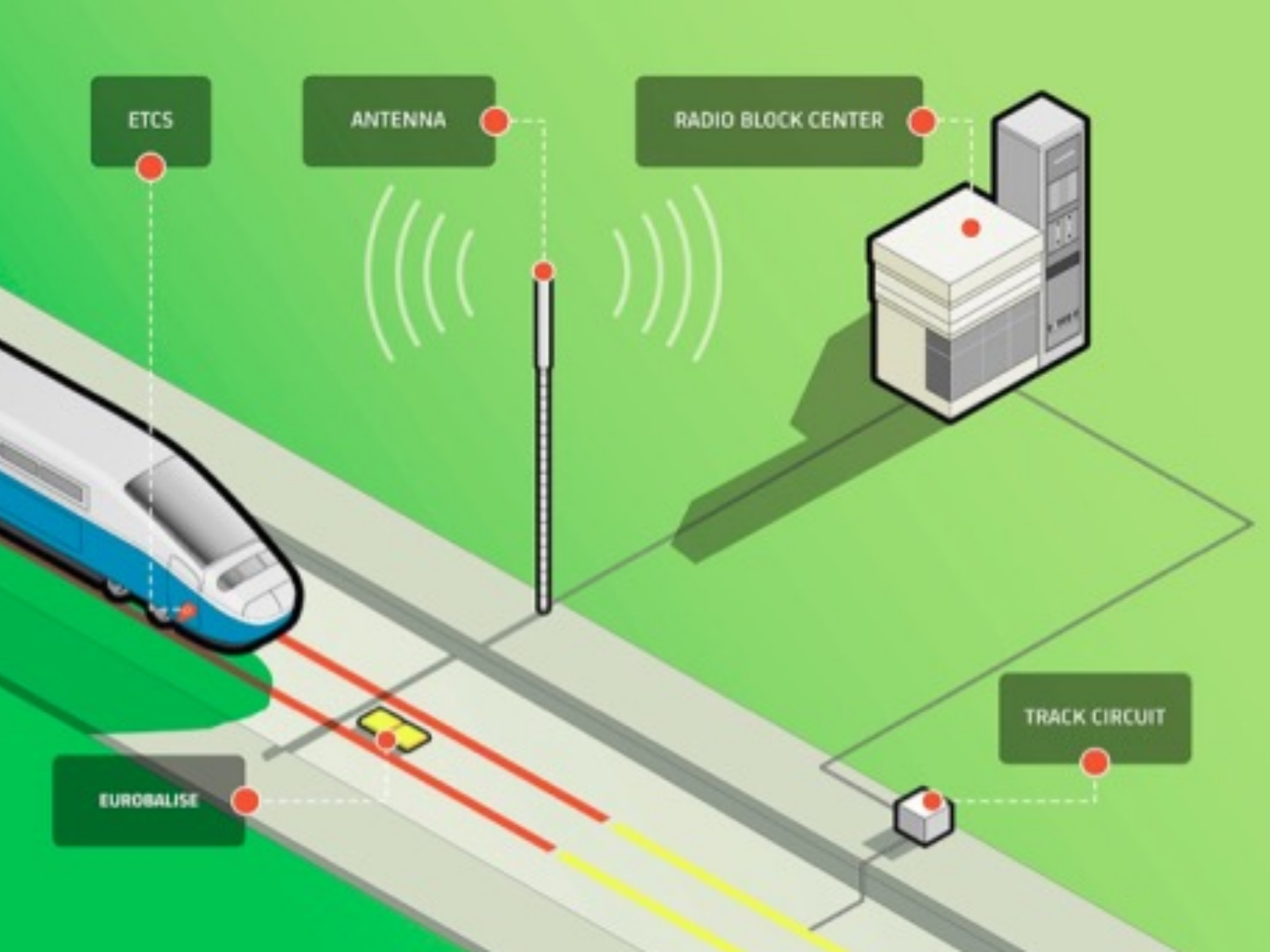
An Attack Against Message Authentication in the ERTMS Train to Trackside Communication Protocols

