nano-tera.ch
swiss scientific initiative in health / security / environment systems

SmartGrid RTD 2013

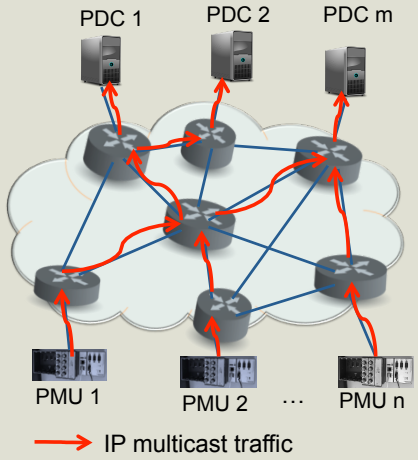
FNSNF

Experimental Comparison of Multicast Authentication for Wide Area Monitoring Systems (WAMS)

Teklemariam Tsegay Tesfay and Jean-Yves Le Boudec

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Multicast for WAMS



Multicast Authentication Challenges

- Resource-constrained field devices (PMUs)
- Real-time smart grid applications

Required properties of authentication schemes

- Guarantee that sources are capable of signing and receivers only verifying
- Asymmetric knowledge of key material between senders and receivers
- Lightweight and fast computation time

Experimental Comparison of Authentication Schemes

Candidates chosen among a host of authentication schemes

1. **ECDSA** (Public-key crypto)
   - over a 112-bit prime field
   - With and without pre-computed tokens
2. **TV-HORS** (One time signature)
   - Parameter values: (N=1358, t=12, v=5)
3. **Incomplete-Key-Set** (MAC based)
   - Three variants with different goals

➢ All provide a security level L ≈ 54 - strong enough for short-term keys

➢ Key refresh time every 20 sec. (5 sec for TV-HORS)

Comparison metrics

1. Computation cost (ms)
   - Signing and verification
2. Communication cost (bytes)
   - Size of signature
3. Key-management cost
   - Key generation time (ms)
   - Key distribution cost (bytes)
   - Storage cost (bytes)

Scheme	Key management overhead per reference session (20 sec)			
	key generation time at PMU (ms)	key distribution overhead (bytes)	Storage overhead at source (bytes)	Storage overhead at receiver (bytes)
ECDSA without precomputed tokens	8.010	14	14	14
ECDSA with precomputed tokens	3'208	14	2'8014	14
TV-HORS	418.8	32'632	407'900	8'158
Basic Incomplete-key-set	0	7'728	1'932	175
Comm. efficient Incomplete-key-set	0	30'912	7'728	700
Perfectly-secure Incomplete-key-set	0	1'400	350	7

Scheme	Computation overhead per synchrophasor message			Communication overhead (bytes) per synchrophasor message
	Auth. time (ms)	Verif. time (ms)	Total (ms)	
ECDSA without precomputed tokens	3.431	0.223	3.654	34
ECDSA with precomputed tokens	0.104	0.223	0.327	34
TV-HORS	0.014	0.093	0.107	82
Basic Incomplete-key-set	4.571	0.045	4.616	1'725
Comm. efficient Incomplete-key-set	18.182	0.136	18.318	138
Perfectly-secure Incomplete-key-set	1.572	0.012	1.584	350

- ECDSA with pre-computed tokens outperforms all other schemes.
- Though TV-HORS has low computation cost, its high key-management cost and inherent property of hard-deadline to distribute a large public key to receivers makes it less preferable than ECDSA.
- Incomplete-key-set variants have high computation and communication cost.

References

[1] T. Tesfay, J.-Y. Le Boudec "Experimental Comparison of Multicast Authentication for Wide Area Monitoring Systems", Infoscience (http://infoscience.epfl.ch/record/216923/files/Multicast_Authentication_Performance.pdf)