IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

A MTD Strategy: Secure Spreading Codes for Wireless Communications

Renzo Navas

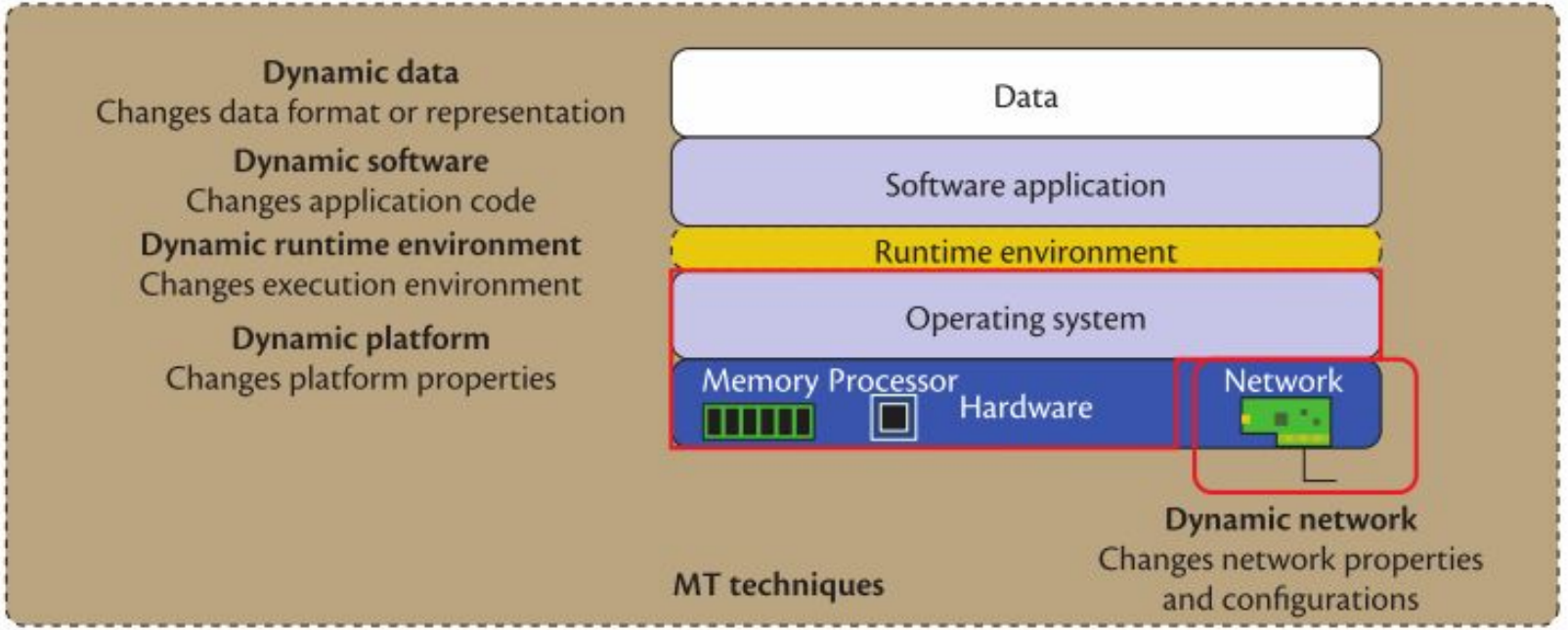
01/01/2018 ASEET Meeting @ Rennes

SUMMARY

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Moving Target Defense (MTD):

Make parts of a system inherently dynamic



Moving-target techniques can be categorized into five different domains according to their place within the execution stack.

Source: Finding Focus in the Blur of Moving-Target Techniques (2014)

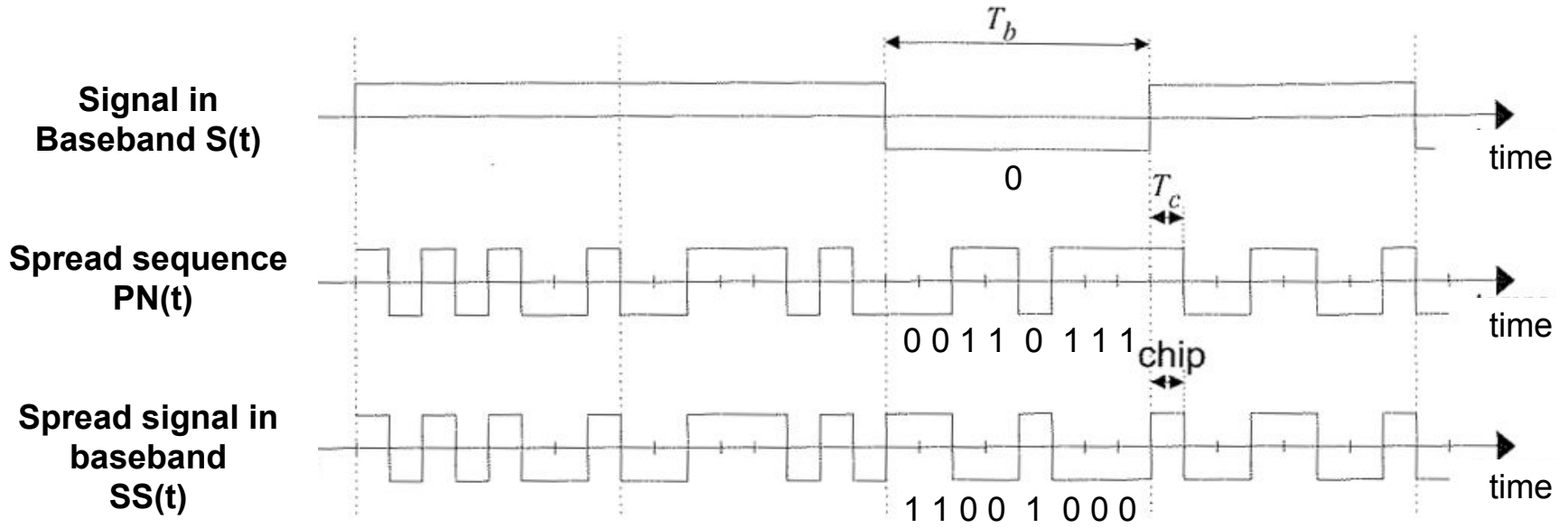
CONTEXT
MTD

- MTD Strategy at the Network Level
- Focus on physical modulation

Direct-Sequence Spread Spectrum (DSSS)