Tom Chothia, **Mihai Ordean**, Joeri de Ruiter, Richard J. Thomas


ETCS
ANTENNA
RADIO BLOCK CENTER
TRACK CIRCUIT
EUROBALISE

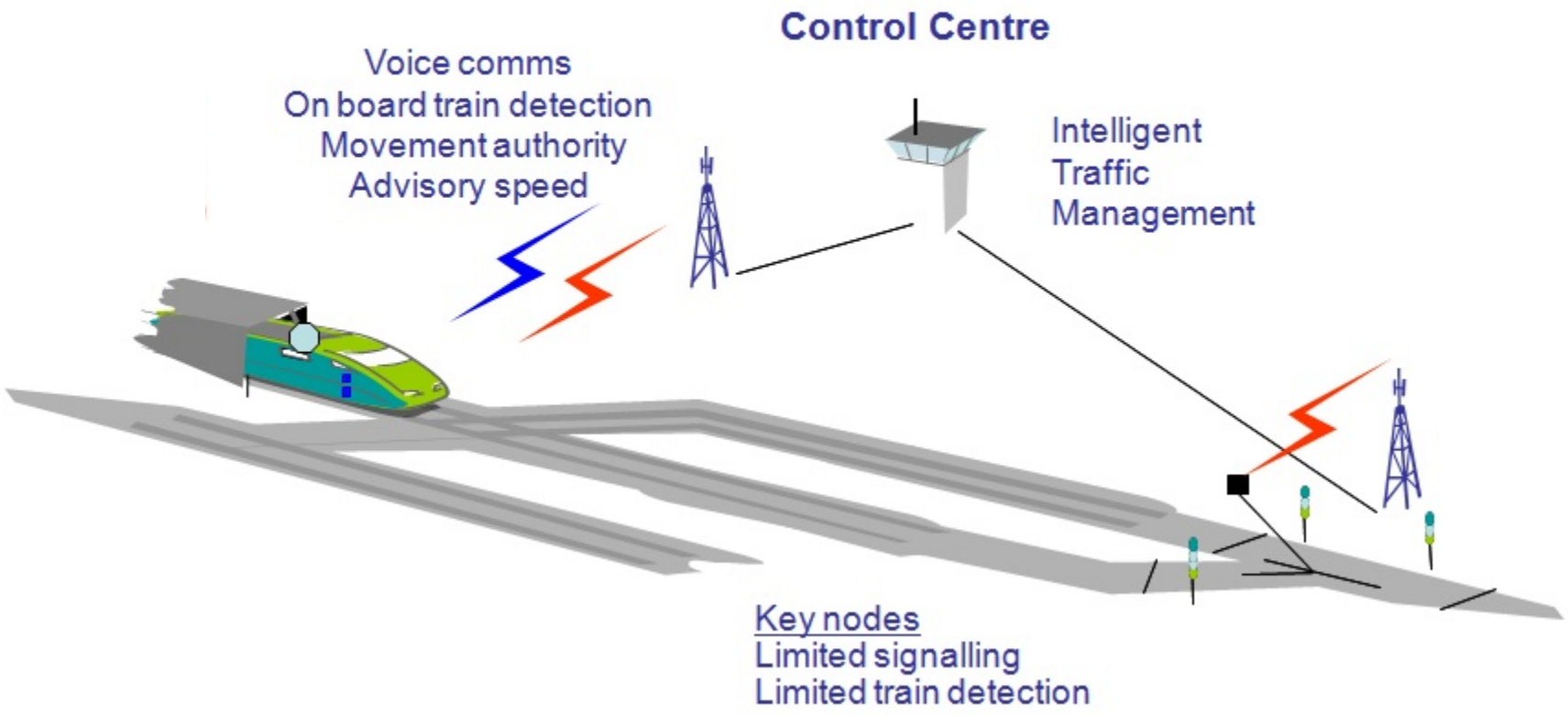
ERTMS Overview

The European Rail Traffic Management System (ERTMS) is a suite of protocols used to deliver next-generation train management and signalling.

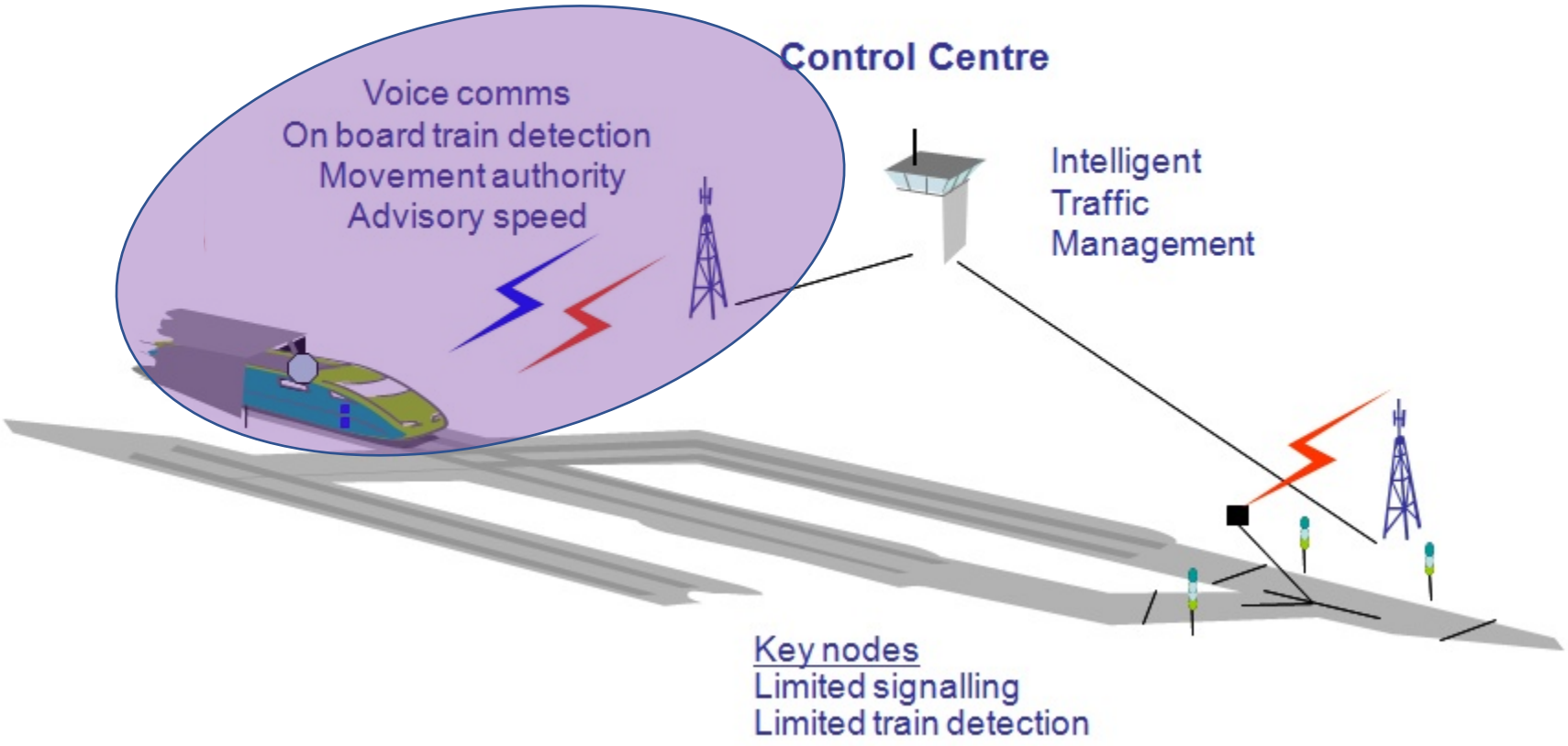
ERTMS components:

