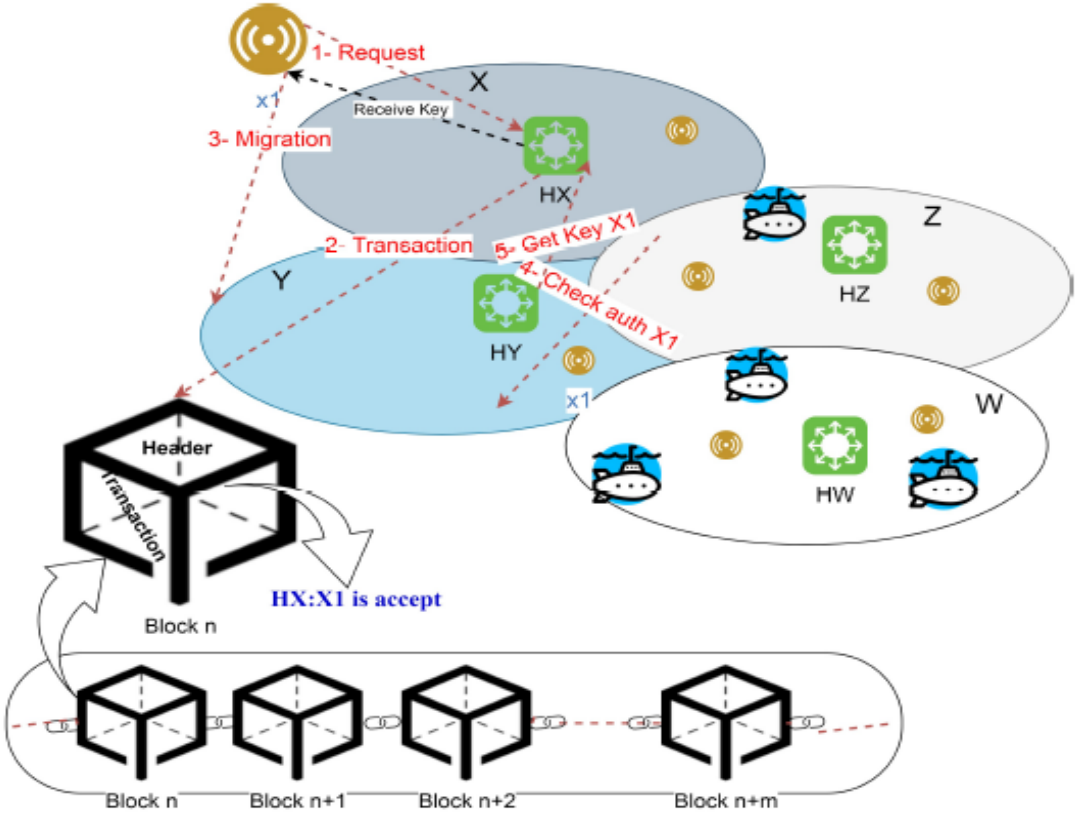
✓ the IoUT devices in each cluster are connected through P2P networks using a blockchain mechanism (removing the need for re-authentication)



Underwater cluster-based network

KENNESAW STATE UNIVERSITY

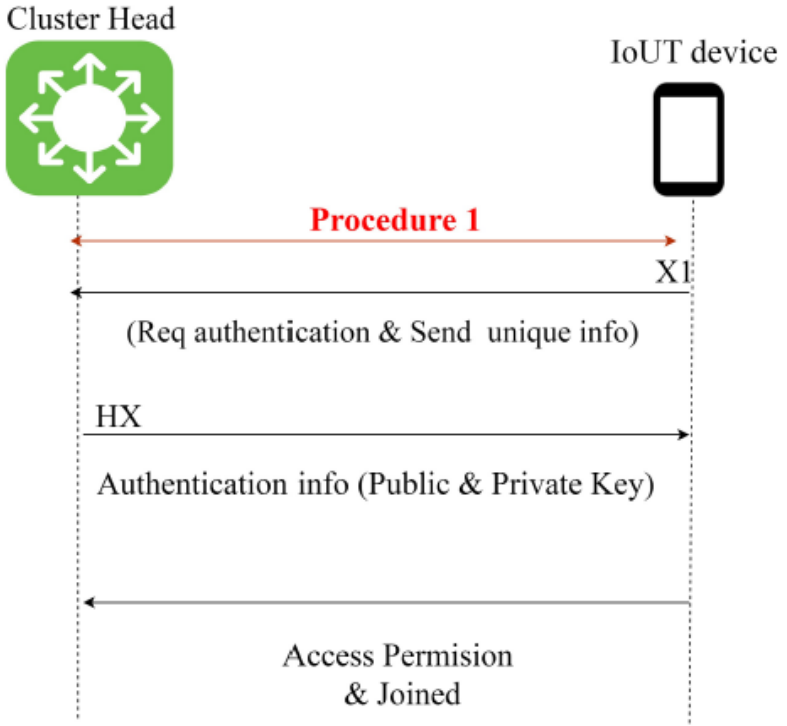
The architecture of the proposed method



KENNESAW STATE UNIVERSITY

Procedure 1 : Joining a Cluster

- X1 is authenticated, and HX sends a transaction to the blockchain.
- X1 is trustful and HX shares a symmetric key for safe transfer with X1.
- These transactions are valid in a new block and are stored by HX.
- When X1 migrates to another cluster, for example, to cluster Y managed by HY, X1 sends a request to HY to join it.



