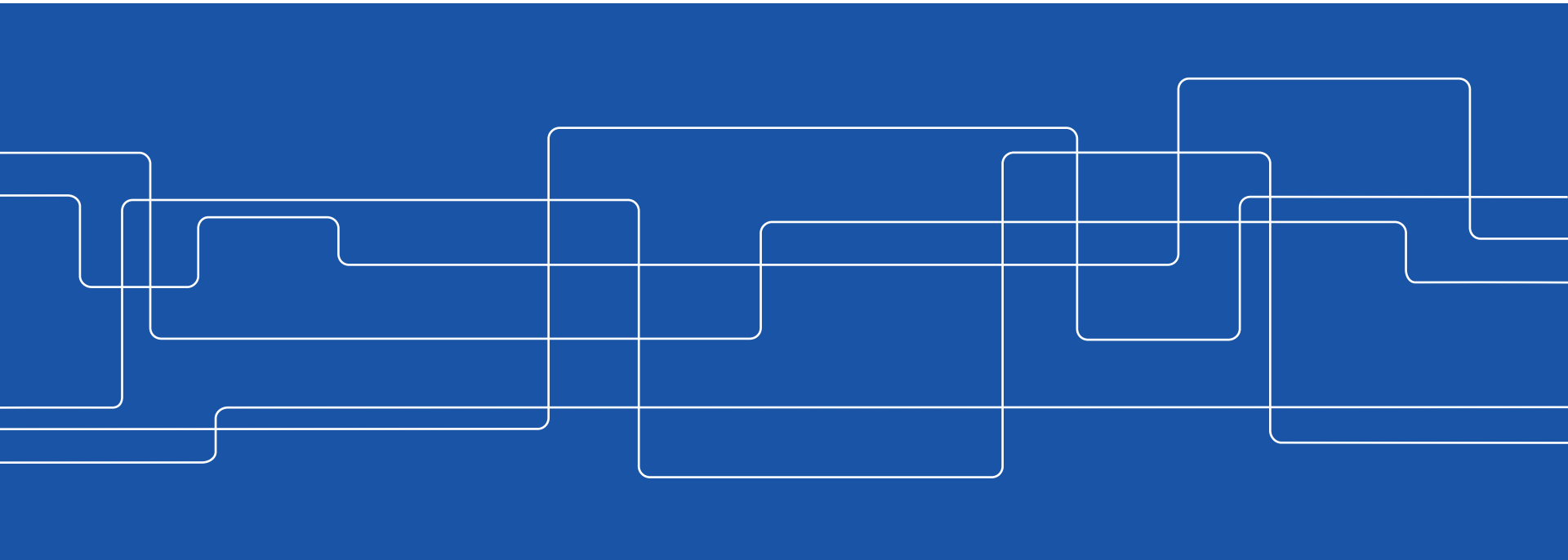
Bringing Reliability and Security Together: Challenges and Opportunities

Elena Dubrova
Department of Electronics
School of ICT, KTH



Overview

- Motivation
- Opportunities
  - How reliability and security techniques can be combined to protect resource-constrained IoT devices with a minimum overhead
- Challenges
- Summary

In the near future …

- **Millions** *not so well protected* Internet-connected "smart" devices will contain private data or be involved in services related to sensitive information
  - E-health
  - Wearables
  - Smart home
  - Connected cars
  - …
- Attack surface of future networks is expected to be enormous

First cyberattack based on Internet-connected home appliances

- Between Dec. 23, 2013 and Jan 6, 2014, more than 100.000 “smart” home appliances were used to send out more than 750.000 malicious emails targeting enterprises and individuals worldwide [1]
  - home-networking routers, connected multi-medial centers, TVs, at least one refrigerator
- No more than 10 emails were initiated from any single IP address, making the attack difficult to block based on location

Massive distributed denial-of-service attack involving IoT devices, Oct 21, 2016

EKONOMI 21 oktober 2016 20:59

”Troligen ingen attack mot Sverige”

De stora internetproblemen i Sverige beror troligen inte på att en överbelastningsattack riktats hit, enligt MSB. Snarare är det efterdyningarna av en stor attack i USA som ställer till det.

Under fredagskvällen drabbades en rad svenska webbplatser av internetproblem med resultatet av att det inte gick att komma in på dem. Bland annat påverkades regeringens webbplats. Myndigheten för samhällsskydd och beredskap (MSB) drabbades också.