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

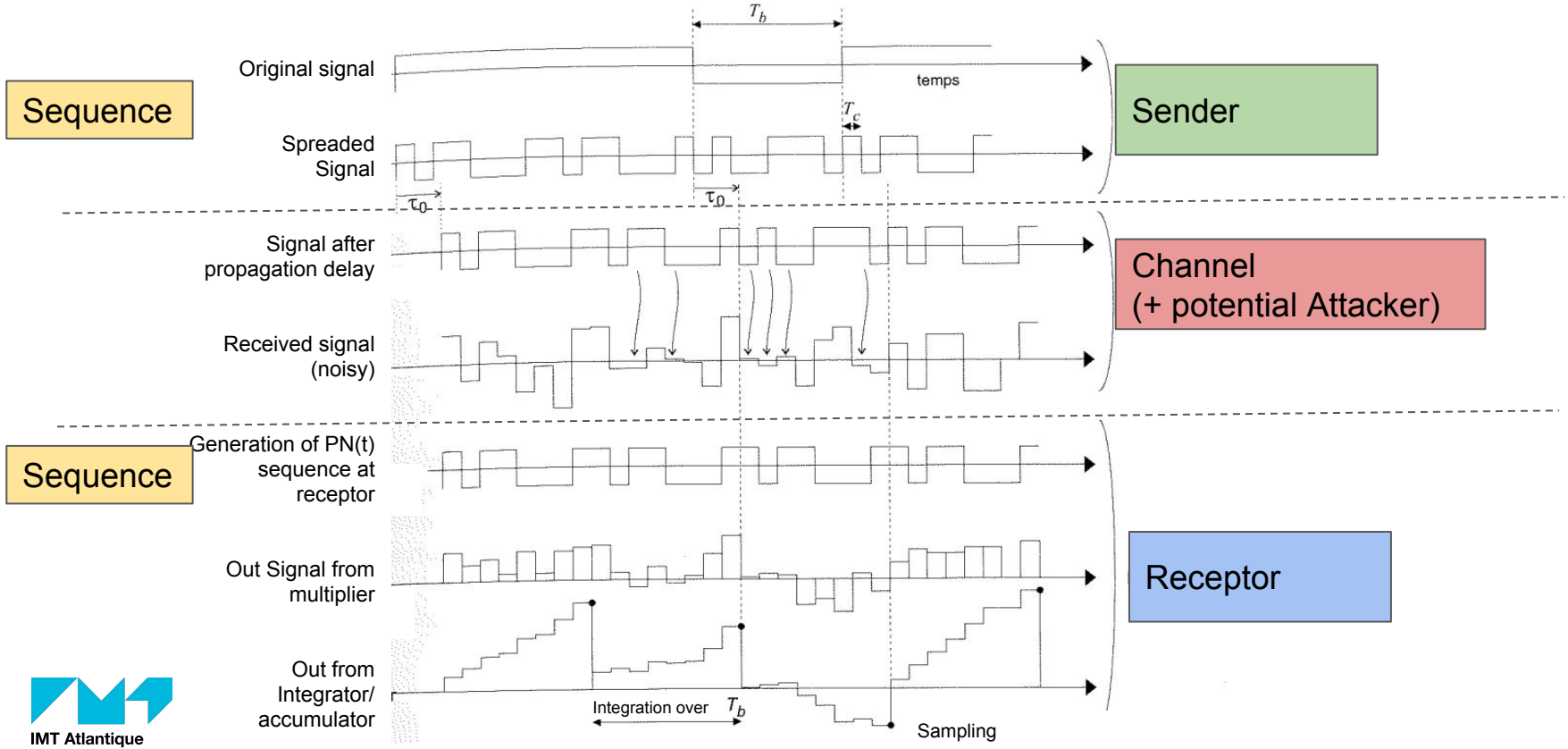
DSSS
Principles



Basic Principle of Direct-Sequence Spread Spectrum

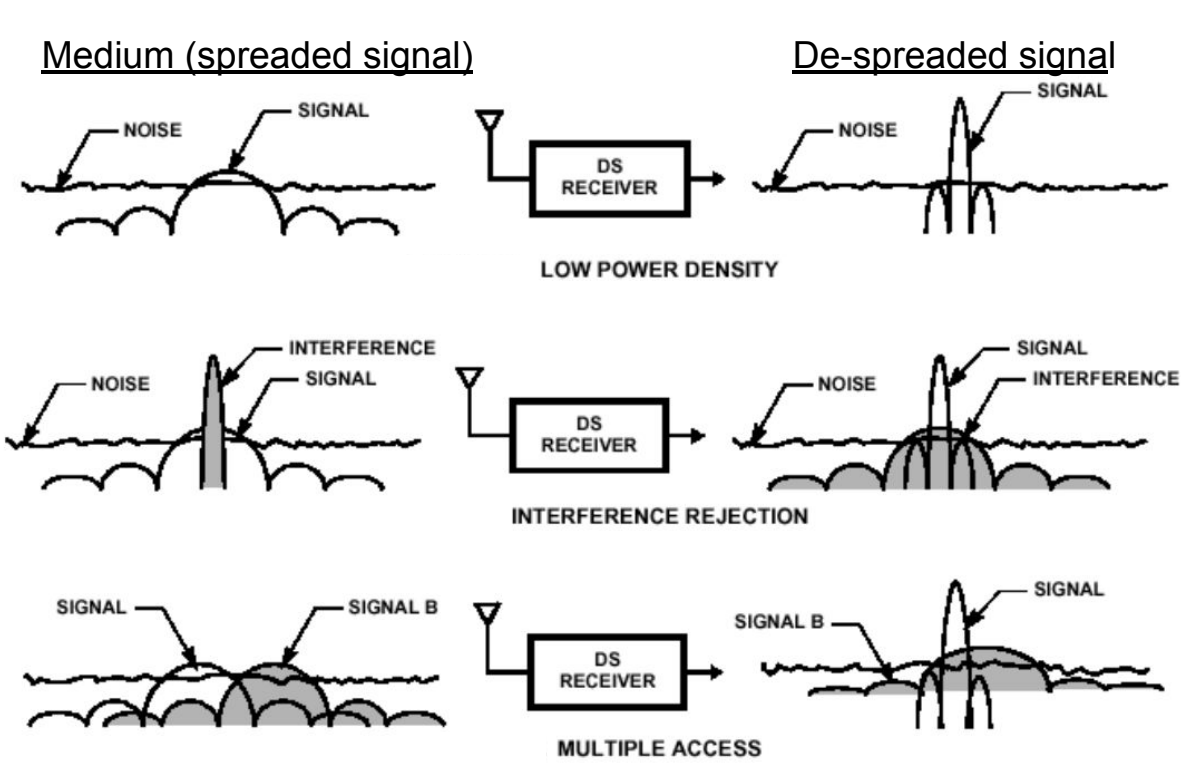
Note: this example shows a Negated XOR (instead of a more common xor). The principle remains the same

DSSS
Principles



Example: reception of a noisy DSSS signal

DSSS
Characteristics



- Wide bandwidth, every component has low signal-to-noise ratio(below 0 dB)
- The signal is “buried in the noise”: difficult to detect with a spectrum analyser.
- Resilient to narrowband interference.
- Resilient to jamming in general: In order to jam it an attacker must know the exact spreading sequence

Sequence sets in wireless communication

Introduction

- What Sequence sets to use? Well-studied problem*
- **Desired Properties** that increase robustness to interference and channel use
  - **Balance** (0s and 1s)
  - **Orthogonality:** Two sequences are orthogonal if the dot product is zero.
  - **Correlation:** Measure of similarity of sequences (f*g)[n]
    - Autocorrelation Function (ACF): Distinguish from a time shifted version of itself
    - Cross-correlation Function (CCF): Distinguish from (possibly a time-shifted version of) every other sequence in the set.

$$(f \star g)[n] \stackrel{\text{def}}{=} \sum_{m=-\infty}^{\infty} f^*[m]\, g[m+n].$$

Discrete cross-correlation

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

* “Sequence sets in Wireless communication Systems: A survey” (2010)

Sequence sets in wireless communication

Hadamard-Walsh

- Examples: Walsh-Hadamard-codes, Gold-codes, Baker Codes, **Pseudo-random sequences.**

  Hadamard Matrix:

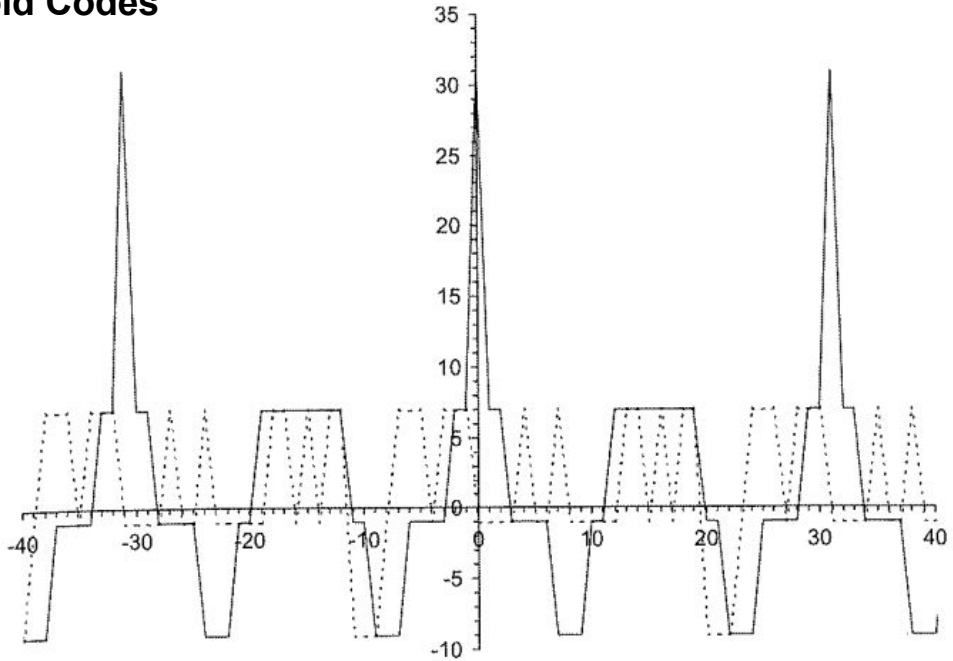
$$H = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & -1 & -1 & +1 & +1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{bmatrix}$$

- All rows are orthogonal (0 cross-correlation)
- … but shifted version of them are not
- A wireless system that uses this sequences set needs to be **synchronized** (e.g. OVSF-CDMA)

Sequence sets in wireless communication

Gold codes

Gold Codes



Correlation and auto-correlation of two Gold codes of 32-bit length

- Auto- and cross- correlation have low values (mathematically bounded).
  - We can isolate the expected signal at the receptor.
- We can use this codes in **asynchronous** systems
- **Drawback**: The set of gold sequences needs to be generated in a **centralized** way.

Sequence sets in wireless communication

What do we want? we want it all...

- **Good auto- and cross correlation** properties
  - Close to theoretical limit (Welch's bound).
- **Asynchronous** Wireless systems
- **Decentralized** and **ad-hoc** generation of the sequences in the set
- …. and **Security**-related properties, Good:
  - Length of sequence codes
  - Size of sets (cardinality)
  - **Randomness** of the codes:
    - Unpredictability of the sequences for an attacker.