KENNESAW STATE UNIVERSITY

The process of migration and file transfer between IoUT devices

Algorithm 1 Migration mechanism among clusters

```
Call register (X1) // Reg devices in Cluster
Device X1 → Req authentication
HX → Send(authenticationvector (Public & Private/ Key))
Hash_Function (X1)
Node X1: receive (Hash 256)
Call Join_Cluster (X1) // join to cluster
    If (X1== Rang)
      auth = 1
      Calculate (mobility)
    else
      auth = 0
      Calculate (migration)
    While (auth = 0 ) do{
      if (Mobility = 1 or migration = 1)
        if (authenticate)) // in cluster
          HX: Message (X1)
          Update(cluster_info)
          Migrate(X1, current, Target)
      else
          Hx: Message (Blockchain)// send to BC Update X1
      }
While (migrate or mobility != 0 ){
    New_cluster_head = Received (data_X1)
    New_cluster_head = Decrypt (dataCreate header)
      }
end
```

Algorithm 2 Transfer files in cluster

```
Device X1 Announce to X2// User X1 wants to send information to User X2
    If (user X1== authentic in cluster && trust)
        HX (Check traffic cells)
        X1 calculate (optimize (path))
        X1 Encrypt (send data (dK)) // encrypt with Private key
        X1 = Send (WK)
        X2 = monitor_trust-data_ (X1)
    else
      Add to block ()
  X2= Received (data)
  X2 = Decrypt (data) // using private key and re-organize data
end
```

KENNESAW STATE UNIVERSITY

Preliminary Results

- Using the NS-2 V2:35 simulation
  - Average energy consumption
  - Packet delivery rate
  - End-to-end delay
  - Authentication attacks

Simulation Parameters	Values
Simulator	NS-2.35
Type of channel	Wireless channel
Radio range of a node	Random
Propagation model	Propagation/Two ray channel
MAC protocol	Mac/802.11
Mobility model	Random waypoint model
Nodes speed	3 m/s
Number of IoUT Devices (sensor)	200 - 500
Link type of queue	Queue/Drop Tail
Number of Cluster	10
Traffic Type	Constant Bit Rate (CBR)
Type of Antenna	Antenna/Omni Antenna
Simulation Time (Second)	800
Evaluation parameters	End to End delay, delivery ratio, Energy consumption
Number of Simulation runs/scenario	30
Area	2500 m * 2500 m
Packet size	512 Byte
Length of packets (Cluster to BC)	32 Byte
Previous hash	16 Byte
Transaction counter	9 Byte
Block Header|Block Size	80|8 Byte

KENNESAW STATE UNIVERSITY

- The proposed method was compared with a classic authentication method as given in through simulation.

✓ Specifically, the classic method does not consider the constraints of an underwater environment and cluster structuring.

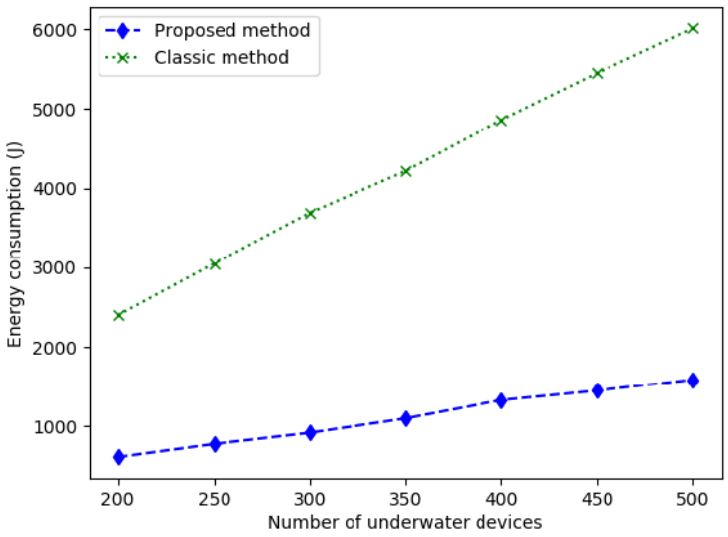
✓ The given classical method needs to be re-authenticated during movement of nodes between clusters.

