TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

K-TIME SIGNATURES FOR SMARTGRID MULTICAST

NOVEMBER 12, 2014

KELSEY CAIRNS

PHD STUDENT, WASHINGTON STATE UNIVERSITY

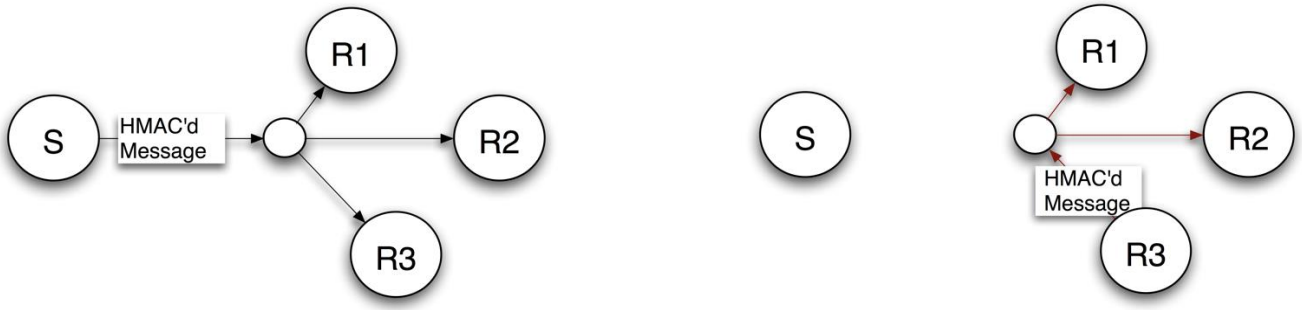
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

SMARTGRID DATA COMMUNICATION

- Massive sensor data streams
  - Measurements streaming from potentially thousands of PMUs
    - State Estimation
    - Wide area monitoring and control
    - Islanding detection and restoration
    - Renewable Integration
- Widely distributed application level data
  - Pricing and energy market information
- Malicious data could cause applications to malfunction
- Data authentication protects against corrupt data

MULTICAST AUTHENTICATION PROBLEM

- Current data authentication standards present complications
  - RSA signature generation takes 30ms to 50ms
  - HMAC is fast, but not secure for one-to-many (multicast) communication