Pseudo-random Sequences

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Pseudo-Random Sequences

Goal

Goal: Use Pseudo-Random (PR) Sequences as **secure spreading codes** for wireless communication.

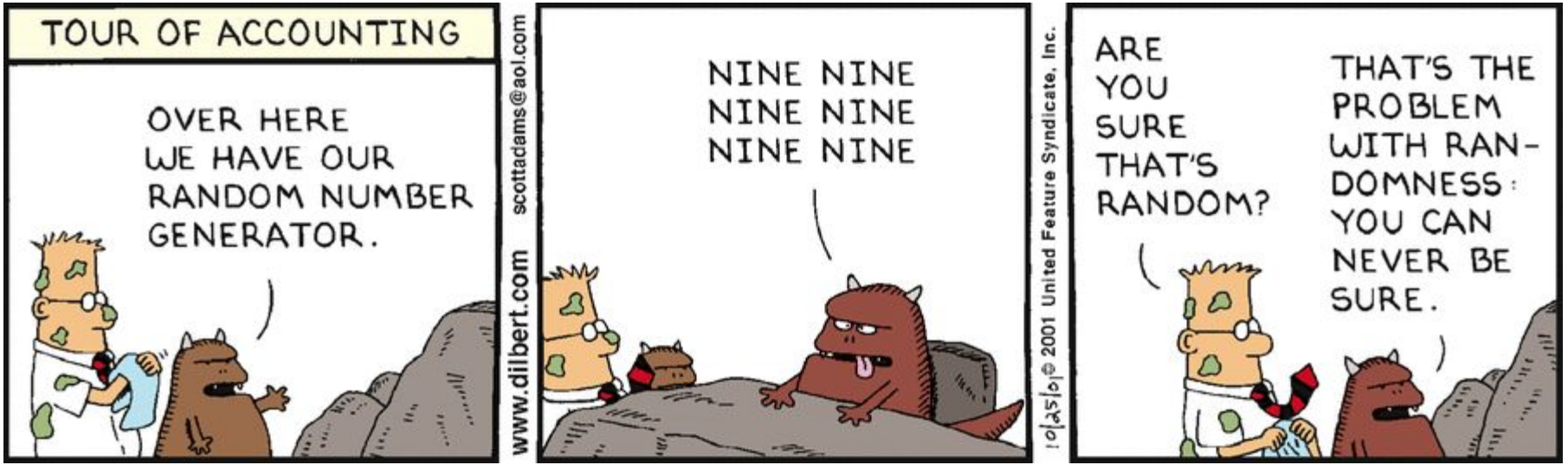
Sub-goals:

- [Wireless Communication] Prove that the pseudo-random sequence sets generated have good correlation properties.

- [Security] Prove that a particular pseudo-random generator has good randomness and cryptographic properties
  - cryptographically secure pseudo-randomness
  - e.g. their output must be unpredictable in the absence of knowledge of the inputs

Pseudo-Random Sequences

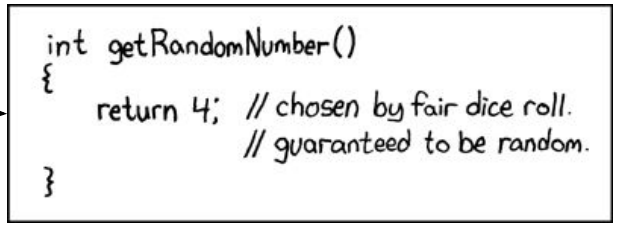
The quest for randomness



Pseudo-Random Sequences

The quest for randomness: Randomness Testing

- Golomb's postulates (necessary conditions, not sufficient)
  - Balance Property (1s and 0s differ at most by 1)
  - *Run* property
    - Run: a set of consecutive 0s or 1s. Half the runs have length 1, one-fourth have length 2, one-eighth have length 3, etc. (~Binomial distribution)
  - Ideal 2-level Autocorrelation
- Kolmogorov complexity
  - "The length of the shortest computer program that produces the object as output"
- Estimated Linear Complexity
  - Shortest LFSR that generates the sequence
- NIST SP 800-22 Test suite
  - "A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications"
  - **Statistical testing cannot serve as a substitute for cryptanalysis!**



Pseudo-Random Sequences

Brief State-of-the-Art of PR Generators for Wireless Communication

- Linear Feedback Shift Registers (LFSR)
  - Binary maximal-length sequences (m-sequences)
    - Gold Codes, Kasami Codes
  - Low complexity (good for speed HW, not so for security)
  - Small number of sequences (Bad for security)
- Non-Linear Feedback Shift Register (NLFSR)
  - e.g. Non-linear Maximal-Length, Bent sequences, De Bruijn sequences.
  - Non-linear boolean functions: better for security.
- Others (e.g. Barker codes, Low Correlation Zone ...)

Proposal

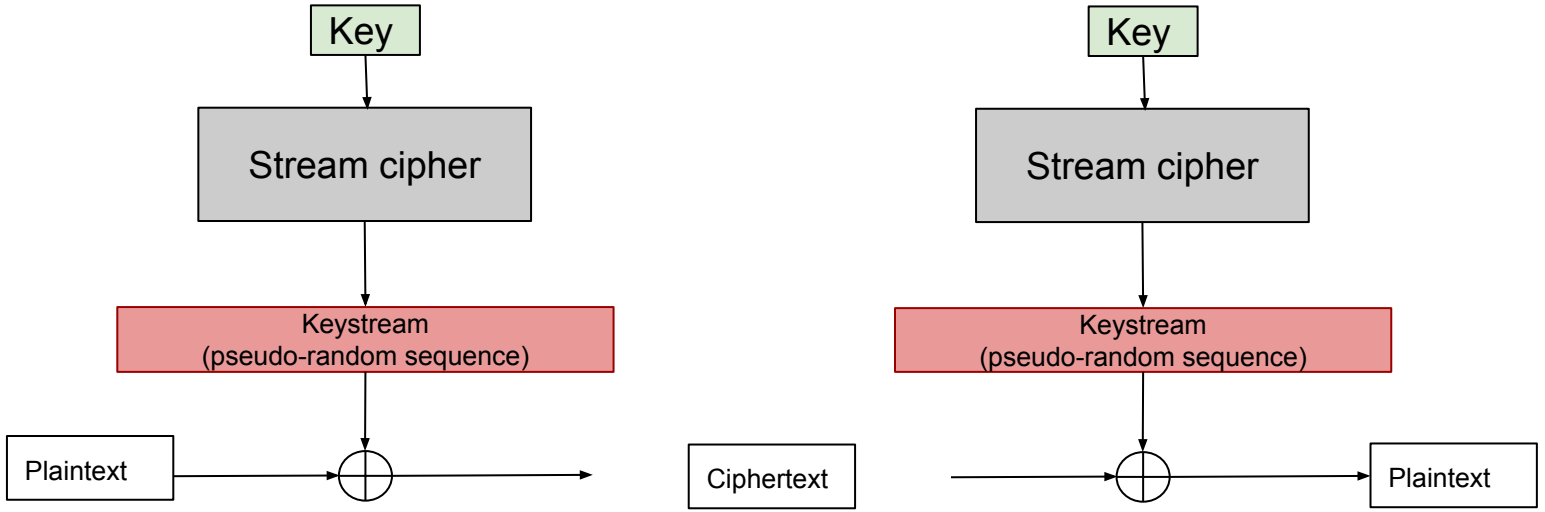
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Proposal
In two lines

Use **stream ciphers** for the generation of pseudo-random sequences sets for DSSS-modulation