- GSM-R – encryption/physical interaction
- EuroRadio – message authentication
- Application Layer protocol - instructions

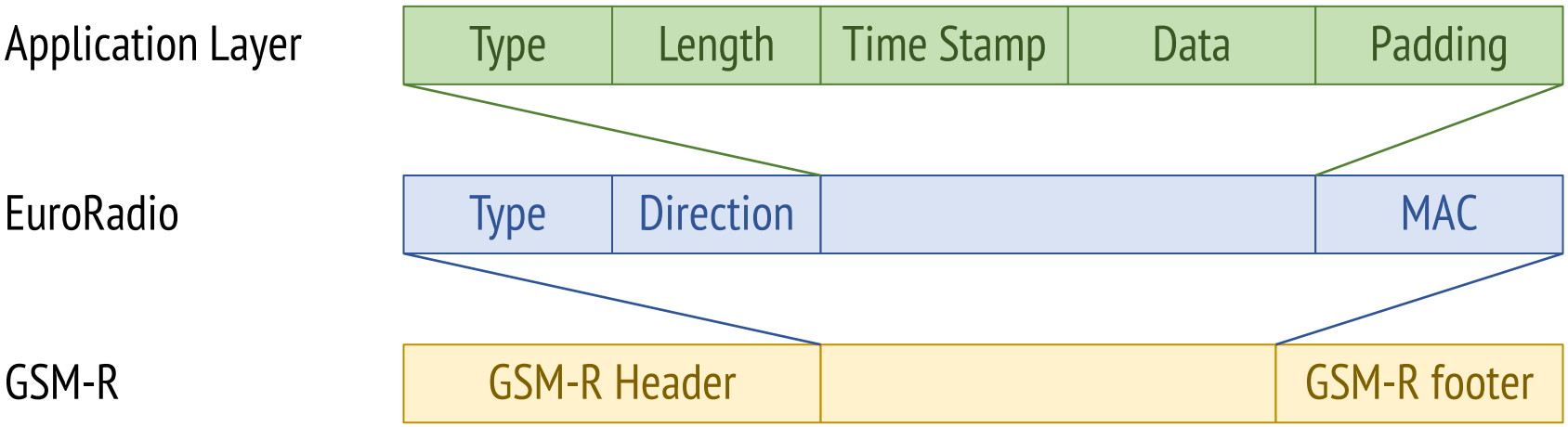
ERTMS Overview



ERTMS Overview



ERTMS stack


Application Layer
Type
Length
Time Stamp
Data
Padding
EuroRadio
Type
Direction
MAC
GSM-R
GSM-R Header
GSM-R footer

GSM-R

- Provides data encryption on the ERTMS stack
- Based on the GSM Mobile Communications Standard

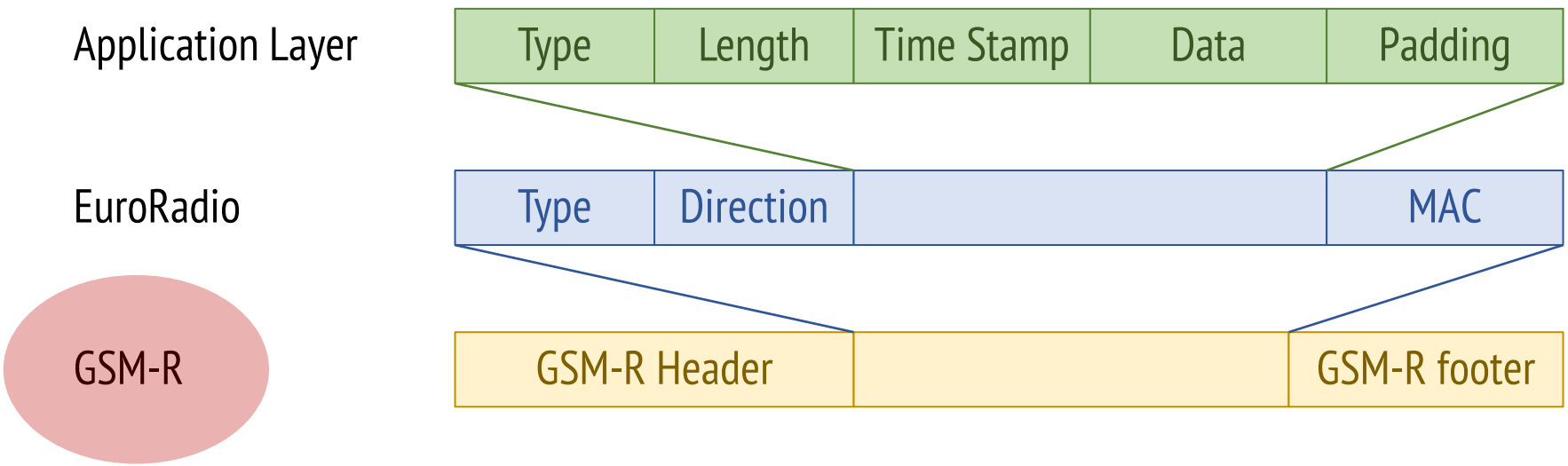
  (i.e. basically 2G) with:
  - different frequency ranges
  - rail-specific functionality (multi-party communication, emergency calling functionality, priority-based pre-emption, etc.)
- Crypto:
  - A5/1* a stream cipher based on (LFSRs)
  - A5/3 (optionally) a block cipher