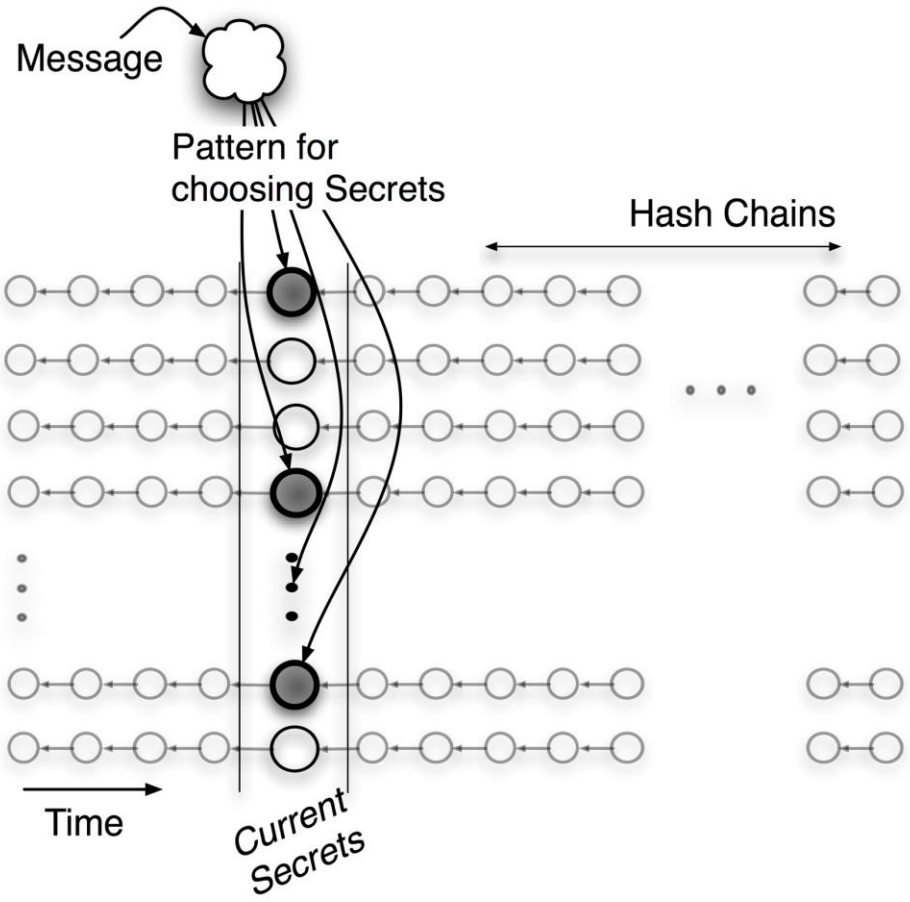


Receivers cannot distinguish expected sender and malicious group member

- Hash based k-time signatures address these issues
  - TV-OTS: Time-Valid One-Time-Signatures

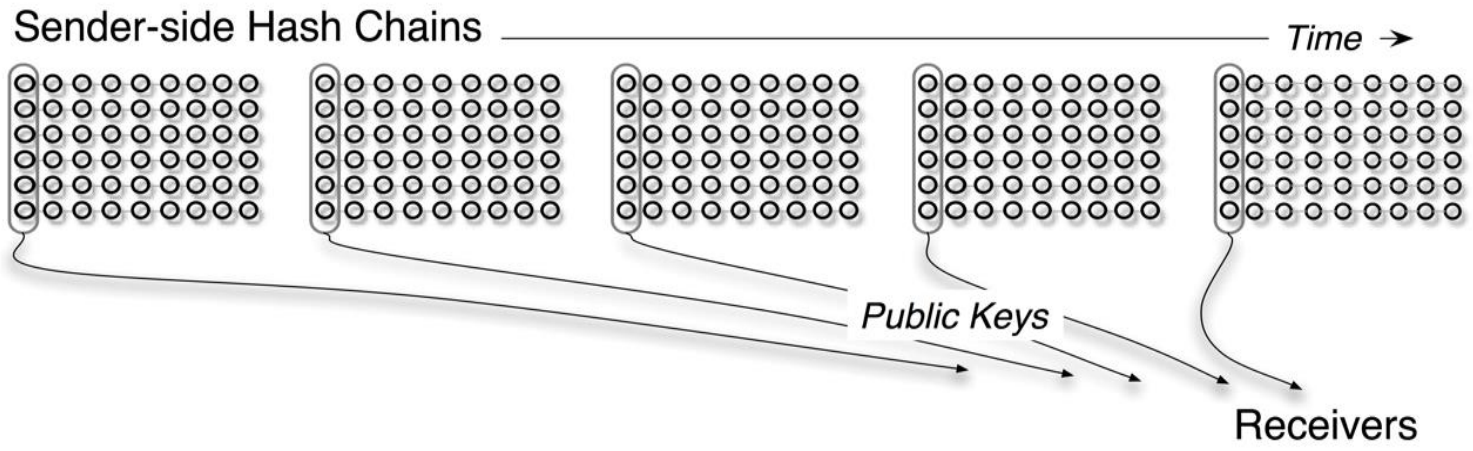
TV-OTS: HASH CHAINS AND SIGNING

- Signature Creation
  - Senders own a large array of hash chains
  - Slices from the hash chains provide secrets available for use in signatures
  - Each message maps to a set of currently available secrets



TV-OTS: PUBLIC KEYS AND VERIFYING

- Public keys contain arrays of values allowing receivers to prove that any given secret belongs to a particular chain
- Receivers verify signatures by verifying each contained secret
- New public keys must be distributed once hash chains are exhausted
  - Chains must be pre-computed on sender's side