Proposal

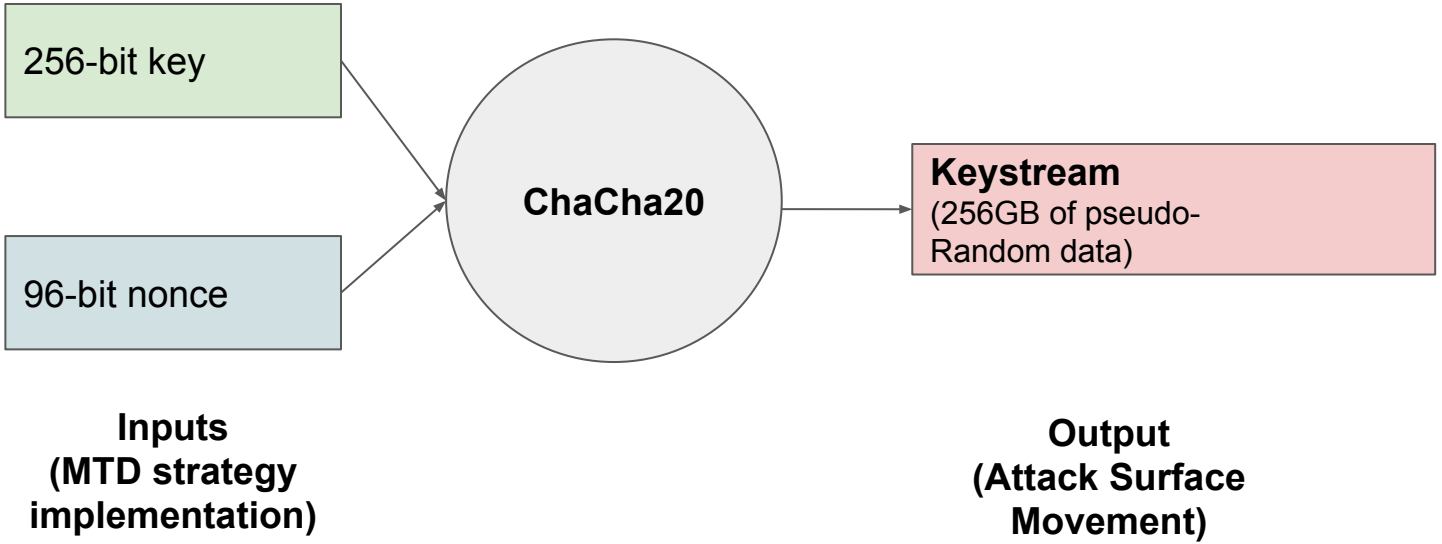
Stream-cipher high level (Approximating the one-time pad)



Proposal

Rationale and ChaCha20

- Use state-of-the-art IoT friendly stream-ciphers (for MTD strategy)
  - We study ChaCha20 (and AES in CTR mode)
  - The security of our proposal relies on the cryptanalysis of the used cipher.
  - Why not use Key Derivation Functions (KDF)? We can (but more complex).



Empirical Results

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Measurements

Recap:

Two sub-goals:

- [Wireless Communication] Prove that the pseudo-random sequence sets generated have good correlation properties.

- [Security] Prove that a particular pseudo-random generator has good randomness and cryptographic properties
  - i.e. cryptographically secure pseudo-randomness
  - e.g. their output must be unpredictable in the absence of knowledge of the inputs

Measurements
Cross-correlation

Python Code:

- ChaCha20 and AES-CTR codes set generation
  - Code lengths of 128, 256, 512, 768 and 1024 bits
    - (we truncate the output to match those lengths)
  - One set of 1024 codes for each bit length.
    - Generated with input key from 0 to 1024 (…)

Sequence Sets Generation

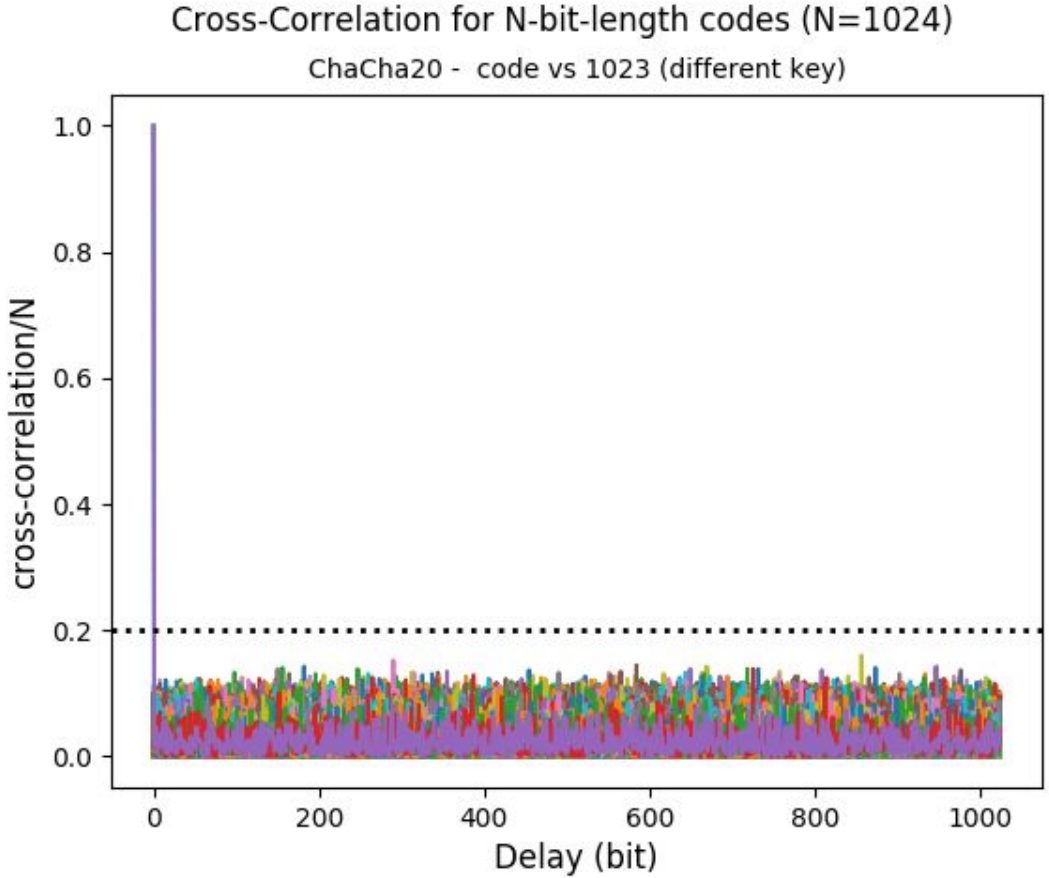
- Cross-correlation analysis
  - Normalized cross correlation
  - Used fast fourier transform instead of cross-correlation.
    - migrate to MATLAB?
  - Cross-correlation vs. every time-shifted version of every other code

Sequence Sets Analysis

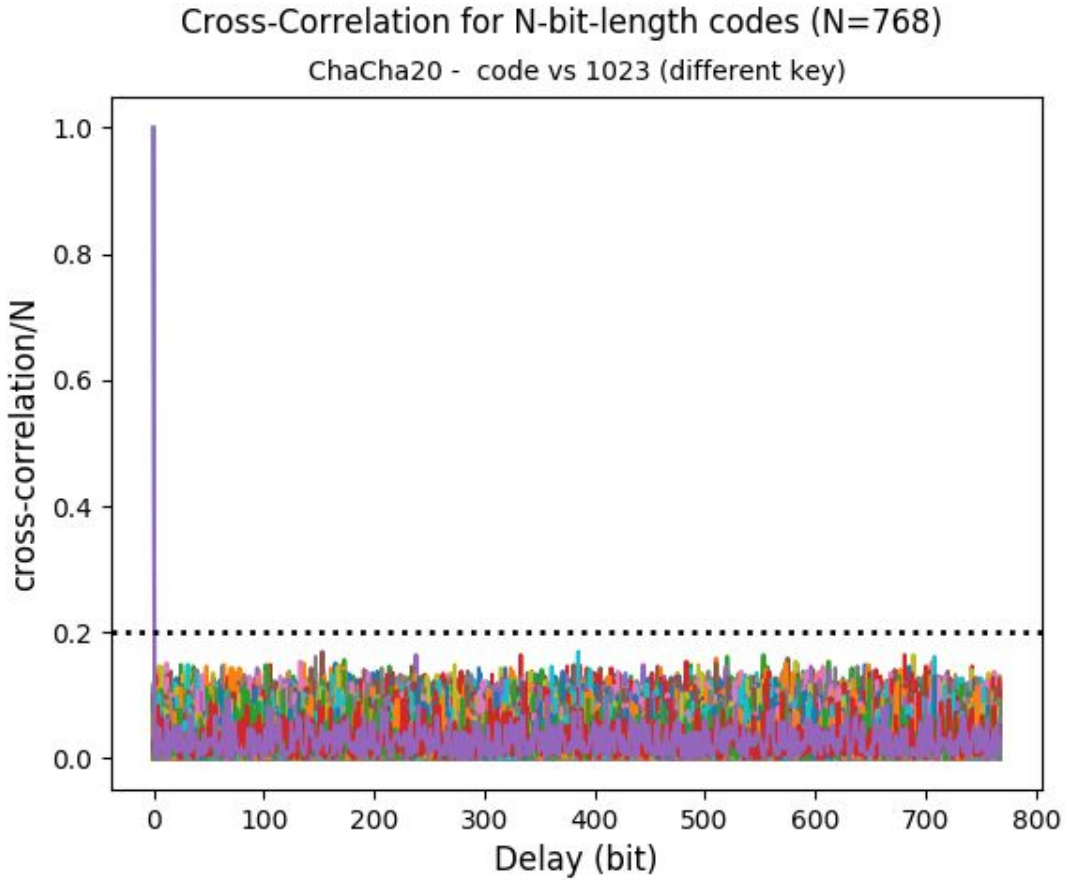
Visualising Cross and Auto-correlation for one code

vs every other code in the 1024 set (and for every time-shifted version of it)

