Information-Theoretic Approach to Authentication Codes for Power System Communications

Authors: T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi

Presenter: Emal Latifzai

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Agenda

- Introduction
- Background
- Computational Authentication
- Information-Theoretic Authentication
- Case-Studies
- Implementation
- Personal Assessment
- Conclusion
- References

Introduction

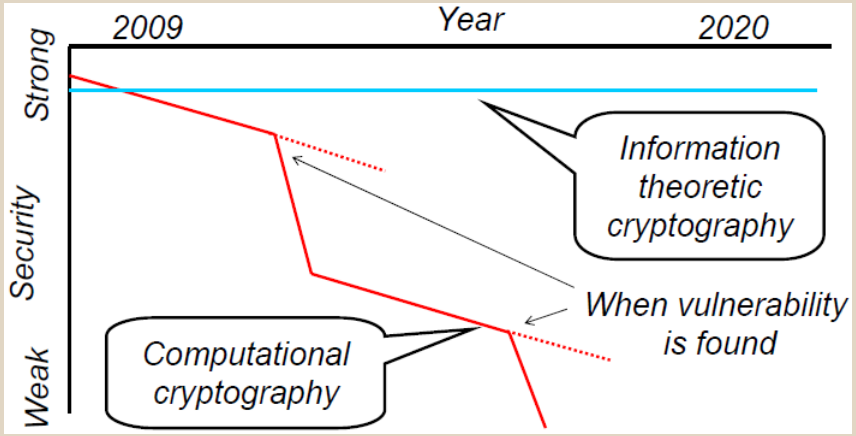
- Objective:
  - To realize a practical method of providing cyber security for power system communications that meets the requirements of real-time communication and long-term maintenance.
- Motivation
  - Current cyber security methods do not adequately address two important requirements of the power system communications network
    - Real-time communications dictates that the security overhead should be minimized
      - Thus the algorithms should be simple and require as little processing power as possible
    - Long-term maintenance requirements necessitate durable security structures
      - Reliability of algorithm should not degrade with time
- Approach
  - Apply information theoretically secure authentication system having short authentication tags and a feasible number of keys

Background

- The integrity of messages, rather than their confidentiality, is much more important for most power system operations
  - Therefore, the focus will be on authentication of data rather than encryption
- Authentication schemes can be divided into 2 major classes
  - Computational Security
    - Relies on computational infeasibility of an attack
  - Information-theoretic security
    - Independent of computing power or time an opponent can bring to bear

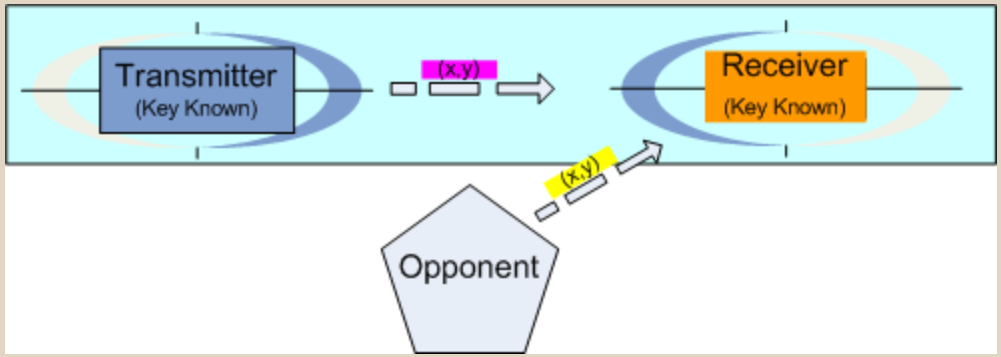
Computational Authentication

- Computationally secure algorithms may have excess overhead, therefore making them poor choices for real-time applications
- Computational security decreases with the advent of new methods of attack
  - Certain flaws have been detected in some algorithms suggesting that these and other algorithms could be deceived in the future
- Unable to provide the long-term security as the computational power available to attackers increases
  - Replacement of algorithms can be difficult in view of the shear number of devices utilizing them



