ERROR-CORRECTING MESSAGE AUTHENTICATION FOR 5G

Karl Norrman, Mats Näslund and Göran Selander
Ericsson Research, Stockholm

Elena Dubrova
Royal Institute of Technology (KTH), Stockholm

OUTLINE

- Context for message authentication
- Construction of MAC and properties
- Applicability of MAC for 5G radios

CONTEXT
MESSAGE TRANSMISSION

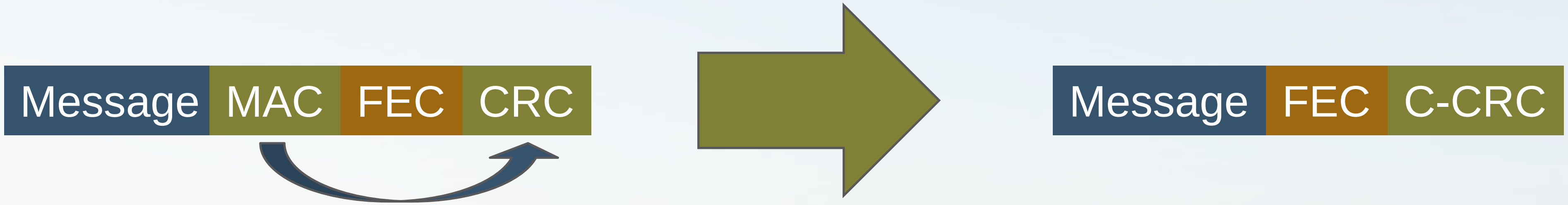
Transmitter

Receiver

Message	MAC	FEC	CRC

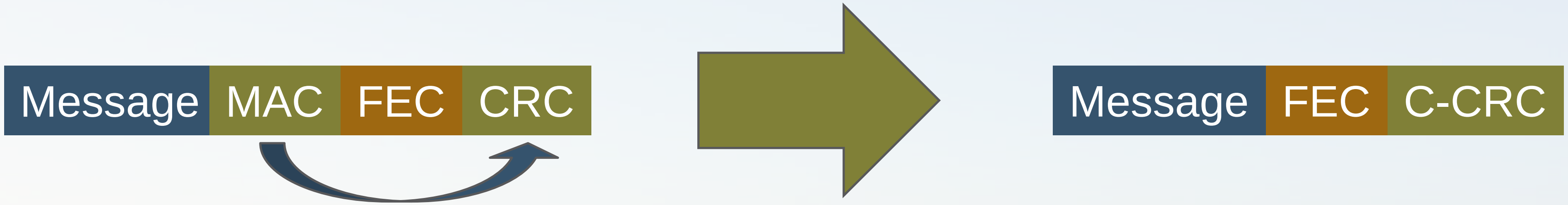
- CRC (Cyclic Redundancy Check)
  - Intended to detect non-malicious transmission errors
- FEC (Forward Error Correction)
  - Additional information receiver can use to correct errors in Message
- MAC (Message Authentication Code)
  - Intended to detect malicious transmission errors

CONTEXT
MESSAGE TRANSMISSION



Combine MAC and CRC => reduce bandwidth consumption

CONTEXT
MESSAGE TRANSMISSION



Combine MAC and CRC => reduce bandwidth consumption

Combine FEC and CRC => reduce bandwidth consumption

- Alternatively, add cheap FEC to links that have none

OUR CONTRIBUTION

- MAC combining integrity protection with single-bit error correction

MACs typically don't do this!

  - Detects burst errors => can replace CRC
  - Less computational resources than HMAC or CBC-MAC
  - Provably secure with a quantifiable failure probability
  - Does not require irreducibility test, as some CRC-based MACs

  - Good candidate for simpler 5G radio types and constrained devices

BACKGROUND
MESSAGE AUTHENTICATION CODES

- Let H be a family of functions mapping $\{0,1\}^m$ to $\{0,1\}^n$
- H is ⊕-linear if, $\forall$ M ≠ M'$\in$ $\{0,1\}^m$ and h$\in$H: h(M ⊕ M') = h(M) ⊕ h(M')
- H is ε-balanced if, $\forall$M, a: $Pr_{h \in H}$ [h(M) = a] < ε
- H is ε-opt-secure if, for any message M, attacker cannot generate M' with valid MAC with probability higher than ε, where a MAC is computed as h(M) ⊕ z for a random pad z.
- If H is ⊕-linear, it is ε-opt-secure iff it is ε-balanced

CONSTRUCTION

- Start from Krawczyk's LFSR based Wegman-Carter MACs

- $h_a = (M \cdot A) \oplus z$, where
  - M is the message as a bit-vector $\in \{0, 1\}^m$
  - A is a Toeplitz matrix generated by an LFSR
  - Z is a pseudo-random bit-vector $\in \{0, 1\}^n$

