GridStat Middleware Communication Framework: Management Security and Trust

Focused Targeting in Fractal Hash Sequences

Kelsey Cairns, Carl Hauser, Thoshitha Gamage

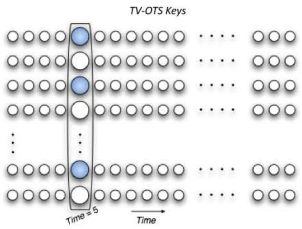
Goals

- Support real-time multi-cast message authentication (MMA) with low latency and computation cost in GridStat to allow emerging power grid monitoring systems to exploit sensor data for many purposes and at many locations,
- Improve performance of *Time-Valid One-Time-Signatures* (TV-OTS) [1] by extending the *Fractal Hash Sequence Representation and Traversal* [2] technique to enable *Focused Targeting*

Technical Background

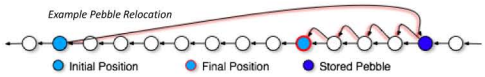
TV-OTS

- TV-OTS is a very promising protocol, showcasing:
  - Highly secure verification through one-time signatures with multiple, periodically refreshed keys
  - Low computational overhead for signing and verification
- TV-OTS generates its keys using hash chains – lists of keys where each is the hashed value of the next
- At time i_t, TV-OTS chooses keys from the set of i_t^{th} hash chain keys

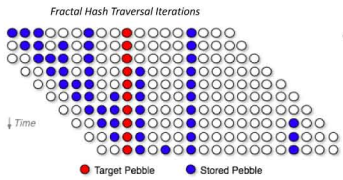


Fractal Hash Sequence Representation

- Amortized computation with $O(\lg(n))$ time bounds
- $O(\lg(n))$ storage achieved by storing only a short list of pebbles: small data structures associating each key with an *index* and *type*
- Pebbles are *relocated* as their keys are retrieved, storing a new unused key. Each new key must be computed by hashing a stored key



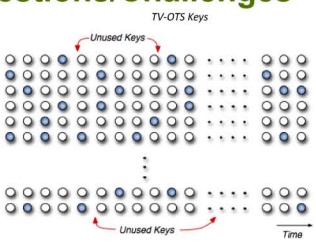
- Pebbles choose new locations deterministically based on their type. A pebble with type t will increase its index by $2t$
- With each retrieval, one pebble relocates to an unused index



- Caveat: Before the retrieval of any specific key, all preceding keys must be retrieved.

Fundamental Questions/Challenges

- TV-OTS uses only a small percentage of generated keys, resulting in hash chains with large ranges of unused elements
- Without a way to skip elements, unwanted keys must be computed and discarded, wasting computation time



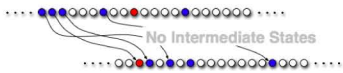
Research Plan

- Design, implement, and compare new versions of Fractal Hash Traversal that use *Focused Targeting:* the ability to jump to specific chain elements with no wasted computation

Research Results

Theoretical Insights

- Pebble distributions can be thought of as states with deterministic transitions. The state after the i^{th} retrieval can be created at any time.
- Conceptually, Focused Targeting can be broken into stages:
  1. State Calculation
  2. State Transition



- *Focused Targeting saves hash operations by transitioning directly between initial and final states*

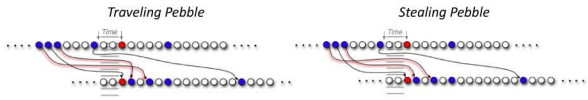
State Calculation

- Only two rules are necessary to calculate a new state in $O(\lg(j))$steps, for a jump length j
  1. If t and i are pebble p's type and final index, there must be a pebble with larger type at index $i' = i + t$
  2. Each pebble's new index is the smallest permitted by rule 1 that is greater than the retrieved index

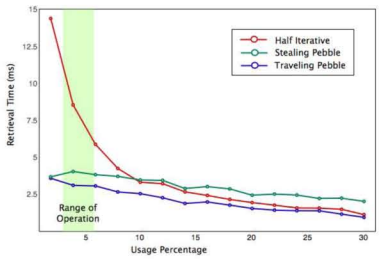
State Transitions

- Pebbles must be moved in an order that minimizes performed hash operations

- Two ordering strategies were found, with prioritization differences potentially impacting runtime. Associated algorithms were christened *Traveling Pebble* and *Stealing Pebble.*



Analysis



- Tests on 100-element hash chain indicate near-linear performance as the usage percentage nears zero
- Performance significantly improved for TV-OTS's operational range

Broader Impact

- With Focused Targeting, TV-OTS becomes a more feasible protocol for reliable authentication in many applications

Interaction with Other Projects

- A logical continuation of the work done in designing TV-OTS
- Implemented as part of the GridStat infrastructure

Future Efforts

- Combine state transition strategies to move the most available pebble
- Redesign states, choosing a pebble distribution optimized for the expected jump length

References:

[1] Qiyan Wang; Himanshu Khurana; Ying Huang; Klara Nahrstedt, "Time Valid One-Time Signature for Time-Critical Multicast Data Authentication," *IEEE INFOCOM 2009*, April 2009

[2] M. Jakobsson, "Fractal Hash Sequence Representation and Traversal," *Proceedings of the 2002 IEEE International Symposium on Information Theory*