Evaluation Results

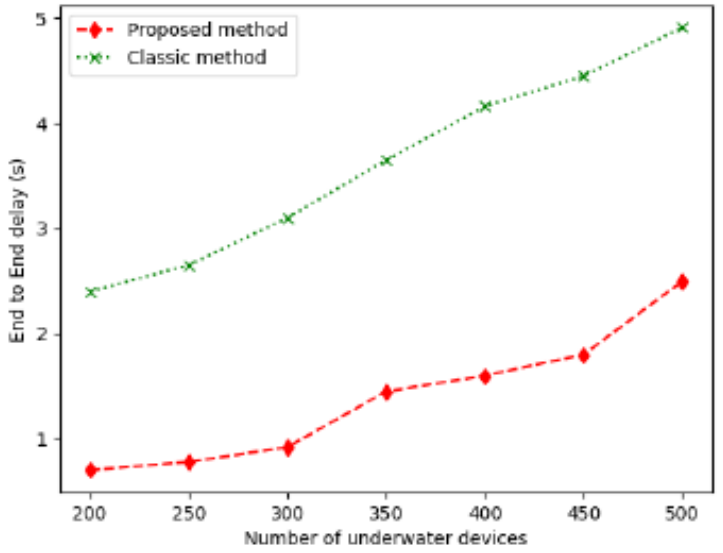
Measures	Classic	Proposed	Reduction (%)
Execution Time (sec)	24.450	12.405	49.26%
P_{com} (mW)	492628	246311	49.99%
Energy consumption (mJ)	12044	3055	74.63%

Equation Parameters	Description
N_t	Number of times a transmitter is switched "on"
P_t	Power consumed by transmitters (mW)
T_t	Transmitter "on" time (sec)
P_{out}	Output power (mW)
N_r	Number of times receiver is switched "on"
P_r	Power consumed by receiver (mW)
T_r	Start-up time for receiver (sec)
E	Energy (mJ)
t	Time (sec)

KENNESAW STATE UNIVERSITY

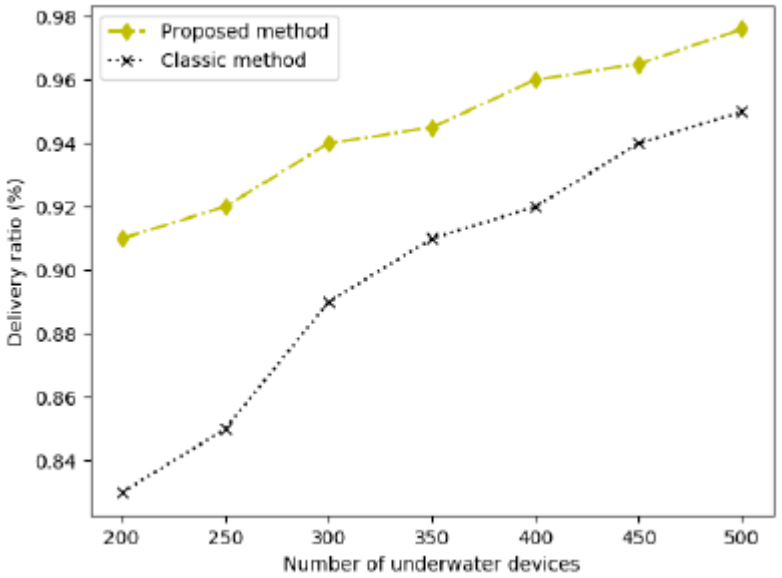


Average energy consumption in Simulated Scenario

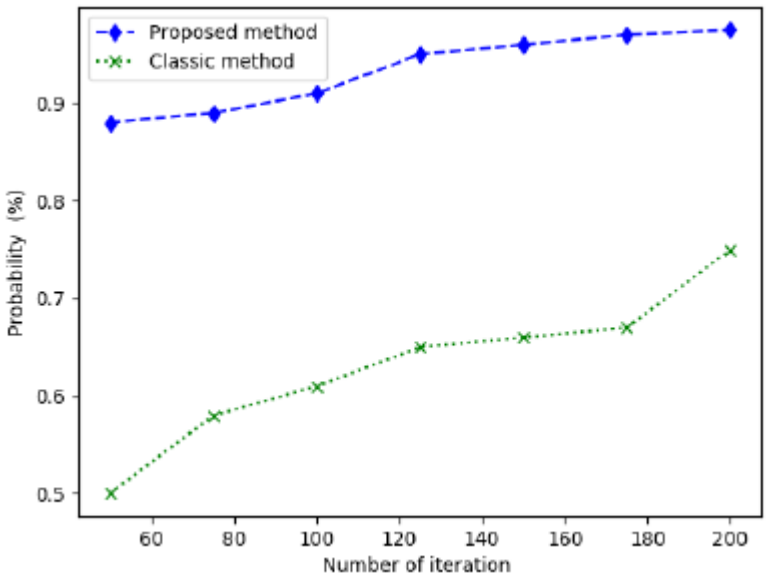


End-to-End delay

KENNESAW STATE UNIVERSITY



Packets delivered in Simulated Scenario



Authentication Attack Detection Probability

KENNESAW STATE UNIVERSITY

Conclusion

- Our preliminary work shows the feasibility of integrating blockchain with IoUT
- For future work, exploring the use of SDN in the underwater environment and its impact on the authentication process. Plus, more evaluation on blockchain performance.

KENNESAW STATE UNIVERSITY

Questions?

Decentralized Science Lab (dSL)

https://www.blockchaincyberlab.com/

Email: rparizi1@kennesaw.edu

KENNESAW STATE UNIVERSITY