CONSTRUCTION

$h_a = (M \cdot A) \oplus z$

$$A = \begin{bmatrix} s_0 & s_1 & \cdots & s_{n-2} & c_0 \\ s_1 & s_2 & \cdots & s_{n-1} & c_1 \\ & & \cdots & & \\ s_{m-1} & s_m & \cdots & s_{m+n-3} & c_{m-1} \end{bmatrix}$$

Rows generated by LFSR

Initial state non-zero

C_i is even parity code

↓

Rows are pairwise linearly independent

Hamming weight > 1

↓

Can correct 1 bit-error

SECURITY LEVEL

- The hash function family is ε-opt-secure with $\varepsilon < \frac{m}{2^{n-2}}$
- (Krawzcyk's family has $\varepsilon < \frac{m}{2^{n-1}}$)

- Probability of attacker creating multiple errors that appear as a single error (and hence corrected) is $\varepsilon < \frac{3m-1}{2^{n-1}-1}$

SECURITY LEVEL

Hash output length to ensure 32-bit security

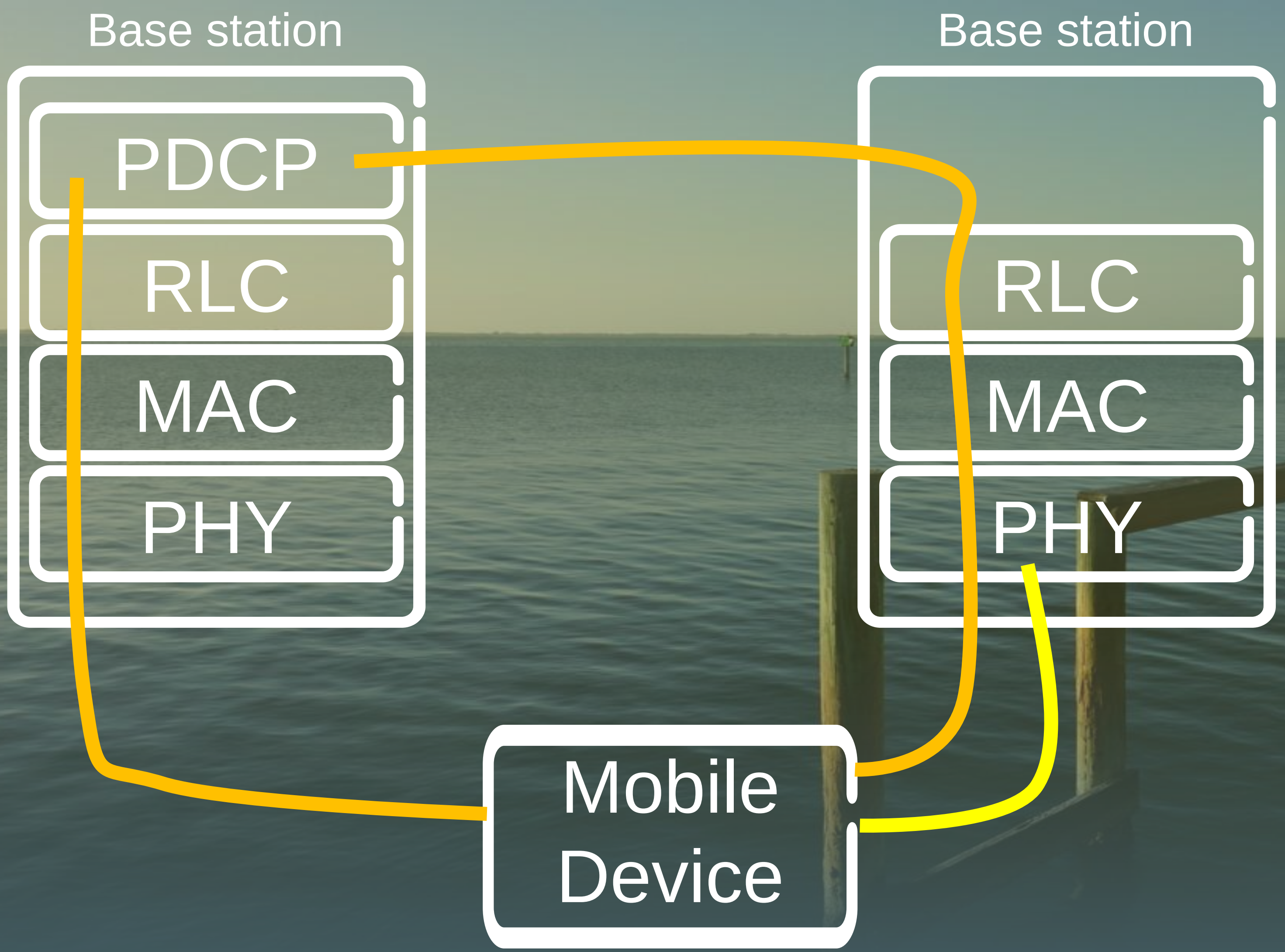
MAC-C length n, bits	Message length m, bits	Failure probability	
		Error Detection	Error Correction
40	43	$2^{-32.6}$	2^{-32}
41	85	$2^{-32.6}$	2^{-32}
42	171	$2^{-32.6}$	2^{-32}
43	341	$2^{-32.6}$	2^{-32}
44	683	$2^{-32.6}$	2^{-32}
45	1365	$2^{-32.6}$	2^{-32}
46	2731	$2^{-32.6}$	2^{-32}
47	5461	$2^{-32.6}$	2^{-32}
48	10923	$2^{-32.6}$	2^{-32}
49	21864	$2^{-32.6}$	2^{-32}
50	43692	$2^{-32.6}$	2^{-32}
51	87384	$2^{-32.6}$	2^{-32}
52	174768	$2^{-32.6}$	2^{-32}
53	349536	$2^{-32.6}$	2^{-32}
54	699072	$2^{-32.6}$	2^{-32}

