CREDC

Resiliency Metrics for Electric Grid and Analyzing Impact of Defense Mechanisms

# Receiver-Side Confidence Estimation and Reporting for TV-OTS Data Authentication

Kelsey Cairns, Carl Hauser, and Adam Hahn

## GOALS

### Overall Goal

- Provide fast authentication using Time-Valid One-Time-Signatures (TV-OTS) for high-rate, low-latency sensor data streams.

### Current Goals

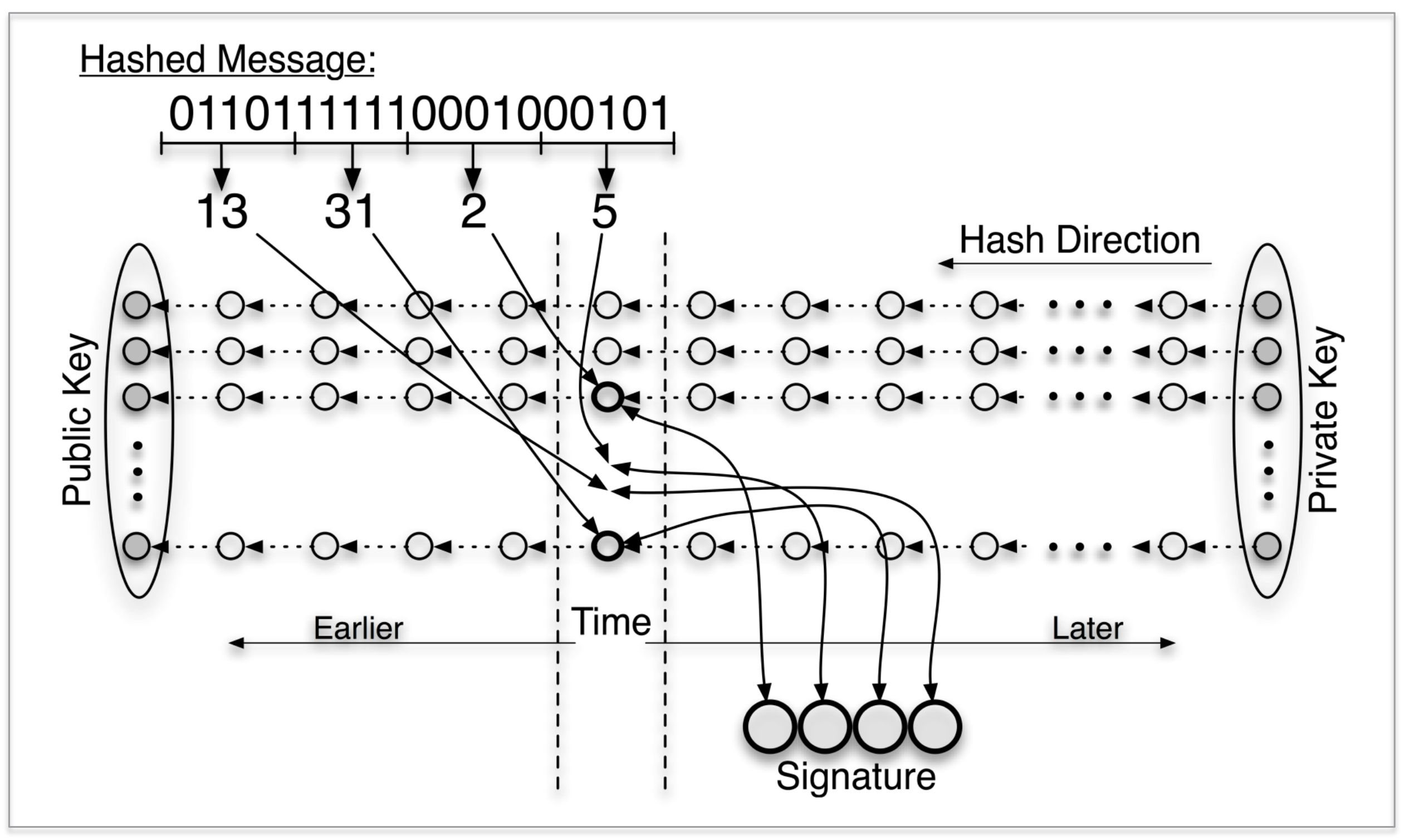
- Use receiver's global knowledge to estimate confidence in the validity of each individual signature.
  - Takes into account known attacks.
  - Uses evidence acquired through signatures to estimate confidence.
- Deploy within GridStat.

