Tradeoffs Between Latency and Security in Multi-cast Message Authentication Protocols

Thanigainathan Manivannan, Dave Anderson, Carl Hauser

Background

- Emerging power grid applications for PMU and other time-synchronized data will use data collected at one point in the grid for a variety of purposes at multiple other points (e.g., NASPInet design).
- Multi-cast uses source and network resources efficiently when the same messages are to be delivered to multiple recipients.
- GridStat (Figure 1) is an experimental data delivery service, similar to NASPInet, for power grid applications, built with multi-cast as a central design principle.
- GridStat's Security Management Framework provides a modular interface for implementing and evolving the security algorithms and protocols used between publishers and subscribers.
- Providing confidentiality as a service is straightforward, based on widely used encryption protocols.
- Providing a message authentication service in a multi-cast environment is a much greater challenge.
- Primary authentication issues are 1) latency, 2) computation cost, and 3) protection against impersonation of sender by group members.

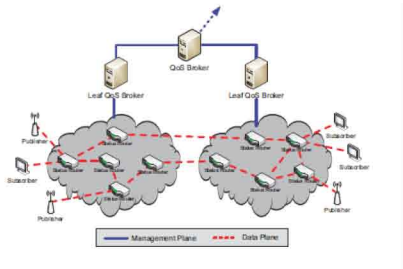

Figure 1: GridStat Managed Pub-Sub Architecture

Goals

- No single multi-cast message authentication (MMA) technique suffices for all power system applications.
  - Public-key-based MMA is computationally costly (Figure 2).
  - Timed-key-release protocols' achievable latency for all recipients is limited by network latency to the farthest recipient.
  - Symmetric-key-based MMA does not protect against impersonation of the sender by a multi-cast group member.
- Therefore, we need to provide a variety of modules in GridStat's Security Management Framework supporting low-latency, high-security MMA.
- We also need to provide guidance to application implementers on choosing among the implemented protocols based on applications' different latency and security requirements. (Unfortunately, the most desirable points in the design space are not simultaneously achievable with current techniques.)

Algorithm/protocol	Publisher Computation cost (ms)	Subscriber Computation cost (ms)	Total computation cost (ms)
AES (128 bit)	0.04	0.03	0.07
RSA (2048 bit)	59.00	2.04	61.04
DSA (1024-bit)	5.10	9.80	14.90
TV-OTS	0.04	1.42	1.46
TESLA	0.03	0.03	0.06
HMAC-SHA1	0.02	0.02	0.04
CMAC	0.04	0.04	0.08
SHA-256	0.01	0.01	0.02

Figure 2: Computation Cost for Different Algorithms at Publisher and Subscriber Nodes

Fundamental Question

- What are the performance vs. security tradeoffs when using timed-release protocols vs. public-key protocols vs. symmetric-key protocols?

MMA Design Space

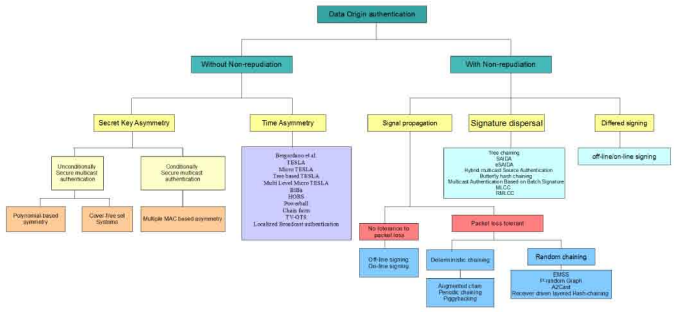

Figure 3: Classification of Data-origin Authentication Protocols

Scheme	Sender comp. cost	Receiver comp. cost	Message size overhead	Packet buffering		key size	Total latency
				Sender	Receiver		
AES	1E	1D	1k	1	1	O(1)	1E+1D+ND
RSA	1S	1V	1k	1	1	O(1)	1S+1V+ND
TESLA	1H	1H	1k+1h	1	Є	O(1)	2H+ND+KD
TV-OTS	1H	1H	0.25* h	1	1	O(N)	2H+ND

E - Encryption D - Decryption k - no of keys H - Hash M - Message authentication code Є - number of packets per key disclosure delay
N - Number of hash chains used S - Signature V - Verification KD - Key disclosure delay h - Hash size TESLA - Timed Efficient Stream Loss-Tolerant Authentication
TV-OTS - Time Valid One time signature ND - Network delay

Figure 4: Theoretical Performance of Various Authentication Protocols

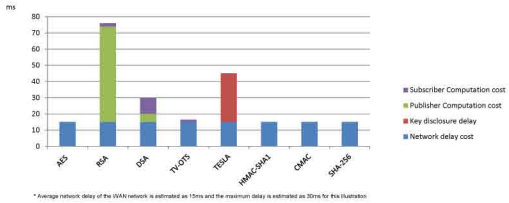

Figure 5: Actual Performance, Various Protocols

- Timed-key release protocols provide data origin authentication by the delayed release of keys with time synchronization between end nodes.
- If non-repudiation is required, a public-key signature scheme is required but comes at a high cost in both computation time and total latency.
- TESLA has low message size overhead and computation cost but incurs a network delay and a maximum network delay (to any subscriber) in latency.
- TV-OTS has higher computation cost and message size overhead than TESLA but lower total latency.
- Symmetric-key-based schemes are fast but don't provide cryptographic protection against spoofing by a group member. Other system properties can help with this, though.

Broader Impacts

- Other resource-constrained applications that require multi-cast authentication, such as other types of sensor networks, may benefit from the use of time-asymmetric protocols for message source authentication.

Future Efforts

- Performance analysis and comparison of other timed-release protocols to evaluate their use in time-critical multicast applications.
- Hardware-assisted public-key cryptography at commodity prices would potentially be of great help in meeting emerging authentication needs of wide-area cyber-physical systems.