---

* broken:

1. Elad Barkan, Eli Biham, Nathan Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. J. Cryptology 21(3): 392-429 (2008)
2. L. Karstensen. GSM A5/1 rainbow tables in Oslo, Norway. Available: https://lassekarstensen:wordpress:com/2013/08/08/gsm-a51-rainbow-tables-in-oslo-norway/, 2015.
3. https://www.ckn.io/blog/2016/01/25/gsm-sniffing-voice-traffic/
4. https://www.youtube.com/playlist?list=PLRovDyowOn5F_TFotx0n8A79ToZYD2lOv

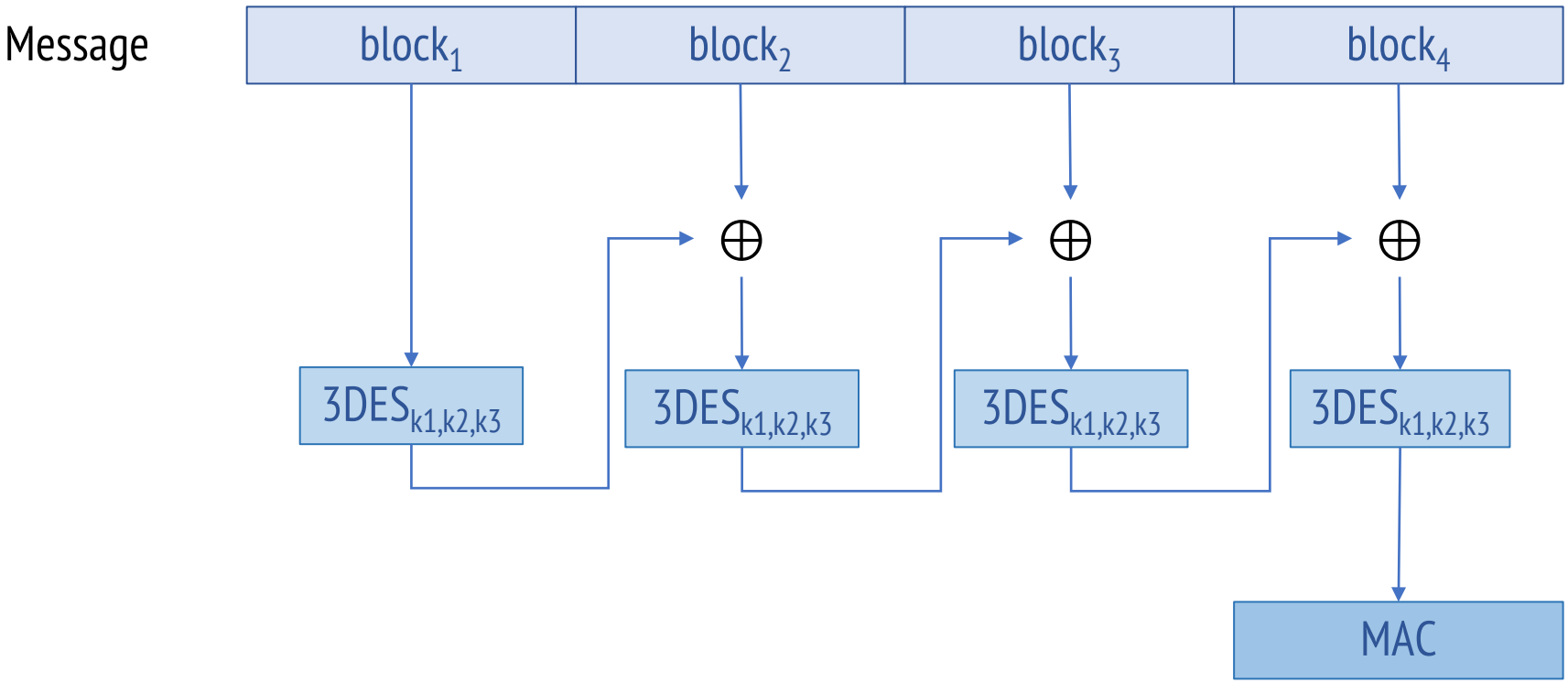
ERTMS stack


Application Layer
Type
Length
Time Stamp
Data
Padding
EuroRadio
Type
Direction
MAC
GSM-R
GSM-R Header
GSM-R footer