PERFORMANCE AND SECURITY

- TV-OTS implemented as a GridStat security module
- Repeatable DETERLab experiments provided results for numerous parameter choices
- Security measured by probability of a successfully forged signature for a given message

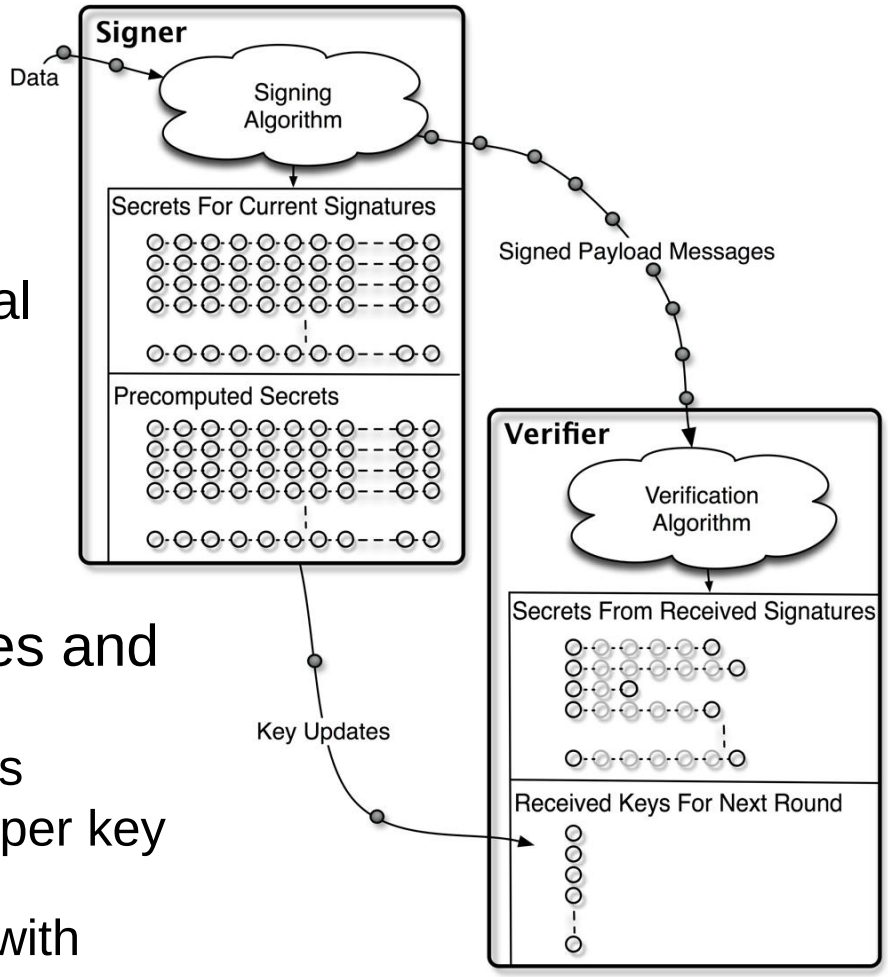
Chains	Secrets per Signature	Epoch	Chain Length	Signing Latency	Attack Success Probability
1024	13	.25s	512 to 16384	.5ms to 1ms	7e-7 to 2.2e-17
		.25s to 1s	8192	.2ms to 1ms	
16384	11	4s	512 to 16384	.5ms to 1.5ms	1.7e-12 to 4.5e-19
		1s to 4s	8192	.5ms to 1ms	
Publisher Specifications: 2.13GHz Intel Xeon Quad Core with 4GB RAM					

