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)
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,e

aCyber Science Lab, School of Computer Science, University of Guelph, Ontario, Canada
bDepartment of Computing and Software, McMaster University, Hamilton, ON, Canada
cDepartment of Computer Science and Engineering, Korea University, Seoul, Korea
dDepartment of Information Systems and Cyber Security, University of Texas at San Antonio, Texas, United States

title: 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
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!
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

IoUT applications

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


IoUT applications

- Military

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)
The architecture of the proposed method
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.
The process of migration and file transfer between IoUT devices

Algorithm 1 Migration mechanism among clusters

1: Call register (X1) // Reg devices in Cluster
2: Device X1 → Req authentication
3: HX → Send(authenticationvector (Public & Private/ Key))
4: Hash_Function (X1)
5: Node X1: receive (Hash 256)
6: Call Join_Cluster (X1) // join to cluster
7: If (X1 == Rang)
8: auth = 1
9: Calculate (mobility)
10: else
11: auth = 0
12: Calculate (migration)
13: While (auth = 0) do{
14: if (Mobility = 1 or migration = 1)
15: if (authenticate) // in cluster
16: HX: Message (X1)
17: Update(cluster info)
18: Migrate(X1, current, Target)
19: else
20: Hx: Message (Blockchain)/ send to BC Update X1
21: }
22: While (migrate or mobility ! = 0) {
23: New_cluster_head = Received (data_X1)
24: New_cluster_head = Decrypt (dataCreate header)
25: }
26: end

Algorithm 2 Transfer files in cluster

1: Device X1 Announce to X2 // User X1 wants to send information to User X2
2: If (user X1== authentic in cluster && trust)
3: HX (Check traffic cells)
4: X1 calculate (optimize (path))
5: X1 Encrypt (send data (dK)) // encrypt with Private key
6: X1 = Send (WK)
7: X2 = monitor_trust-data_ (X1)
8: else
9: Add to block ()
10: X2 = Received (data)
11: X2 = Decrypt (data) // using private key and re-organize data
12: end
Preliminary Results

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

<table>
<thead>
<tr>
<th>Simulation Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS-2, 35</td>
</tr>
<tr>
<td>Type of channel</td>
<td>Wireless channel</td>
</tr>
<tr>
<td>Radio range of a node</td>
<td>Random</td>
</tr>
<tr>
<td>Propagation model</td>
<td>Propagation/Two ray channel</td>
</tr>
<tr>
<td>MAC protocol</td>
<td>802.11</td>
</tr>
<tr>
<td>Mobility model</td>
<td>Random waypoint model</td>
</tr>
<tr>
<td>Nodes speed</td>
<td>3 m/s</td>
</tr>
<tr>
<td>Number of IoUT Devices</td>
<td>200 - 500</td>
</tr>
<tr>
<td>Link type of queue</td>
<td>Queue/Drop Tail</td>
</tr>
<tr>
<td>Number of Cluster</td>
<td>10</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>Constant Bit Rate (CBR)</td>
</tr>
<tr>
<td>Type of Antenna</td>
<td>Antenna/Omni Antenna</td>
</tr>
<tr>
<td>Simulation Time (Second)</td>
<td>800</td>
</tr>
<tr>
<td>Evaluation parameters</td>
<td>End to End delay, delivery ratio, Energy consumption</td>
</tr>
<tr>
<td>Number of Simulation runs</td>
<td>30</td>
</tr>
<tr>
<td>Area</td>
<td>2500 m² * 2500 m</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 Byte</td>
</tr>
<tr>
<td>Length of packets (Cluster to BC)</td>
<td>32 Byte</td>
</tr>
<tr>
<td>Previous hash</td>
<td>16 Byte</td>
</tr>
<tr>
<td>Transaction counter</td>
<td>9 Byte</td>
</tr>
<tr>
<td>Block Header/Block Size</td>
<td>80/8 Byte</td>
</tr>
</tbody>
</table>
• 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

<table>
<thead>
<tr>
<th>Measures</th>
<th>Classic</th>
<th>Proposed</th>
<th>Reduction (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution Time (sec)</td>
<td>24.450</td>
<td>12.405</td>
<td>49.26%</td>
</tr>
<tr>
<td>$P_{com}$ (mW)</td>
<td>492628</td>
<td>246311</td>
<td>49.99%</td>
</tr>
<tr>
<td>Energy consumption (mJ)</td>
<td>12044</td>
<td>3055</td>
<td>74.63%</td>
</tr>
</tbody>
</table>
Average energy consumption in Simulated Scenario

End-to-End delay
Packets delivered in Simulated Scenario

Authentication Attack Detection Probability
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.
Questions?

Decentralized Science Lab (dSL)
https://www.blockchaincyberlab.com/

Email: rparizi1@kennesaw.edu