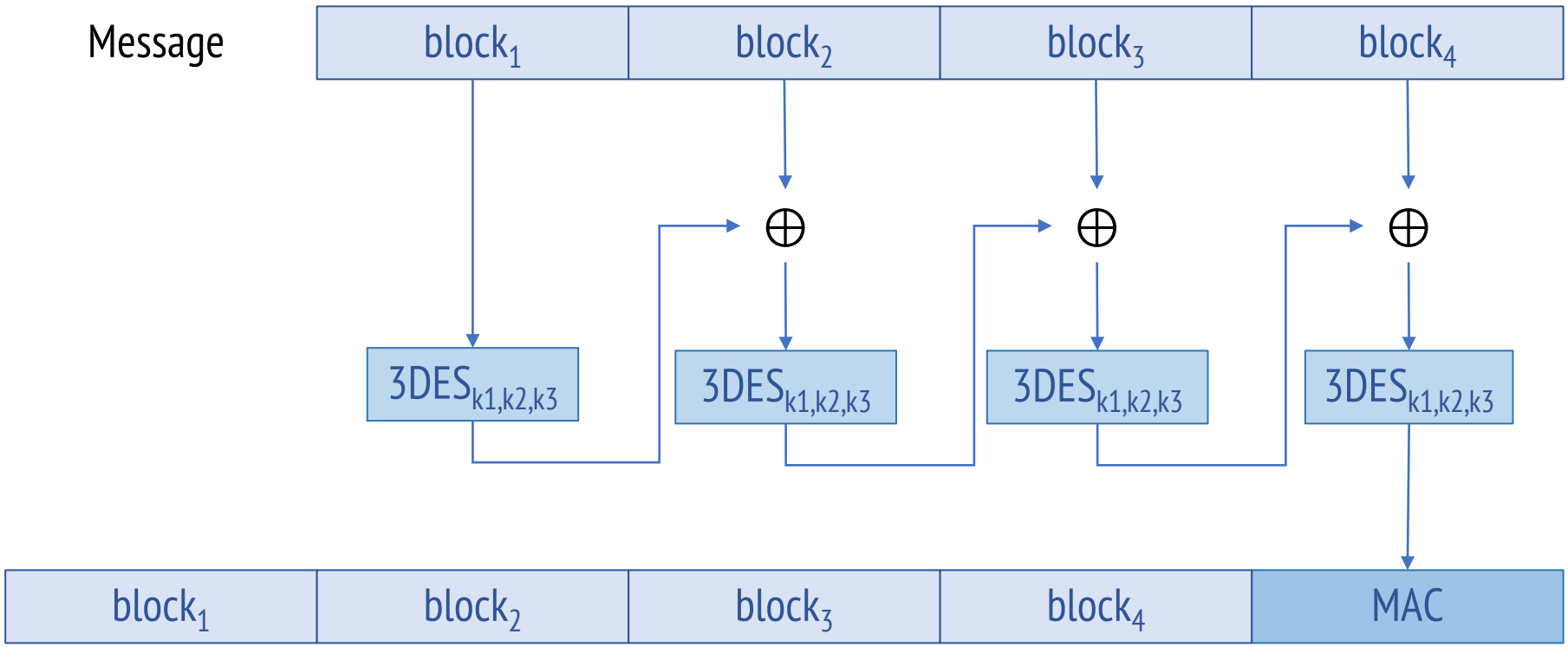
EuroRadio

- Provides authentication for messages on the upper layers
- Based on the ISO 9797-1 MAC Algorithm 3:
  - A CBC circuit which uses a combination of DES and 3DES
  - ISO 9797 padding, i.e. 0s are used as padding until data becomes a multiple of the block size
- Supports priority:
  - Normal priority: messages have a MAC
  - High priority: messages do not require a MAC (e.g. emergency stop messages)