Related Publication: *Flexible Data Authentication Evaluated for the Smart Grid*

UNDERWAY: DEPLOYMENT FRAMEWORK

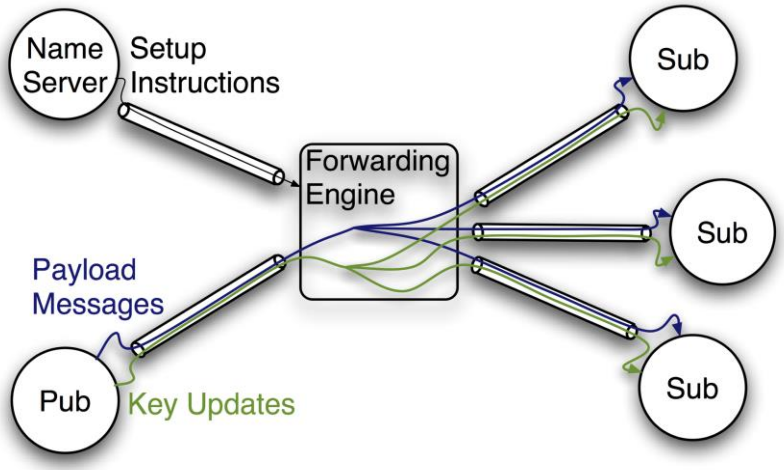
- The Challenge: Distribute verifiable key material
  - 5Kb to .5Mb depending on number of chains and size of secrets
  - .005 to 30 bytes of key material per payload message

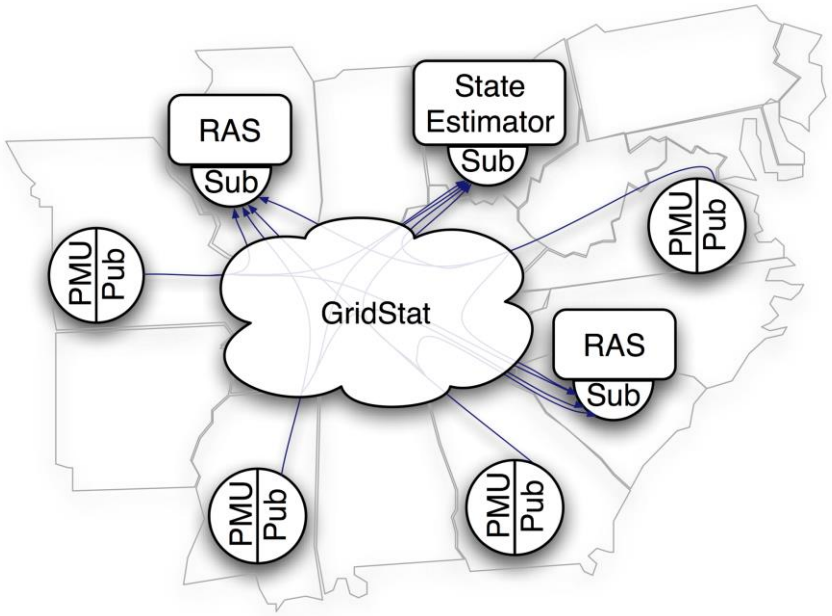
- Solution: Key distribution framework
  - Distribute payload messages and future keys concurrently
    - Keys distributed in segments
    - Several payload messages per key update message
    - Key updates authenticated with traditional algorithms



TESTING

- Compare redundancy strategies over unreliable networks
  - Redundant key updates ensure secrets from all chains are verifiable





- Include past secrets from infrequently used chains in the key updates to reduce verification workload
- Add nodes and network delays to experiment to simulate larger scale

CONCLUSION

- K-time signatures such as TV-OTS provide fast authentication for multicast environments
- The framework being developed enables k-time signatures for a large class of big data applications including sensor networks in the Smart Grid

MORE INFORMATION

- Talk to us:
  - kelsey.cairns@email.wsu.edu
  - hauser@eecs.wsu.edu

- TCIPG Industry Workshop ‘14 Poster:

  GridStat Middleware Communication Framework: Management Security and Trust

  K-Time Signature Deployment: A Practical Framework

TV-OTS SECURITY

- TV-OTS provides probabilistic security: an attacker can do better than brute force
- Eavesdrop attack:
  - Attacker collects secrets exposed in signatures
  - The secrets necessary to sign a given message may be among the exposed secrets
  - A more advanced approach: the attacker may search for messages that can be signed with the collected secrets
- Attack success probability controlled by the fraction of secrets exposed and time elapsed before using a fresh set of secrets