## BACKGROUND AND FUNDAMENTALS

- Data authentication for Smart Grid applications ideally supports the following features:
  - Low latency.
  - Secure multicast.
  - Low key distribution overhead.
  - Message independence.
- Current protocols do not satisfy these requirements.
- Our previous work shows TV-OTS has these features:
  - Low-latency signature generation and verification.
  - Flexibility to adjust security and performance.
  - Robust against attacks (dictionary, DoS, dropped packet, replay).

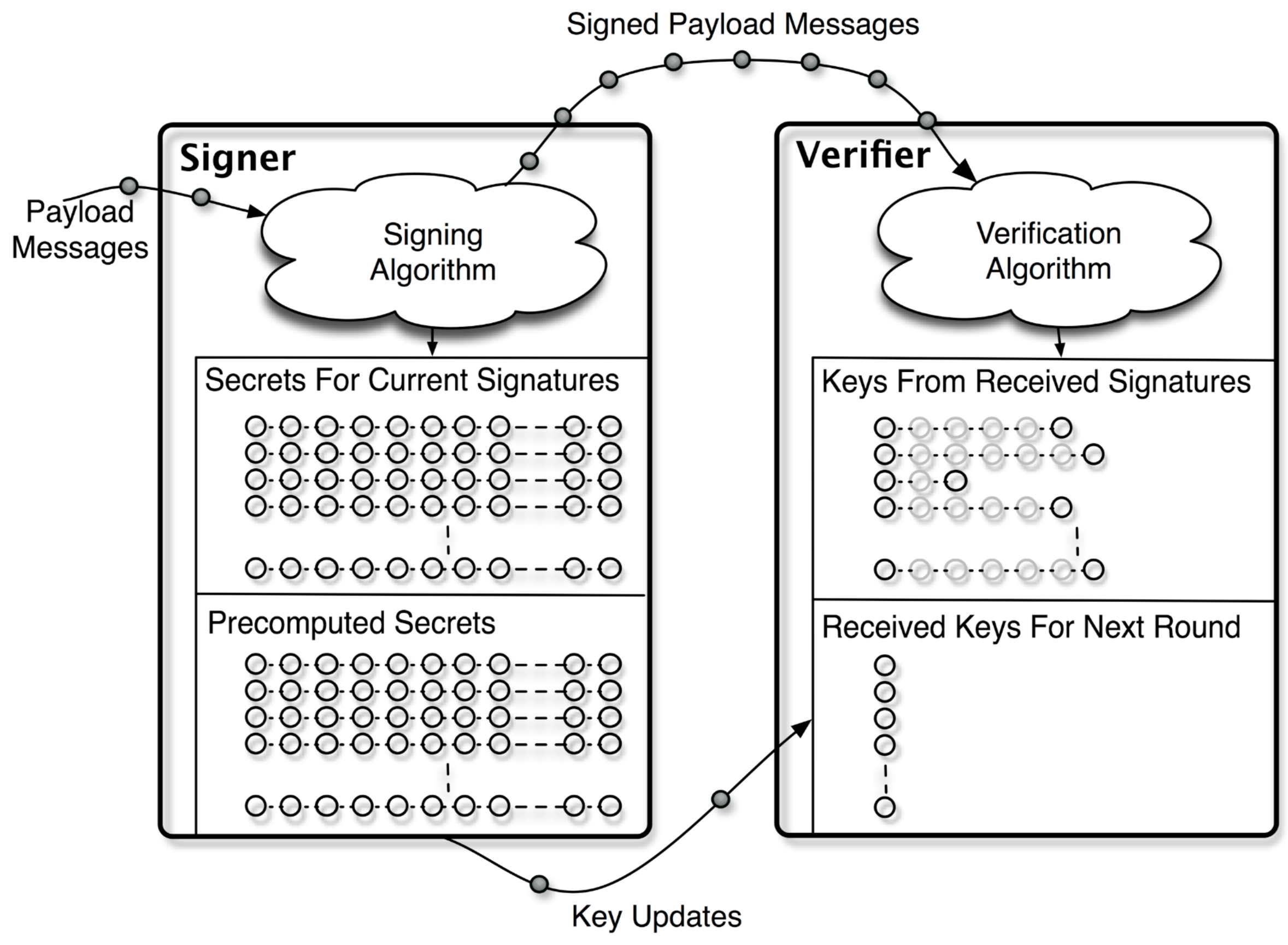
### *TV-OTS Overview*

- Time divided into fixed-length epochs.
- Senders maintain a set of secret hash chains.
- Signatures are created with the HORS signature scheme, using the set of hash chain secrets during each epoch:
  - Messages hashed into multiple short bit strings (indices).
  - Generated indices specify secrets to include in signature.
  - Timestamp also included in signature.
- Signature verification.
  - Packet freshness verified.
  - Indices generated from message to determine expected index of each included secret's chain.
  - Each secret verified by hashing to recreate publicly known value.
  - Verified for the epoch of the signature timestamp.



### *Key Exchange*

- Key stream sends future public keys independently of current messages.
- Senders compute future public keys while signing with current secrets.



- Key update messages sent much less frequently than payload messages.
  - Allows traditional public key authentication (e.g., RSA) for key updates.