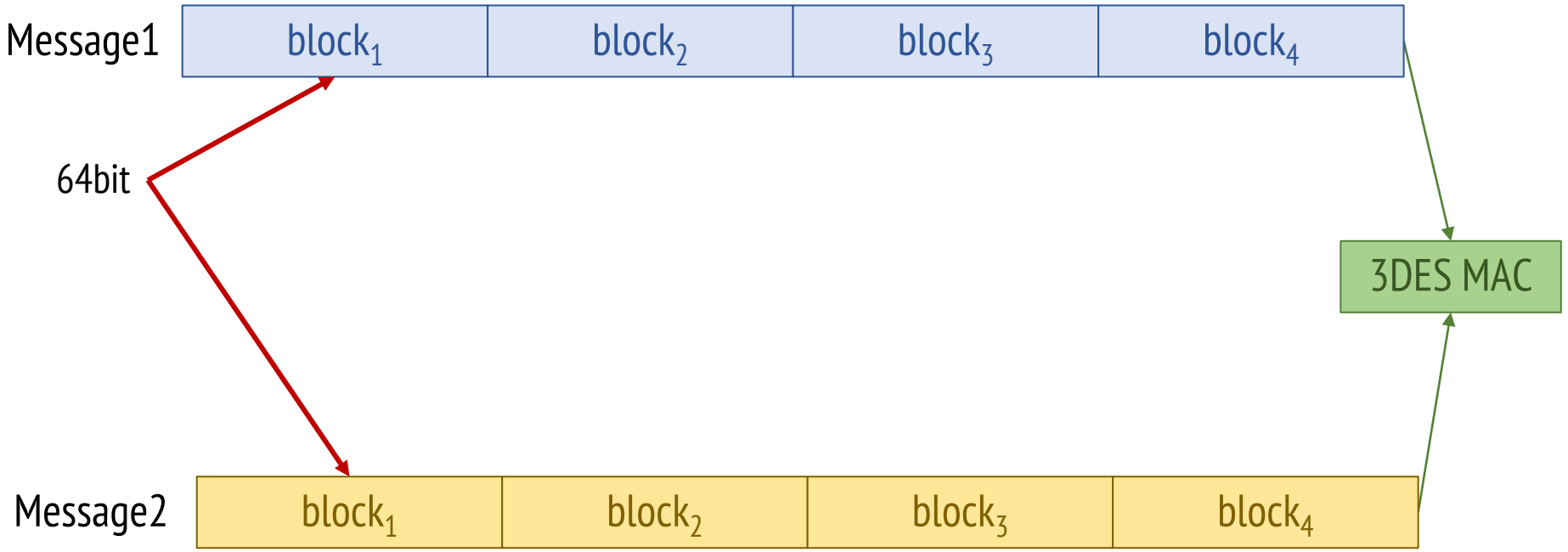
3DES-CBC-MAC


Message
block1
block2
block3
block4
3DESk1,k2,k3
3DESk1,k2,k3
3DESk1,k2,k3
3DESk1,k2,k3
MAC

3DES-CBC-MAC

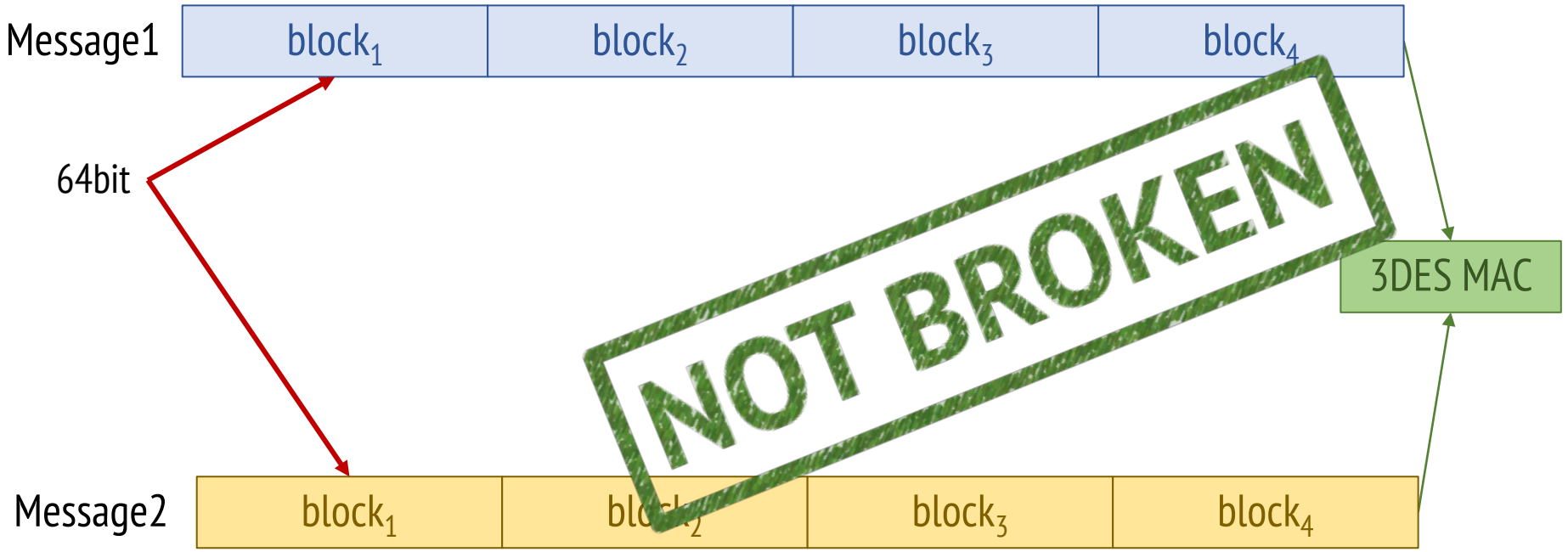

Message
block1
block2
block3
block4
3DESk1,k2,k3
3DESk1,k2,k3
3DESk1,k2,k3
3DESk1,k2,k3
block1
block2
block3
block4
MAC