Do we need to protect low-cost IoT devices?

ANDY GREENBERG SECURITY 08.11.15 7:00 AM

HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET

Cars hacked through wireless tire sensors

Researchers have shown that the tire pressure monitoring sensors found in new ...

PETER BRIGHT - 8/10/2010, 1

The price of wearable craze: Personal health data hacks

Your personal health information is about 10 times more valuable than a stolen credit card number on the black market.

Maggie Overfelt, special to CNBC.com
Saturday, 12 Dec 2015 | 5:05 PM ET

How to protect low-cost IoT devices with a minimum overhead?

- A low-cost connected device can be used as a stepping stone for attacking the network
- Many low-cost IoT devices (sensors, RFID tags) cannot afford more than a few hundred gates for implementing security functionality
  - We can minimize overhead by re-using existing functionality
    - e.g. combine error detection/correction mechanisms with data integrity protection

Message Transmission (LTE view)

Transmitter

Receiver

CRC (Cyclic Redundancy Check)

- Intended for detection of random transmission errors

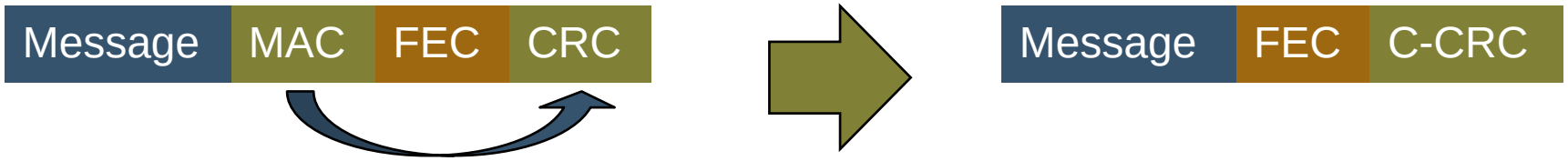
FEC (Forward Error Correction)

- Intended for correction of random transmission errors

MAC (Message Authentication Code)

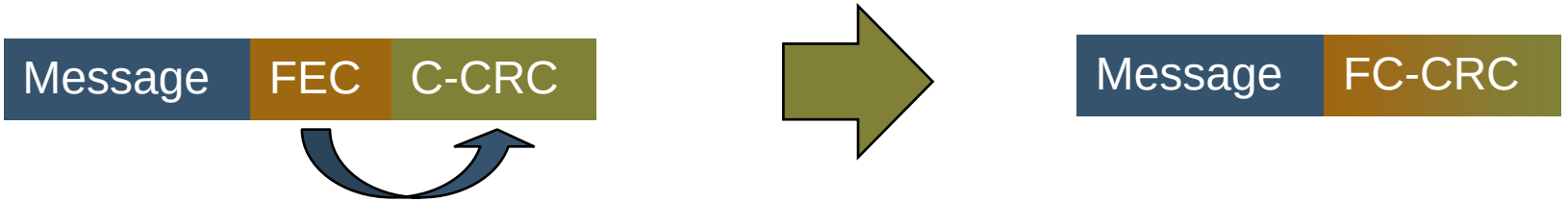
- Intended to confirm that the message came from the stated sender (its authenticity) and has not been changed in transit (its integrity)

Intuitive Idea



Combine MAC and CRC => reduce bandwidth

=> re-use CRC/MAC encoding/decoding engine



Combine FEC and C-CRC => reduce bandwidth

- Alternatively, add cheap FEC to links that have none

Background
Cyclic Redundancy Check (CRC)

- For an m-bit binary message M, let $M(x) = \Sigma_i m_i x^i$ be its encoding as a polynomial over the Galois Field GF(2)

  1 1 0 0 1

  $x^4\ x^3 \qquad x^0 \Rightarrow M(x) = x^4 + x^3 + 1$

- Let g(x) be a polynomial over GF(2) of degree n
- Define

  $CRC_{g(x)}(M) = M(x) \cdot x^n \bmod g(x)$

$g(x) = x + 1 \Rightarrow CRC_{g(x)}(M) = (x^4 + x^3 + 1)\cdot x \bmod x+1$

$= x^5 + x^4 + x \bmod x+1$

$= x$

CRC Properties

- n-bit CRC detects:
  - All burst errors of length n or less
- CRC does not withstand “crafted” error, only random ones
  - An adversary who knows the generator polynomial g(x) can compute $CRC_{g(x)}(M)$ for any M