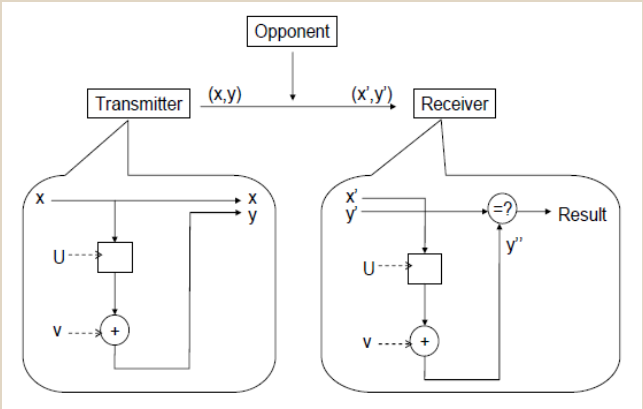
* From [2]

Information-Theoretic Authentication



- Game between transmitter(Tx)-receiver(Rx) as one party and opponent as the other party
  - Opponent assumed to have limitless computational power
  - Opponent wins if he sends a message to Rx and fools it into believing it is from Tx
  - Opponent loses if Rx determines false message was not sent by Tx
  - Message (x,y) consists of an a-bit source state x and a b-bit authentication tag y
    - y is func(x, key)
    - parameter called key shared by Tx and Rx

Information-Theoretic Authentication



* From [1]

- $y = xU + v$ (Eqn 1)
  - x: a-bit vector representing a source state (raw info)
  - y: b-bit vector representing an authentication tag for x
  - (U,v): the authentication key known by tx and rx
  - U: binary matrix with a rows and b columns
  - v: b-bit vector
  - +: bit-wise Exclusive-OR operation

- Tx uses (Eqn 1) to transform source state x into authenticated message (x,y)
  - x is source state and y is authentication tag formed through the use of the key (U,v)
- Rx uses same key (U,v) and function (Eqn 1) to test if received message (x',y') authentic or not
- Function (Eqn 1) is known by opponent but key is not
- For an information-theoretically secure authentication system, the tx must use new key for each new message
  - Opponent has independent problem to solve with each new message
  - In our example, U can be reused but v must be updated for each new message

Information-Theoretic Authentication

- Security Analysis
  - Two options for *deception* by opponent to get message accepted
    - *Impersonation*: opponent directly creates message
    - *Substitution*: opponent changes message from tx
  - Upper bound success probability (P_d) calculation
    - Impersonation

$$P_{d0} \leq \frac{1}{2^b}$$

    - Substitution

$$P_{d1} \leq \frac{1}{2^b}$$

y = xU + v (Eqn 1)

- x: a-bit vector representing a source state (raw info)
- y: b-bit vector representing an authentication tag for x
- (U,v): the authentication key known by tx and rx
- U: binary matrix with a rows and b columns
- v: b-bit vector

Information-Theoretic Authentication

- Independent of computer power attacker can bring to bear
  - Unnecessary to update algorithm
- Opponent's deception probability can be controlled
  - Depends on the length (b bits) of the v vector in the key (U,v)
- Function used is efficient to implement
  - $y = xU + v$ (Eqn 1)
- Theoretically can be very secure although huge number of keys are required when many packets are transmitted

Case Studies

- Current-differential relay

Transmission rate:	600 Hz
Frame data length:	2048 bits
Operation period:	20 years
Authentication tag length:	32 bits

- Deception probabilities are:

  $Pd0 = Pd1 = 1/(2^{32}) = 2.33E\text{-}10$

  - CRC-16 is one of the most widely used error detection codes in power systems
  - Misdetection rate: 10^-5

- Necessary key (U,v) memory size is:

  = (size of U) + (size of all v's)

  = 32 bit x (Frame data length) + 32 bit x (number of transmissions during 20 years)

  = 4 Bytes x (256 Bytes + 600 x 60 x 60 x 24 x 365 x 20)

  = 4 x 3.8E11

  = 1.5 TBytes

  - Widely available Flash memory can record 32 GB of memory today

Case Studies

- Phasor Measurement Units (PMUs)
  - Same parameters as current-differential relay case except with transmission rate of 60 Hz
    - Deception probability: same as relay
    - Necessary key memory size: 150 GBytes

Case Studies

- SCADA / SAS
  - All parameters same as relay except transmission rate which is non-periodic
    - Assume worst case scenario: 1 frame/sec
  - Deception probability: same as relay
  - Necessary key memory size: 2.4 GBytes