Collisions in ciphers with small block sizes



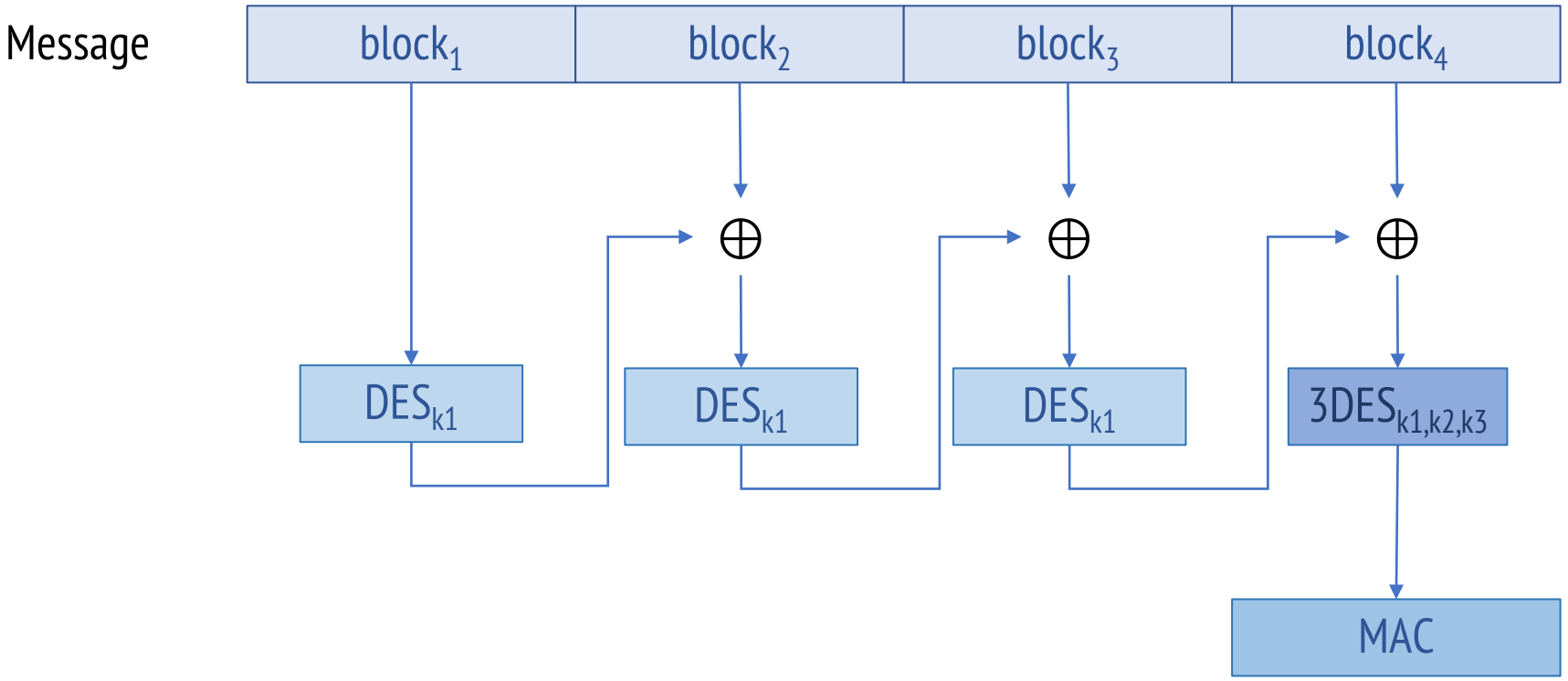
1. B. Preneel and P. C. van Oorschot. Key recovery attack on ANSI X9. 19 retail MAC. Electronics Letters, 1996
2. H. Handschuh and B. Preneel. Minding your MAC algorithms. *Information Security Bulletin*, 2004.
3. Bhargavan, Karthikeyan, and Gaëtan Leurent. "On the practical (in-) security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.