PRACTICALITIES

$h_a = (M \cdot A) \oplus z$

- M is secret but can stay fixed for the session
- z is generated per message (can use a stream-cipher like UIA2/EIA1 from 3G/LTE)

APPLICABILITY TO 3GPP 5G
3GPP ARCHITECTURE



- LTE dual connectivity
- PDCP terminates encryption and integrity protection
- CRC on physical layer

APPLICABILITY TO 3GPP 5G
REPLAY PROTECTION

- PDCP provides replay protection using a counter
- PHY does not have a counter, but RLC counter could be used instead

APPLICABILITY TO 3GPP 5G
BANDWIDTH GAIN (LTE VIEW)

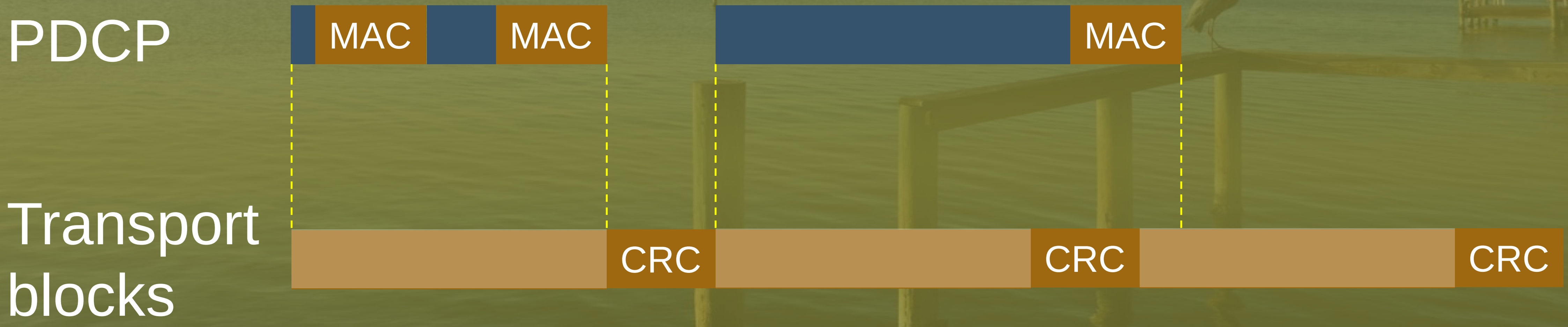
Payload

MAC LTE MAC

CRC LTE CRC

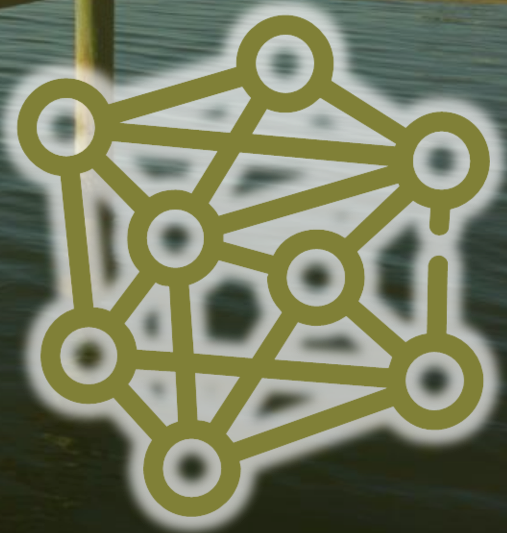
Bandwidth gain depends on distribution of packet sizes.

More study needed!



APPLICABILITY TO SIMPLER 5G RADIOS

- 5G is more than 3GPP air interface
- Simpler radios as used by direct communication sensor networks often lack sophisticated FEC, soft-combining, split-protocol architectures etc.
- More promising use-case



CONCLUSIONS

- New MAC with 1-bit error correction capability
- Guaranteed detection of error bursts
- Known security level
- Promising for simpler 5G radios for sensor networks
- Less suitable for 3GPP 5G radio NR


QUESTIONS?

ERICSSON