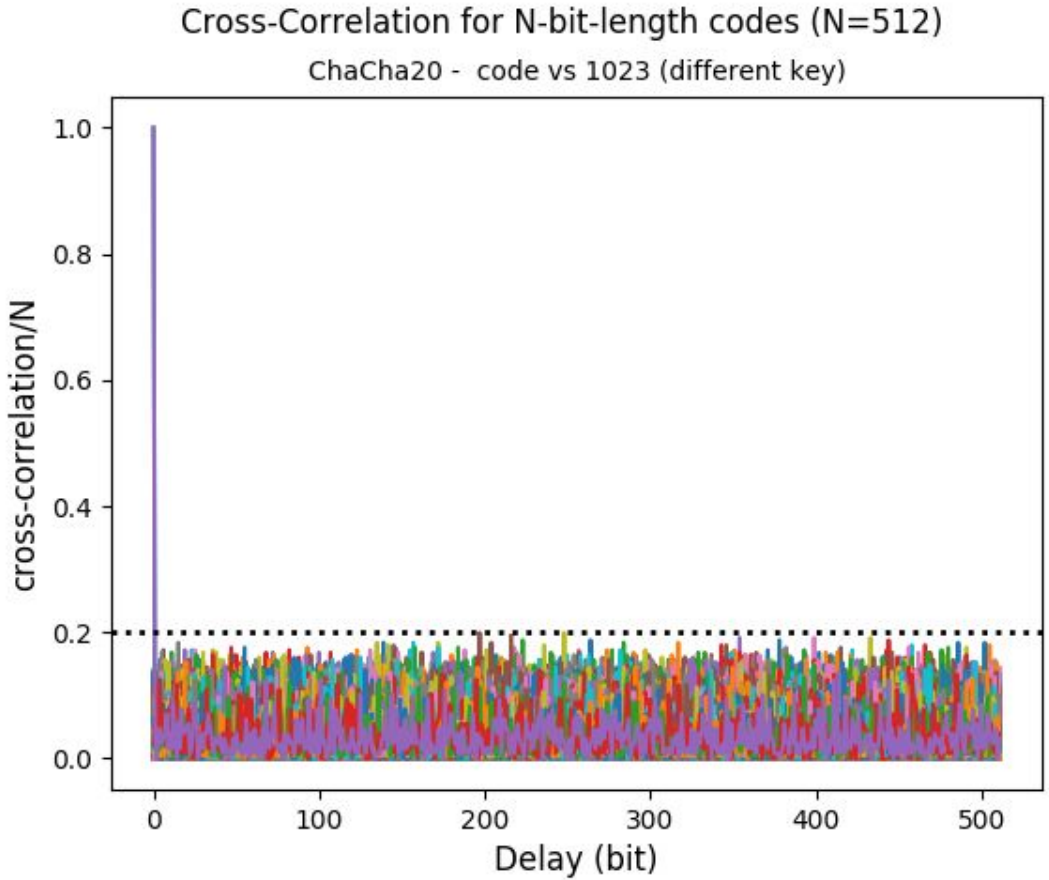
Measurements
Cross-correlation



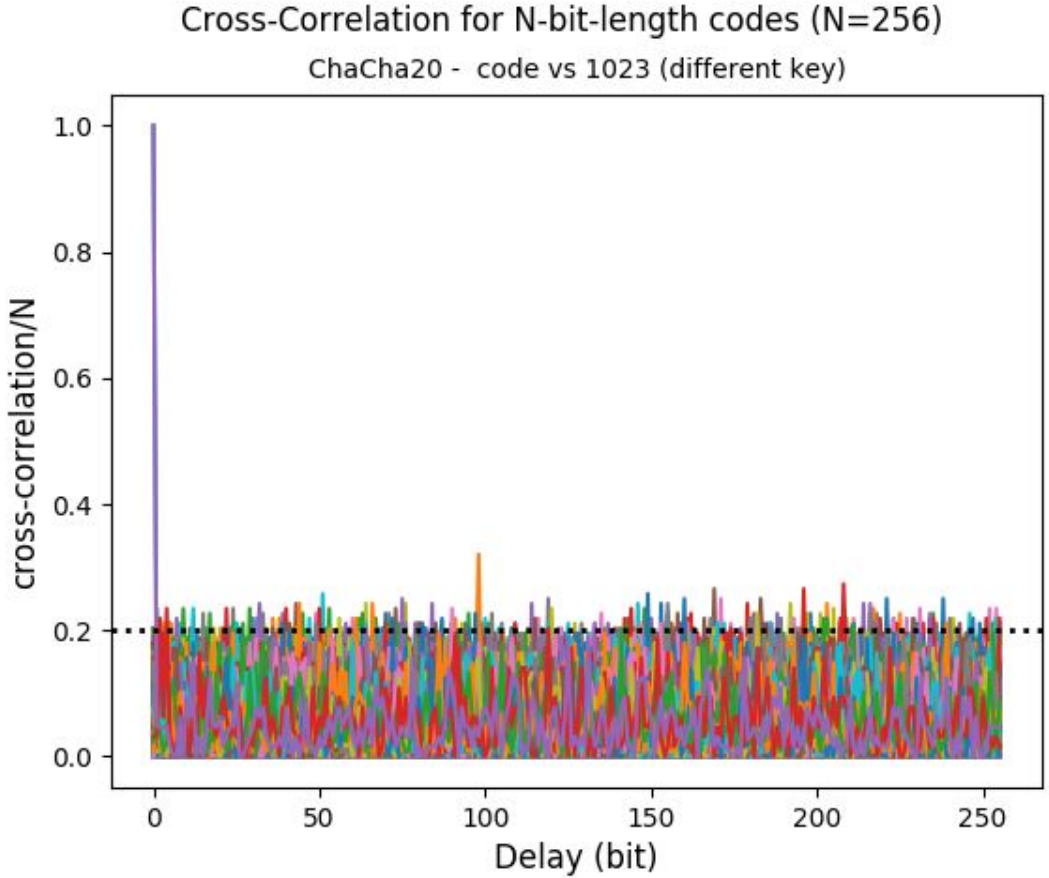
Measurements
Cross-correlation



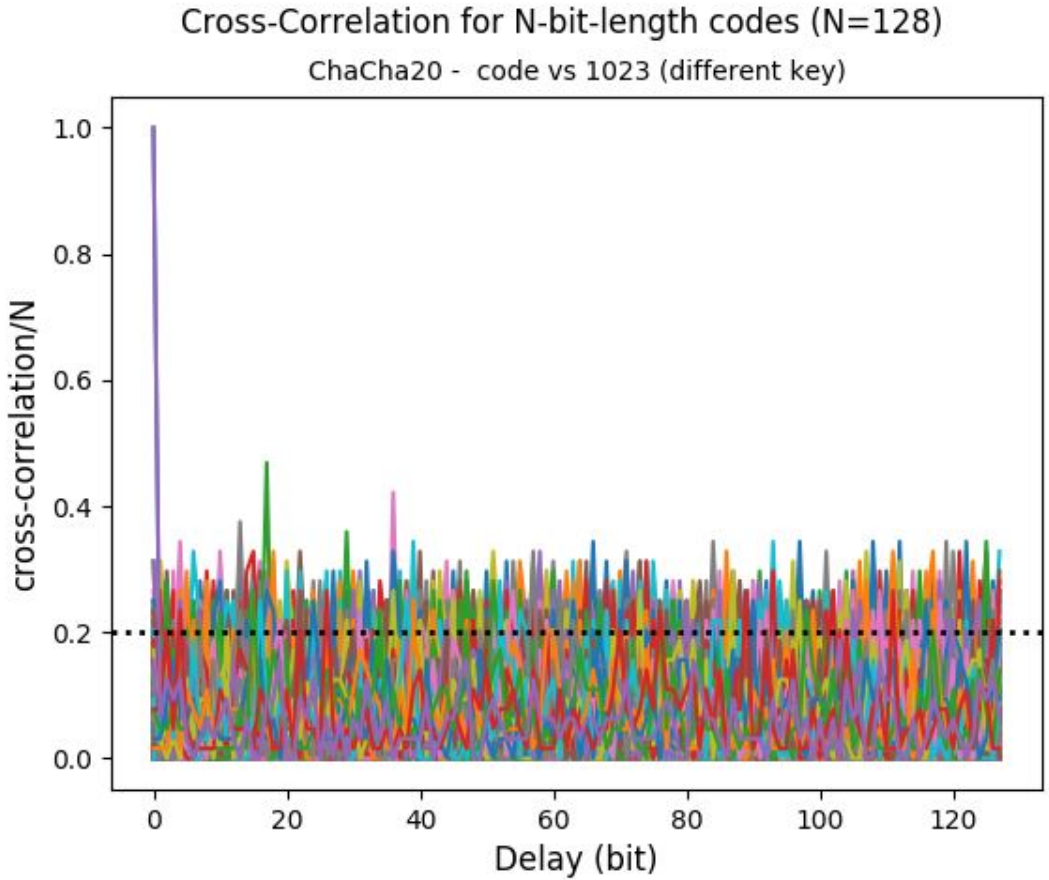
Measurements
Cross-correlation



Measurements
Cross-correlation

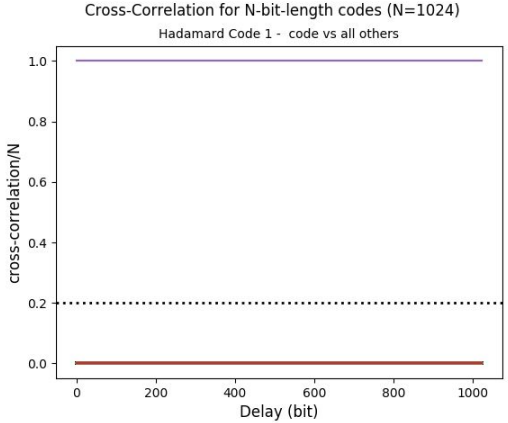


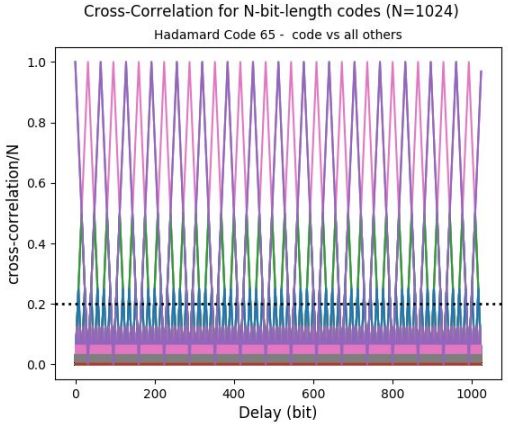
Measurements
Cross-correlation

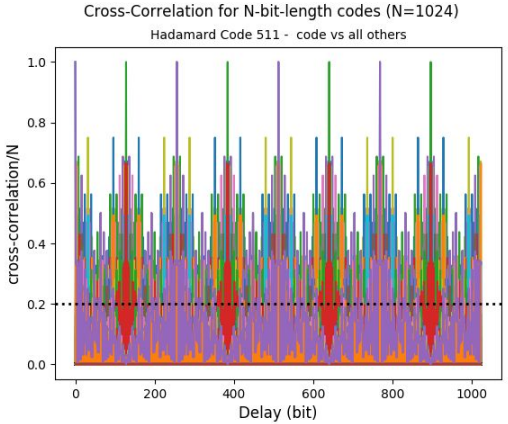


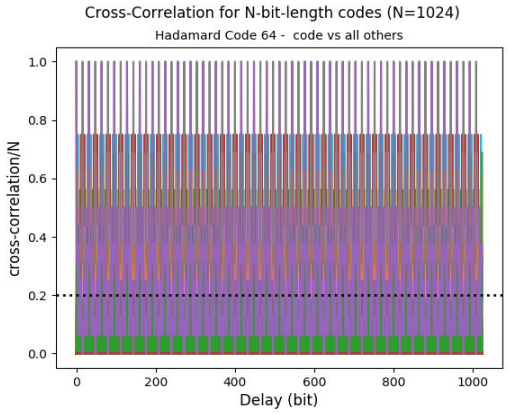