Cryptographic CRC

Krawczyk (1994)

Theorem: If g(x) is *irreducible*, then

$$H = \{ CRC_{g(x)}(M) = M(x)\, x^n \bmod g(x) \}$$

is ε-otp-secure with $\varepsilon = (m+n)2^{-(n-1)}$

$\Rightarrow$ No adversary that sees M and its hash tag $t = h(M) \oplus r$ can generate M' with valid tag t' with probability higher than ε, where r is a random pad

Cryptographic CRC

- h(M) has to be encrypted as h(M) $\oplus$ r with a random pad r to prevent the injection of all-0 messages
  - $CRC_{g(x)}(0) = 0$, independently of g(x)
- Multiplication by x^n is important, otherwise flips in n least significant bits of message and tag will go undetected

New Cryptographic CRCs

- We introduced two new families of cryptographic CRCs:
  - g(x) is a product of irreducible polynomials, with $\varepsilon = (m+n)^2\ 2^{-n}$
  - g(x) is a random polynomial with non-0 constant term
- Burst errors of MAC size are guaranteed to be detected
- Less resources are required for the implementation
  - Irreducibility tests have $O(n^3)$ complexity
- Proofs of security are given in [2] and [3]

Implementation Details

- LFSRs with programmable connections should be used for computing cryptographic CRC encoding/decoding
- New generator polynomial g(x) should be used for each session
- New pseudo-random pad r should used for each message (can be generated using a stream cipher)

Comparison of crypto-CRC to KMAC (65 nm CMOS, 128-bit key, 128-bit MAC)

	Area, μm^2	Through put, Gbit/s	Throughput per Area, bit/(s*μm^2)	Energy per bit, pJ
KMAC 128	101968	1.28	12553	0.30
CRC 128	3177	1.28	402941	0.01

32 times smaller

30 times more energy efficient

Error-Correcting MAC

- Previous crypto-CRC and other MACs cannot correct errors
- If MAC verification fails, the message is discarded and a retransmission is requested
- Re-transmissions waste energy and increase average packet latency
- Excessive re-transmissions may lead to network congestion

Error-Correcting MAC

- We introduced a MAC which efficiently combines integrity protection with single-bit error correction [4]
  - Detects burst errors of MAC size - 1
  - Does not require irreducibility tests
  - Provable secure with $\varepsilon = m\, 2^{-(n-2)}$
  - Efficient to implement

Bandwidth Gain (LTE view)