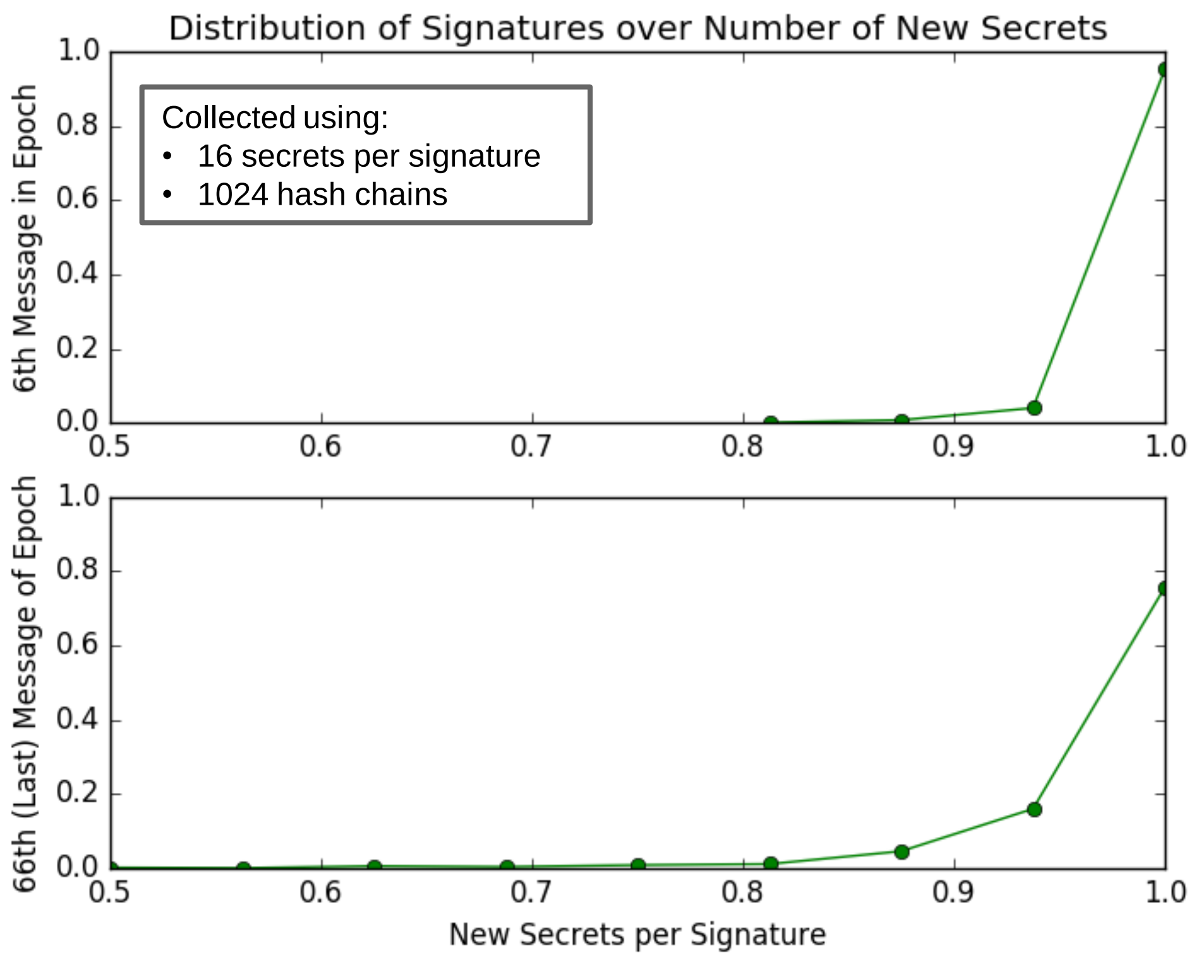
## CURRENT RESEARCH

### *Probabilistic Signature Verification*

- TV-OTS security is inherently imperfect.
  - Small probability that each signature may be forged.
  - That probability, hence the system security, is tunable using TV-OTS parameters.
- Receivers can use global knowledge and local evidence to estimate a per-signature confidence.
- **Signature verification result is a probability, not a Boolean.**