Measurements

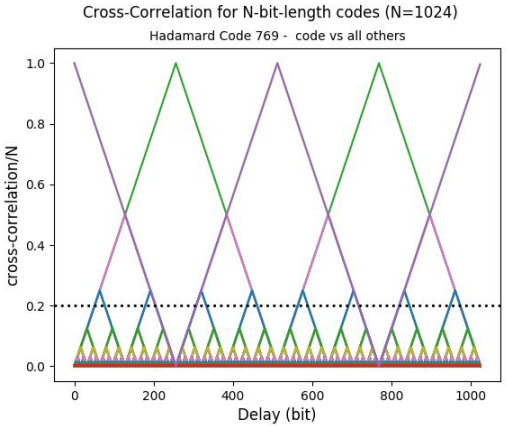
Cross-correlation: Haddamard Codes Visual Example

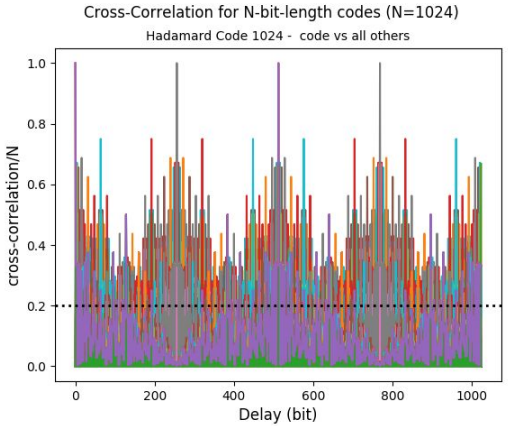












Measurements

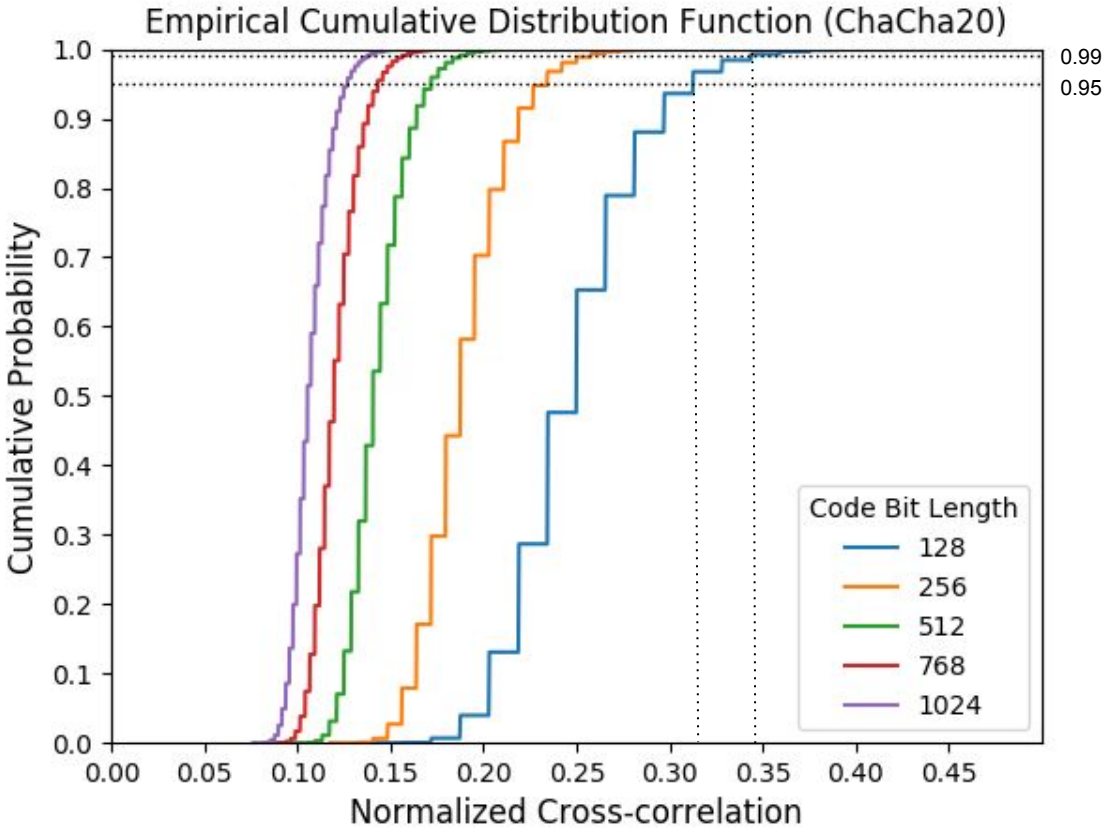
Cross-correlation

- We want statistically relevant results
- For each set, and for every possible combination of pair of codes* calculate the maximum cross-correlation
- Plot: Empirical Cumulative Distribution Function

* 523776 combinations for a set of 1024

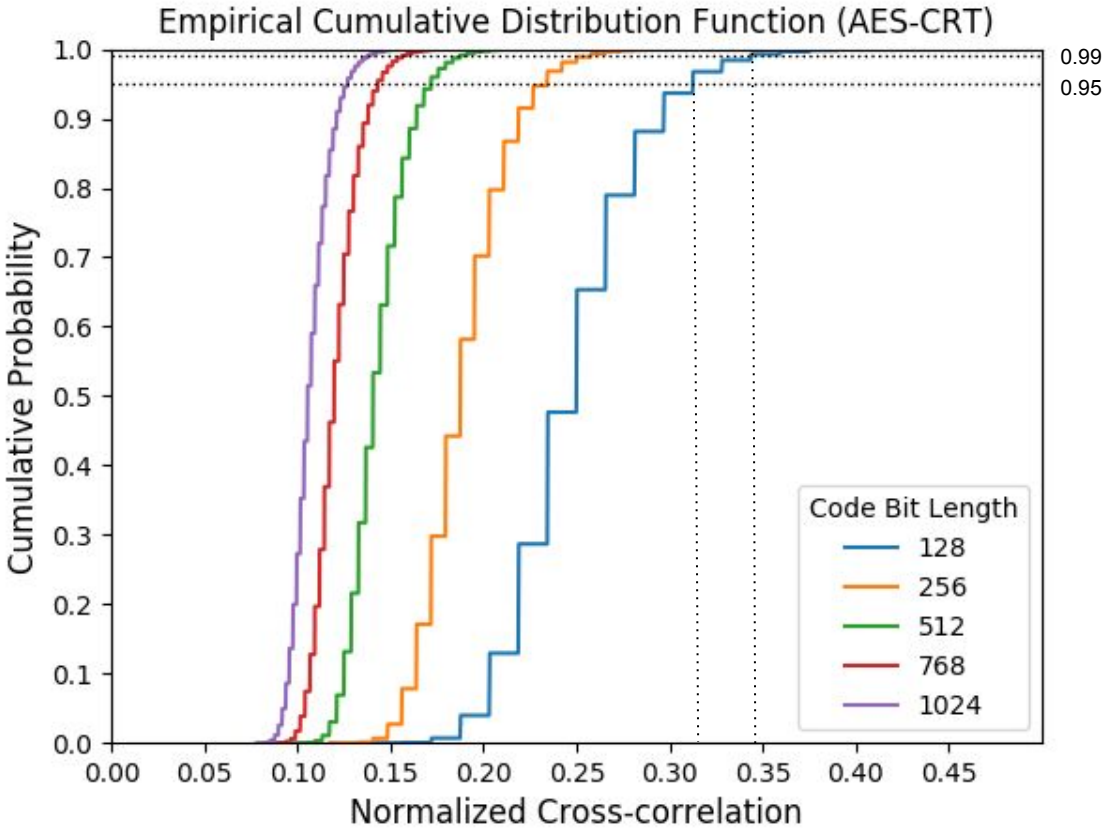
Measurements

Cross-correlation



Measurements

Cross-correlation



Measurements
Partial conclusions

Sequence sets of cardinality 1024 ~~randomly~~ generated with Chacha20 and AES-CTR:

- Have bounded and acceptable auto and cross- correlation values.
- The longer the sequences the lower the correlation values.
- … seem to be good candidates for our purposes.
  - We will need to have more statistically relevant results

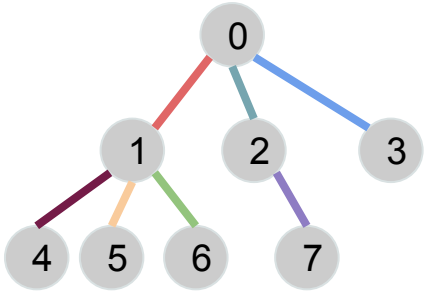
Current and Future Work

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Concrete MTD Strategy: MTD for DSSS Modulation

1. Key Bootstrapping: Authenticated Key Establishment
   - Ephemeral Diffie-Hellman Over COSE (EDHOC): 3 Messages
   - Hypothesis: the medium is not being jammed (rendeszvous modulation), or we rely on keyless jam resistance techniques (e.g. UDSSS)
   - Derived work: We can envisage group keys (trade off: resilience vs simplicity)

2. **DSSS Code derivation (what I presented today) and rotation**
   - Use stream ciphers to derive PN codes (TODO: strengthen statistical analysis)
   - MTD Strategy
     - Define the strategy to “move” codes
       - When? e.g. Fixed frequency of change
       - How? e.g. Nonce increment, key renegotiation.



Possible work to explore for current solution:

- Comparison of different PRNG (e.g HKDF, eStream Portfolio)
  - Speed (HW SW), Resources (RAM ROM CPU), Security analysis.

- Code length impact on system characteristics
  - Throughput, Robustness (cross correlation, gain -range-)
    - (MATLAB model?)
  - Resilience (attacker effort); Leverage on attacker models on jam biblio.

- Solution prototype on SDR (cognitive radio)
  - (... I -gladly- need to learn more signal processing basics)

Future: Generic proposal

MTD for IoT

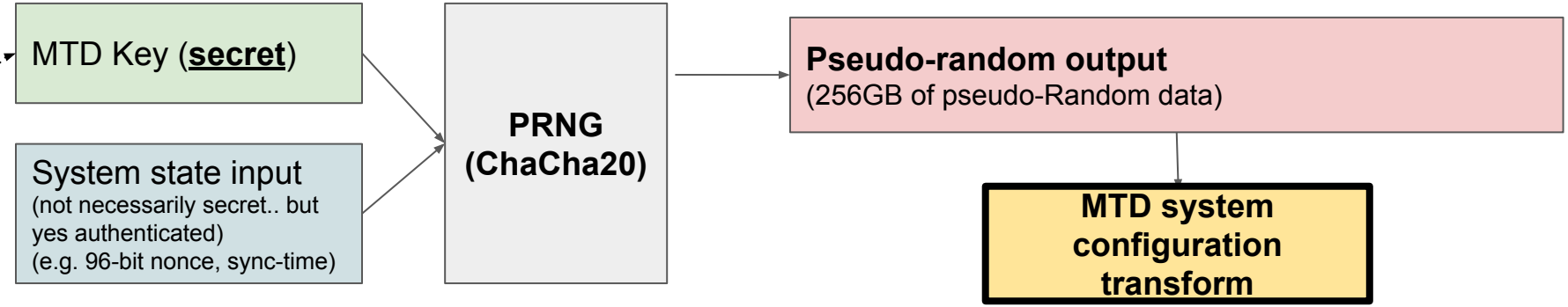
Current Vision: Generic solution

- Apply same method to (potentially) configure any component of any system
- Good randomness and security properties of PRNG and keystream is fundamental
  - This work can be leveraged on the designers/bibliography of the PRNG :)
- Map the pseudo-random output to a concrete description/configuration of the system.
  - MTD security (attack surface movement) depends on cardinality of possible configuration states.

MTD for IoT

Current Vision: Generic solution

- A generic MTD system configuration generator



Inputs (MTD strategy)

The only secret information on the system. (Kerchkoff's priciple)

… ***2^256GB*** *(cryptographically random) possible outputs, enough to pseudorandomly configure any parameter/s of a system.* Examples:

- IPv6 Address (2^128 space); Port Hopping
- DSSS 1024-bit length Codes (2^1024 space)
- Frequency Hopping schedule
- Key to randomize RAM object allocation
- Key to encrypt App. layer information

Output (Attack Surface Movement)

KISS design principle: "Keep it simple, stupid"

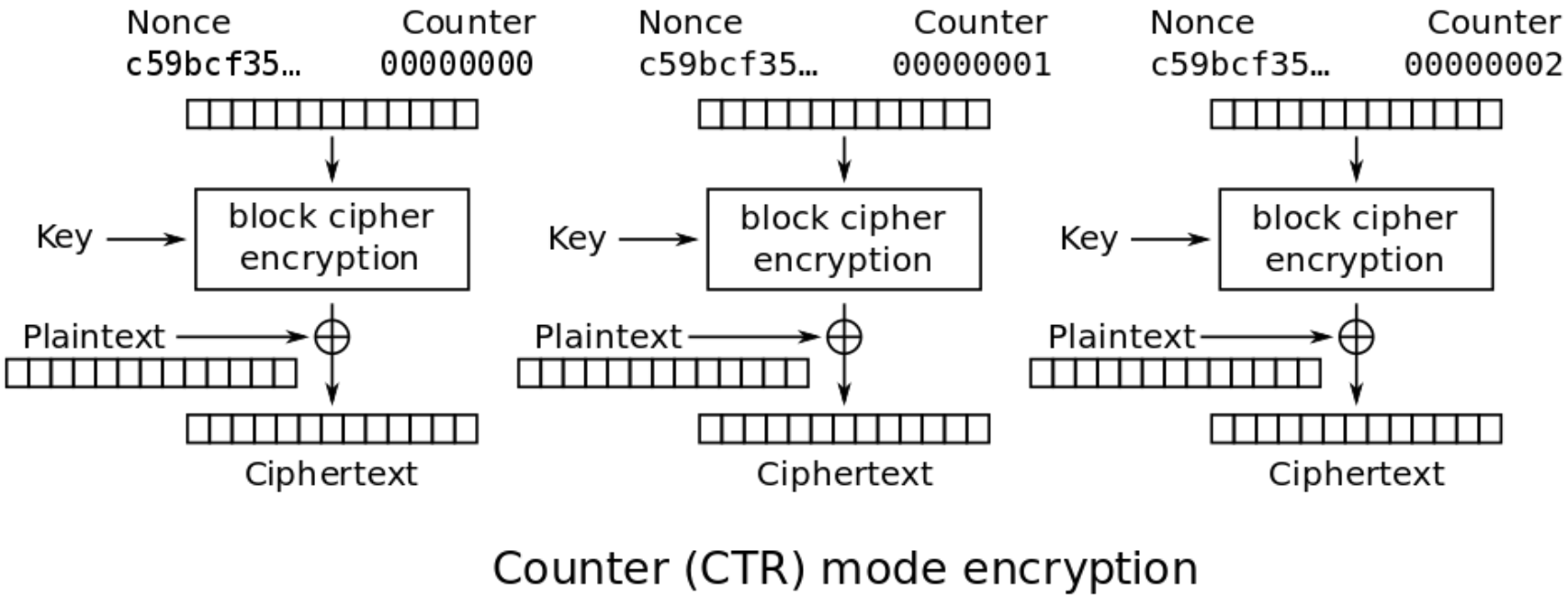
"It seems that perfection is reached not when there is nothing left to add, but when there is nothing left to take away"
A. Saint-Exupéry