Payload

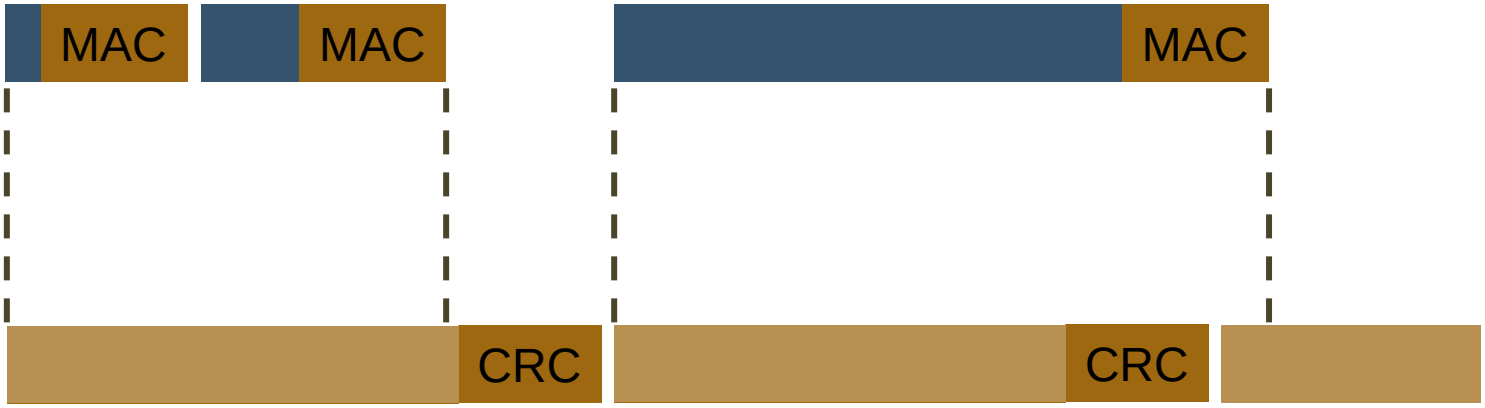
MAC — LTE MAC, 32 bits

CRC — LTE CRC, 24 bits

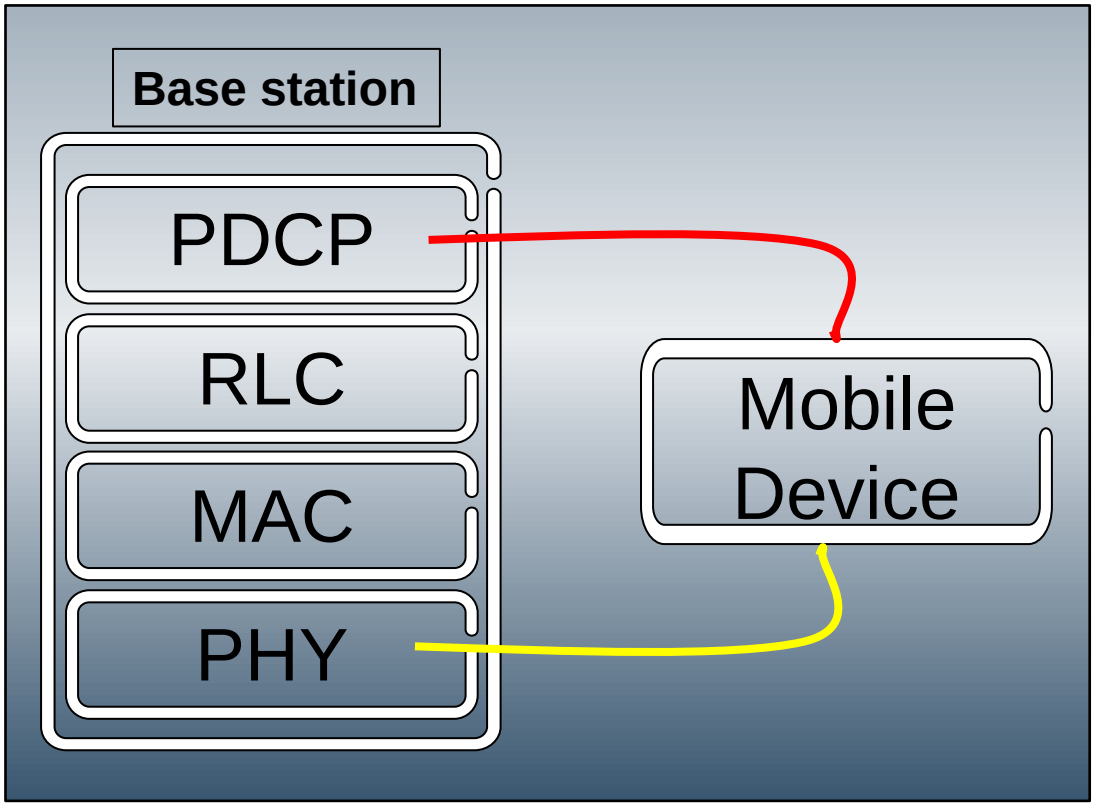
Bandwidth gain depends on distribution of packet sizes. More study is needed!

PDCP (Packet Data Convergence Protocol)

PHY Transport blocks



Security Management Issues



PDCP terminates encryption and integrity protection

CRC is on PHY layer

More study is needed!

Summary

- Error detection/correction mechanisms can be efficiently combined with message authentication to minimize overhead
- Promising approach for resource-constrained IoT devices

References

[1] Proofpoint Inc., ”Proofpoint Uncovers Internet of Things Cyberattacks”, Report Jan 16, 2014

[2] “Cryptographically Secure CRC for Lightweight Message Authentication”, E. Dubrova, M. Näslund, G. Selander, F. Lindqvist, Cryptology ePrint Archive, Report 2015/035, January 2015, https://eprint.iacr.org/2015/035.

[3] “Lightweight CRC-based Message Authentication”, E. Dubrova, M. Näslund, G. Selander, F. Lindqvist, Cryptology ePrint Archive, Report 2015/1138, Nov. 2015, https://eprint.iacr.org/2015/1138

[4] “Error-Correcting Message Authentication for 5G”, E. Dubrova, M. Näslund, G. Selander, K. Norrman, *International Workshop on 5G Security*, 2016