### *Eavesdrop Threat*

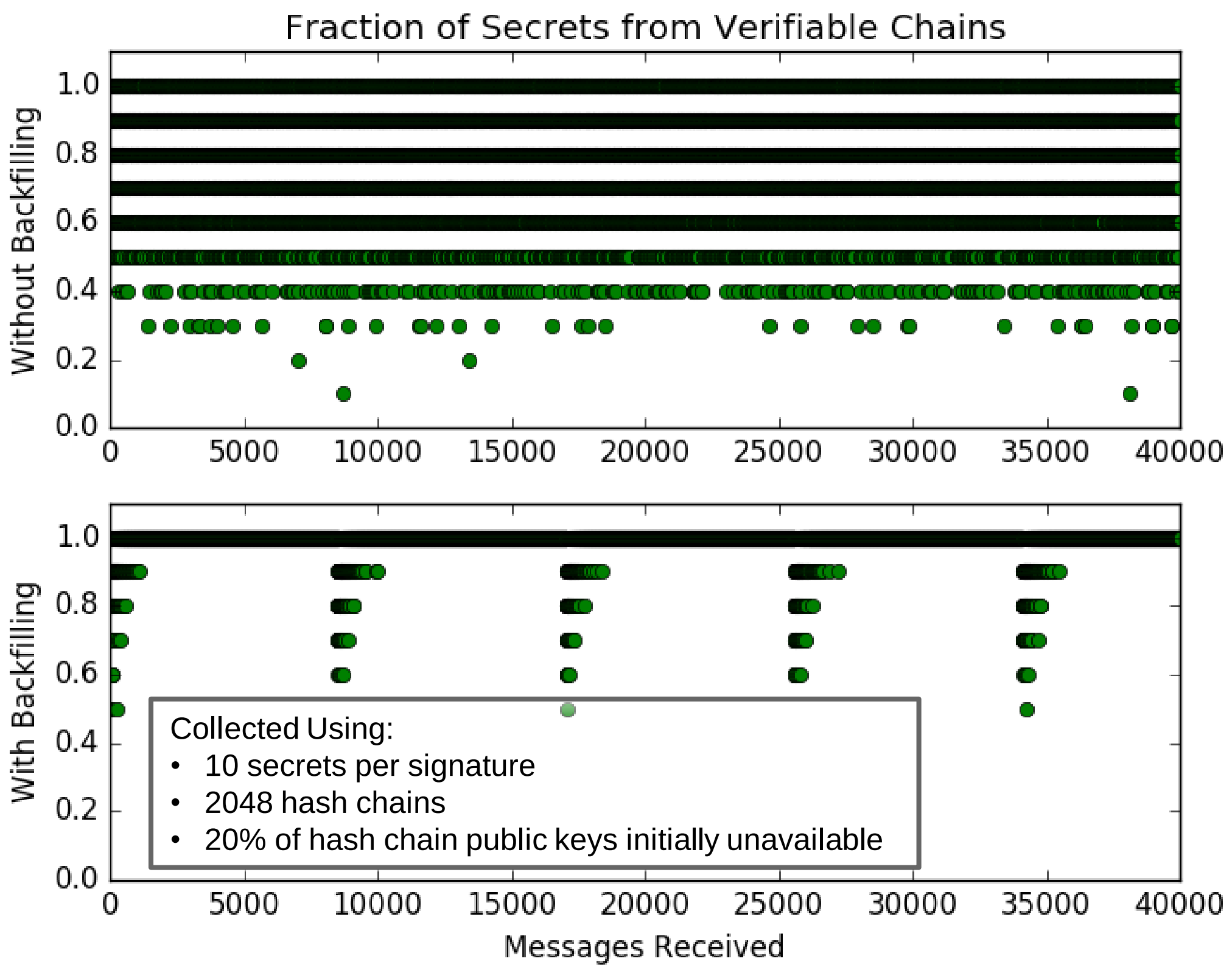
- Secrets that receivers successfully verify may be subject to eavesdrop attacks:
  - Attacker learns secrets from legitimate signatures.
  - Attacker substitutes learned secrets into malicious signature.
  - Requires overlap in the secrets exposed and secrets needed.



- Secrets in a signature that are duplicates of secrets appearing in previous signatures have certainly been exposed to the attacker.
- Even secrets that haven't been seen before may have been exposed to an attacker if the attacker is blocking messages.

### *Blocked Keys Threat*

- Our key distribution system runs over unreliable networks.
- Some hash chains may be missing public key values.
- Signatures containing secrets with no chain to verify against cannot contribute to confidence.



- *Backfilling idea*: if a secret has no corresponding chain, but otherwise the signature confidence is high, that chain may be recreated from the signature secret and used to verify future signatures.

Note: Parameters chosen to visually show threat effects rather than realistic performance.

## BROADER IMPACT

- Explores the idea of informed probabilistic security.
- Fast authentication, applicable to a large class of big data applications.

## INTERACTION WITH OTHER PROJECTS

- Continuing investigation of TV-OTS, originally a TCIPG project.
- Implemented as part of GridStat.
- Leverages GridStat's deployment in DETERLab.

## FUTURE EFFORTS

- Combine different types of threat evidence into single estimate on signature confidence.
- Build attack code to test accuracy of the confidence estimation system.

References:

[1] Kelsey Cairns; Carl Hauser; Thoshitha Gamage, "Flexible Data Authentication Evaluated for the Smart Grid," IEEE SmartGridComm, October 2013.

[2] Kelsey Cairns; Thoshitha Gamage; Carl Hauser, "Efficient Targeted Key Subset Retrieval in Fractal Hash Sequences," ACM CCS, November 2013.

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

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY