An IoT Data Communication Framework for Authenticity and Integrity

UNIVERSITY OF CALIFORNIA SANTA CRUZ

Xin Li*, Huazhe Wang*, Ye Yu† and Chen Qian*

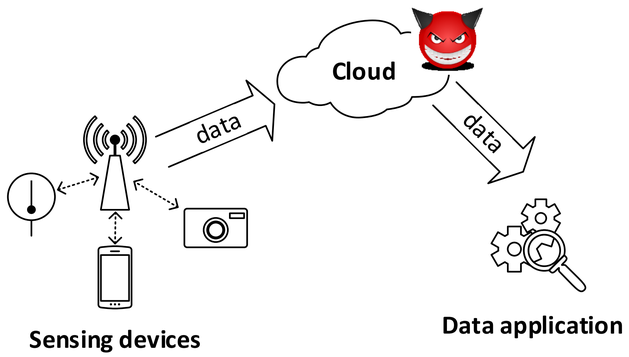
*Department of Computer Engineering, University of California Santa Cruz

†Department of Computer Science, University of Kentucky

NDSS '17 SYMPOSIUM

Introduction

- IoT sensing devices carry constrained resource and storage capacity, therefore sensing data need to be transmitted to a cloud. Data applications retrieve sampled sensing data from the cloud for analysis.



Overview of the IoT data communication framework

- Security Threat
  - Cloud is not trustworthy.
  - Scope
    - Authentication and Integrity, NOT confidentiality.
- Challenges
  - Verifiable authenticity and integrity: Signature
  - Uniform partial data retrial

Comparison of Different Signature Schemes

Signature Scheme	Computation Efficiency	Partial Data Retrieval	Constant Space Cost	Sampling Uniformity
Sign-each	x	✓	✓	x
Concatenate	✓	x	x	x
Hash Chaining	✓	x	✓	x
DSC	✓	✓	x	x
GSC	✓	✓	✓	✓

Dynamic Tree Chaining (DTC)

- One variation of Merkle Tree
  - Buffer digests only, not messages
  - Build authentication tree in an online fashion
  - Space Complexity: O(*log* n)
  - Sign the authentication tree when buffer is used up and then flush all nodes to the cloud.
  - Signing/verifying speed is capped by buffer size.

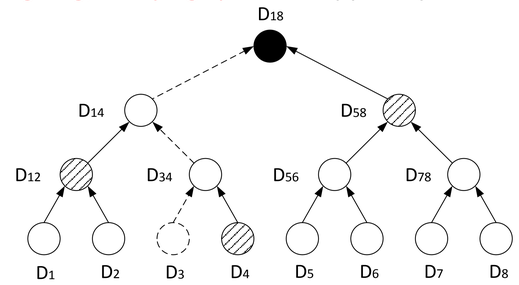
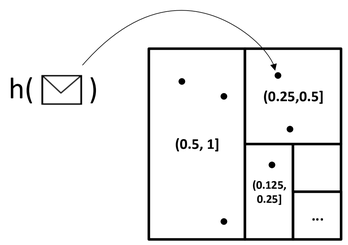


Illustration of Tree Chaining

Geometric Star Chaining (GSC)

- The events included in the sample blocks are in geometric distribution.



Visual Representation of Sample Blocks

- Chain sample blocks in a star topology.
  - $D_{new} = h(h(e)||D_{old})$
  - Space Complexity: O (1)

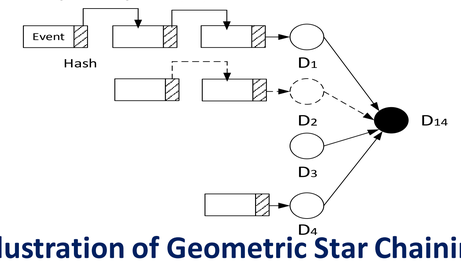
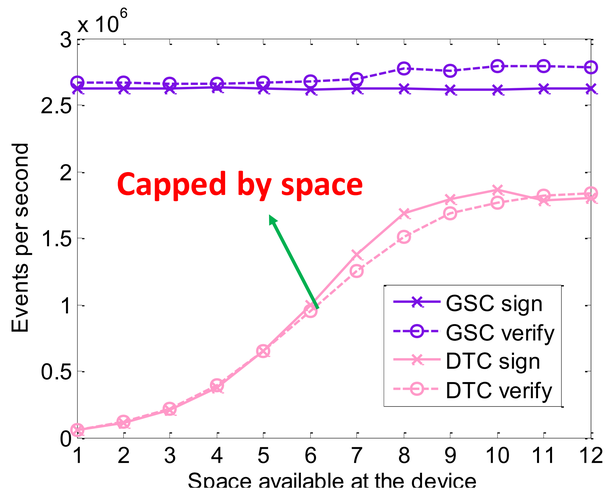


Illustration of Geometric Star Chaining

Prototype Implementation and Evaluation

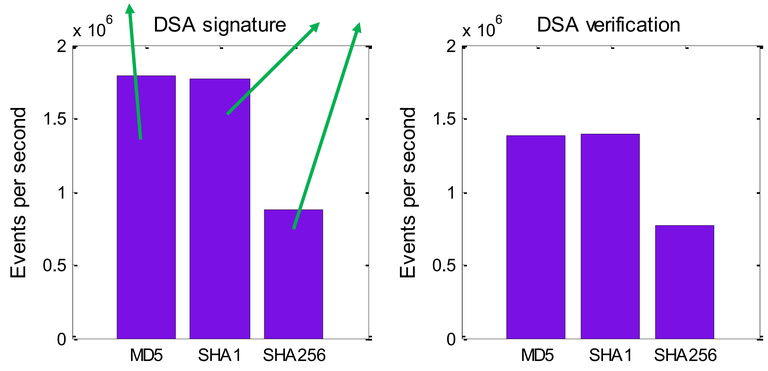
- Implement DTC, GSC and the sign-each method on a quadcore@3.40G Linux desktop with 32GB memory.
  - Asymmetric encryption algorithm: DSA
  - Message digest function: MD5
  - Vary the buffer space limit at the signer side
  - The sign-each method is 50X slower than the others



Signing/verifying throughput comparison.

- Different message digest functions are tested

Hashing dominate running time



GSC throughput with different digest function.

Full paper accepted for publication in Proceedings of ACM/IEEE IoTDI 2017