Thank you!
Discussion

Appendix

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

AES-CTR mode
(AES-CCM uses AES-CTR mode)

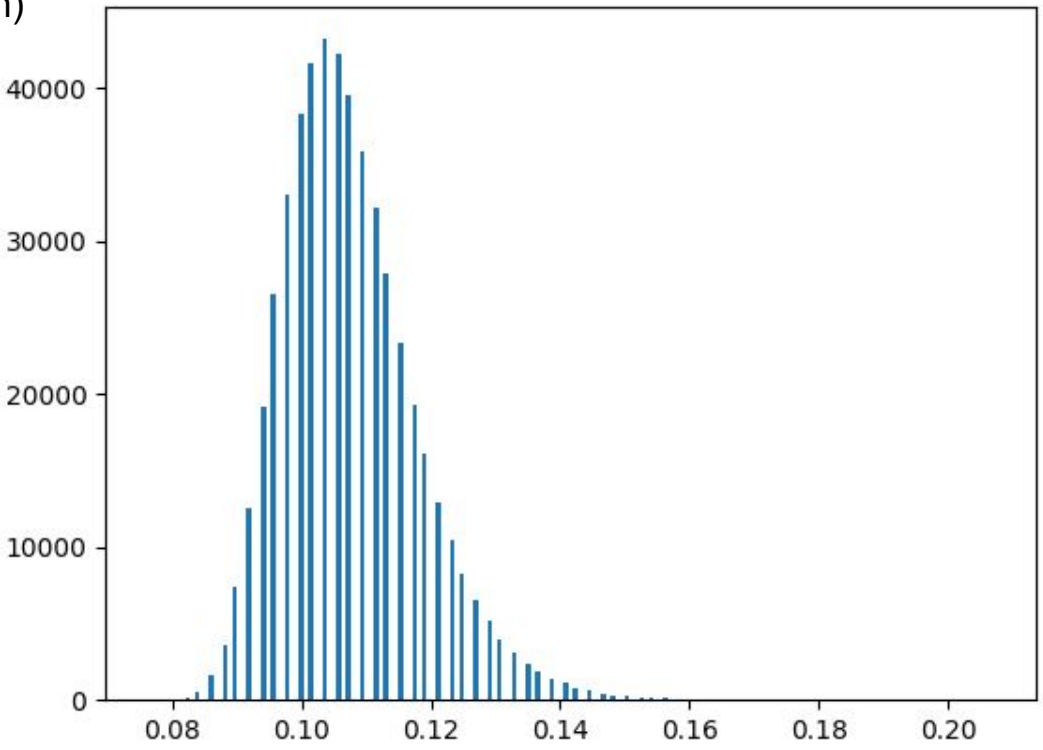


Counter (CTR) mode encryption

Measurements

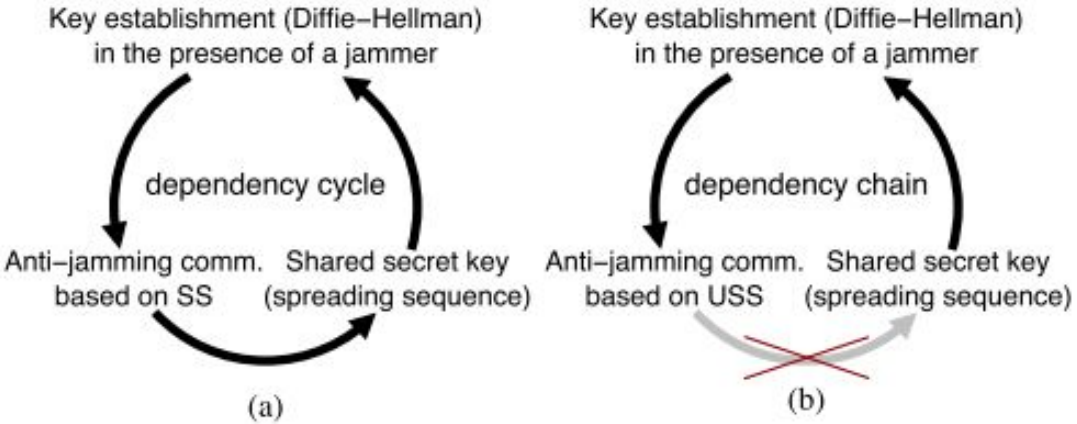
Cross-correlation

Histogram for cross-correlation of every pair of code in a 1024 code set (~500.000)
(1024-bit length)



Problem: Bootstrapping modulation in presence of Jammers

- Not our problem, leverage on bibliography
  - “Zero Pre-shared Secret Key Establishment in the Presence of Jammers” Tao Jin 2009
  - “Keyless jam resistance” L. Baird 2007
  - “Anti-jamming broadcast communication using uncoordinated spread spectrum techniques” C Pöpper 2010

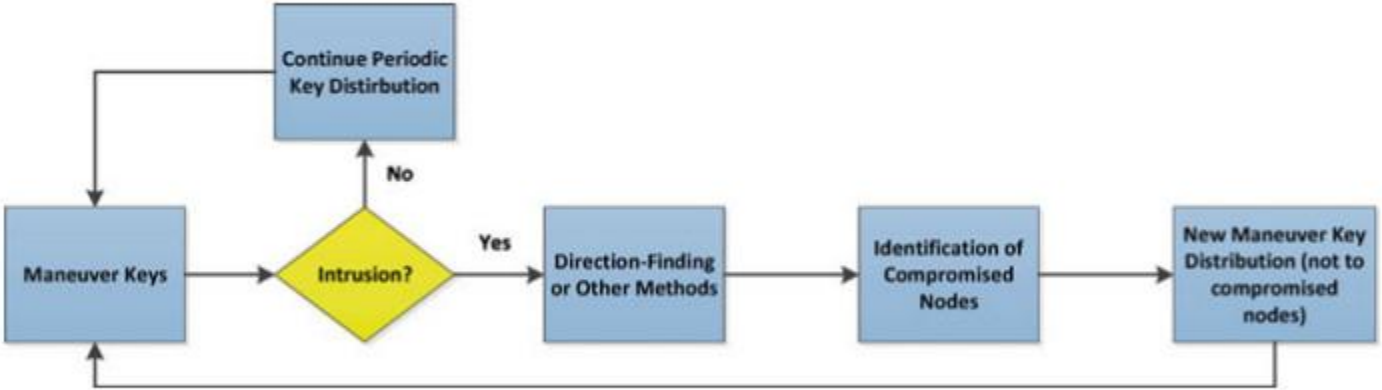


DSSS and MTD: Justification

- Cyber Maneuver Against External Adversaries and Compromised Nodes
  - MTD II Book (2013) . Don Torrieri (US Army Research Laboratory)

> This article identifies the research issues and challenges from jamming and other attacks by external sources and insiders. Based on the spirit of **cyber maneuver**, it proposes a general framework to deal with such issues. Central to our framework is the notion of **maneuver keys as spread-spectrum keys**; they supplement the higher-level network cryptographic keys and provide the means to resist and respond to external and insider attacks.

DSSS and MTD: Justification



Our framework for attacker identification and maneuver-key updating

DSSS and MTD: Justification

- They do not get into the details. Starting point for our solution
- Conclusion:

> This article identified the research issues and challenges from jamming and other attacks by external adversaries and compromised nodes. Based on the spirit of cyber maneuver, it proposes a general framework to deal with such issues. The framework includes components for attack detection, identification of compromised nodes, and group rekeying in the presence of jamming. Some future research is to **(1) do detailed designs of each component in the framework,** and **(2) implement and evaluate both the security and performance of each component** as well as the entire system