Case Studies

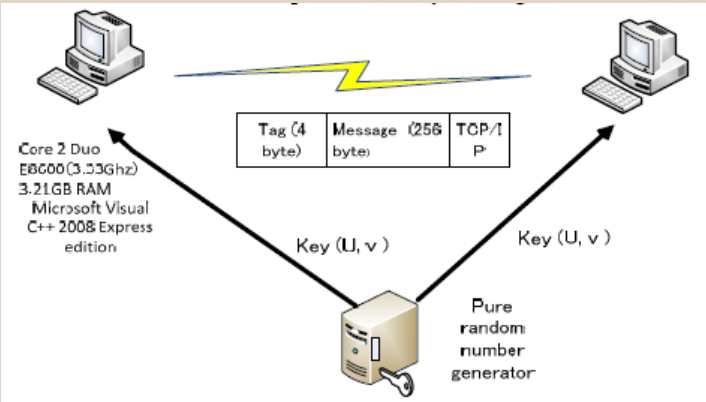
- Smart grids (smart meters)
  - Same parameters as relay except with operation period of 10 years and transmission rate of 1 operation per 30 minutes
  - Deception probability: same as relay
  - Necessary key memory size:
    - = (size of U) + (size of all v's)
    - = 32 bit x (Frame data length) + 32 bit x (number of transmissions during 10 years)
    - = 4 Bytes x (256 Bytes + 2 x 24 x 365 x 10)
    - = 692 KBytes
  - Communication requirement of other devices employed at distributed resources is similar to that of smart meters

Implementation

- Current-differential relay test
  - Proposed algorithm vs. HMAC SHA-256
  - Average time of SHA-256 was several hundred μseconds vs. a few μseconds for proposed algorithm
  - Authentication tag lengths not critical to execution time

Implementation

- Test between 2 computers
  - 500,000 packets sent via 100 Mbps LAN
  - Proposed method superior to HMAC SHA-256 in every category except for last one, key management scheme



* From [1]

Constraint	HMAC (with SHA256)	A- Codes	Requirement from power system
Resource constraint	Security co- processor, such as FPGA, might be needed because of heavy execution time.	No need for additional processor because of light execution time.	IEDs have limited memory and low processing power.
High availability	System maintenance may be necessary for software updates, which is caused by algorithm aging degradation.	Maintenance-free.	System maintenance is not preferable in view of system availability.
Low bandwidth	The length of MAC is 256 bits.	32 bits A-code is enough for practical use.	Low bandwidth serial communication channel is still used.
Long life span	Reliability of algorithm decreases gradually.	Reliability does not degrade with time.	Life time of an IED is several years.
Reliability	Reliability cannot be handled by power system engineers.	Reliability can be handled by power system engineers.	Reliability is preferable to be controllable.
Real time communication	High spec. CPU is needed to achieve real time communication.	Real time communication can be achieved with low power CPU.	Some relay applications, such as current differential relays for transmission line protection, need real time communications.
Easy key management scheme	Key size is small, but periodical key update is commonly recommended.	Key size of current differential relays is 1.5TB for 20 years maintenance free.	ROM size is limited because HDD cannot be used in relays.

* From [1]

Personal Assessment

- Possible Disadvantages
  - The authentication tag generating function (Eqn 1) is simple (as opposed to HMAC SHA-256) and therefore can be assumed to be known by attacker
  - Security focus shifted almost completely to protection of keys from attackers
    - The keys set in each power system component must be encrypted and possibly itself authenticated when installed into flash memory
    - Abundance and accessibility of smart meters/distributed generators makes them more prone to attacks on the keys
- Large number of keys required for proposed method as compared with HMAC SHA-256 could make their unexpected replacement more cumbersome

Conclusion

- Information-theoretic authentication codes have been introduced and their performance as related to the power system communications evaluated
- Proposed method better meets the power system communication requirements of real-time performance and durability against degradation with time (thereby making long-term maintenance easier)
- Proposed method is also comparatively easy to implement and its deception probability can be controlled and chosen during design stage by power system / communications engineers

References

- T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi, “Information-Theoretic Approach to Authentication Codes for Power System Communications”, IEEE PES Transmission and Distribution Conference, April, 2010.
- T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi, “Information-Theoretic Approach to Authentication Codes for Power System Communications”, PowerPoint Presentation, IEEE PES Transmission and Distribution Conference, April, 2010.
- T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi, “Protection Relay Systems Employing Unconditionally Secure Authentication Codes”, IEEE Bucharest PowerTech, Jully, 2009, 95.
- T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi, “Power system communication and information-theoretic cryptography”, IEEE T&D Asia, October, 2009.

TEXAS A&M UNIVERSITY

Thank You

Questions ???