Collisions in ciphers with small block sizes

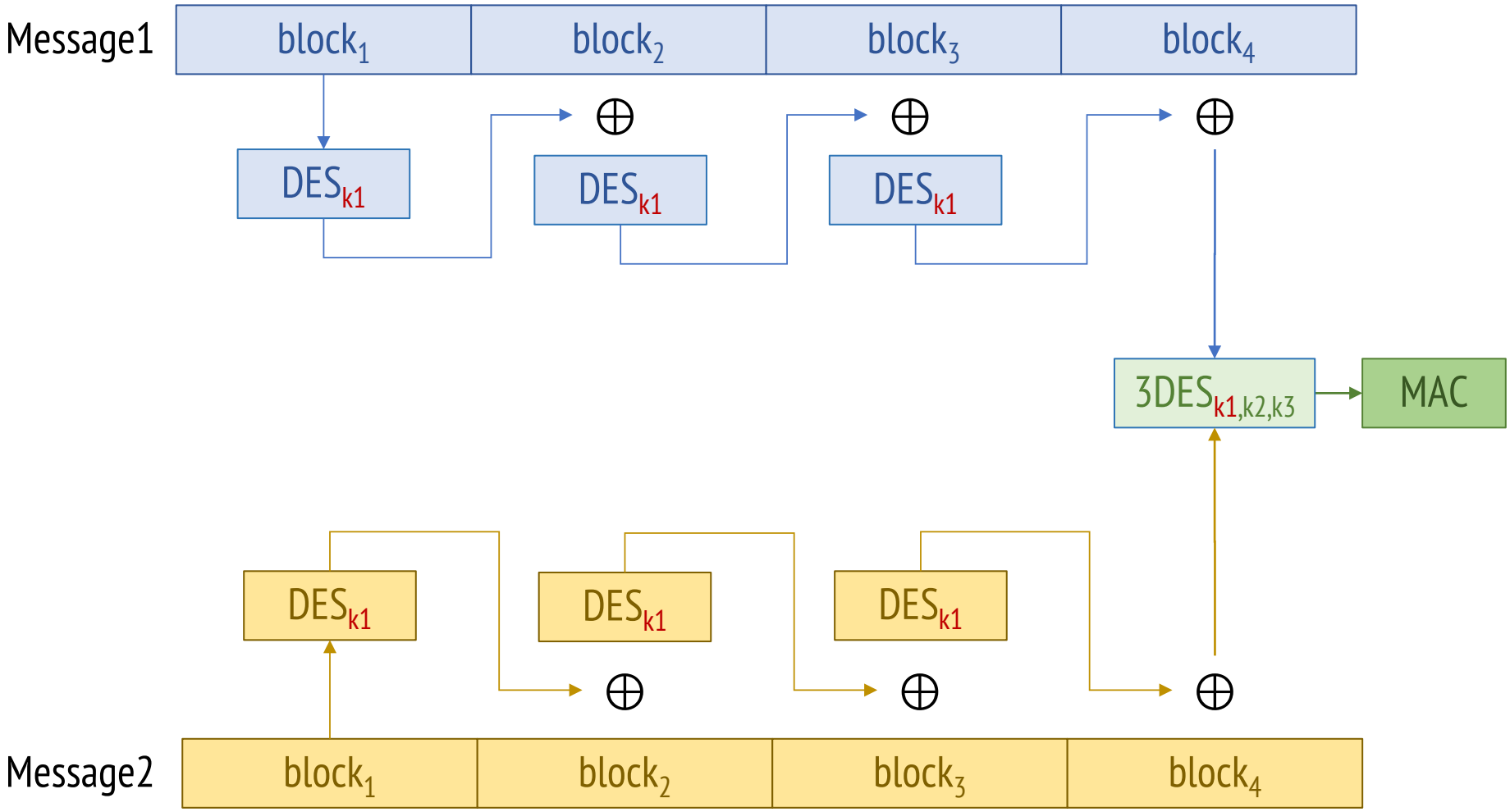


1. B. Preneel and P. C. van Oorschot. Key recovery attack on ANSI X9. 19 retail MAC. Electronics Letters, 1996
2. H. Handschuh and B. Preneel. Minding your MAC algorithms. *Information Security Bulletin*, 2004.
3. Bhargavan, Karthikeyan, and Gaëtan Leurent. "On the practical (in-) security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN."
4. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.

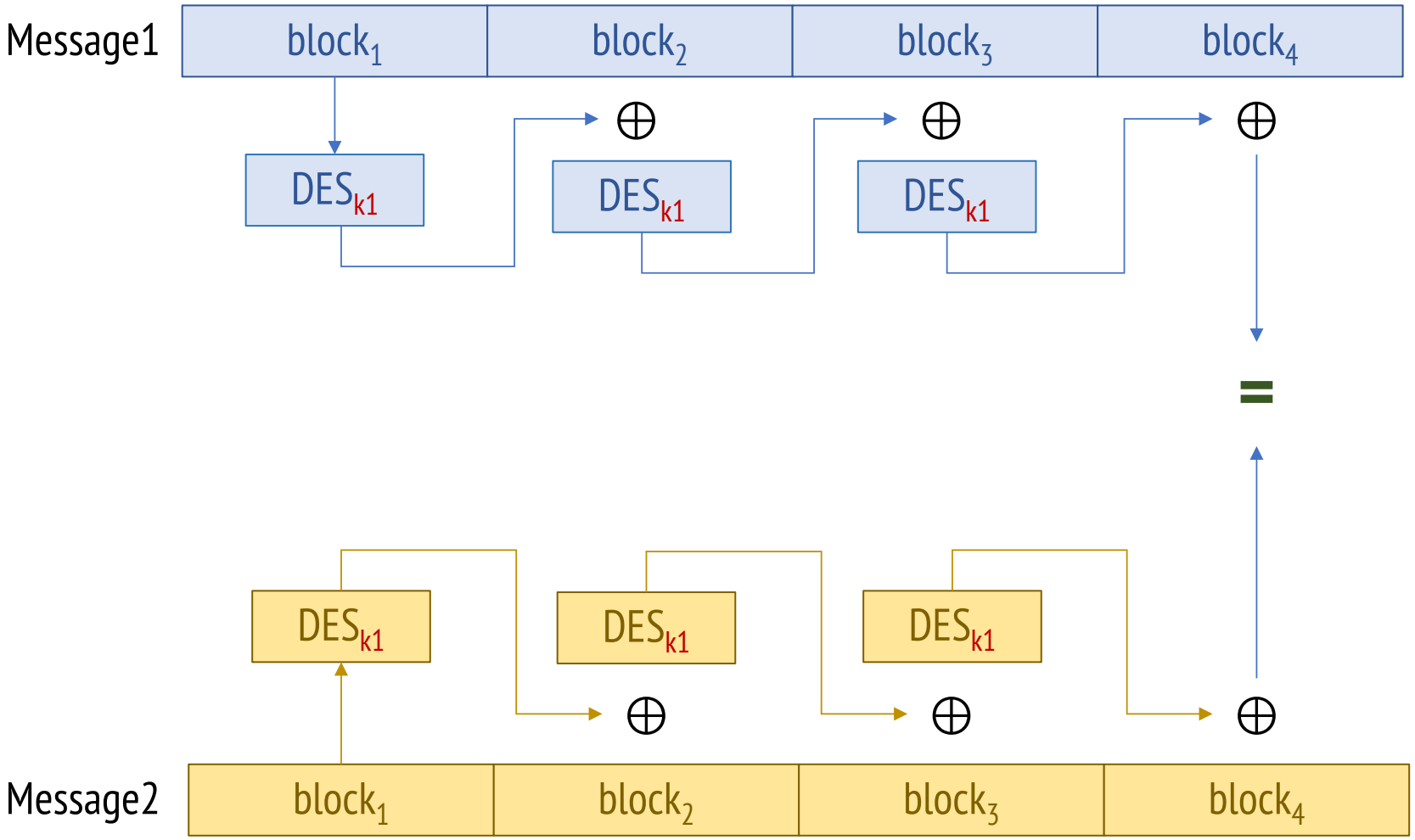
EuroRadio MAC



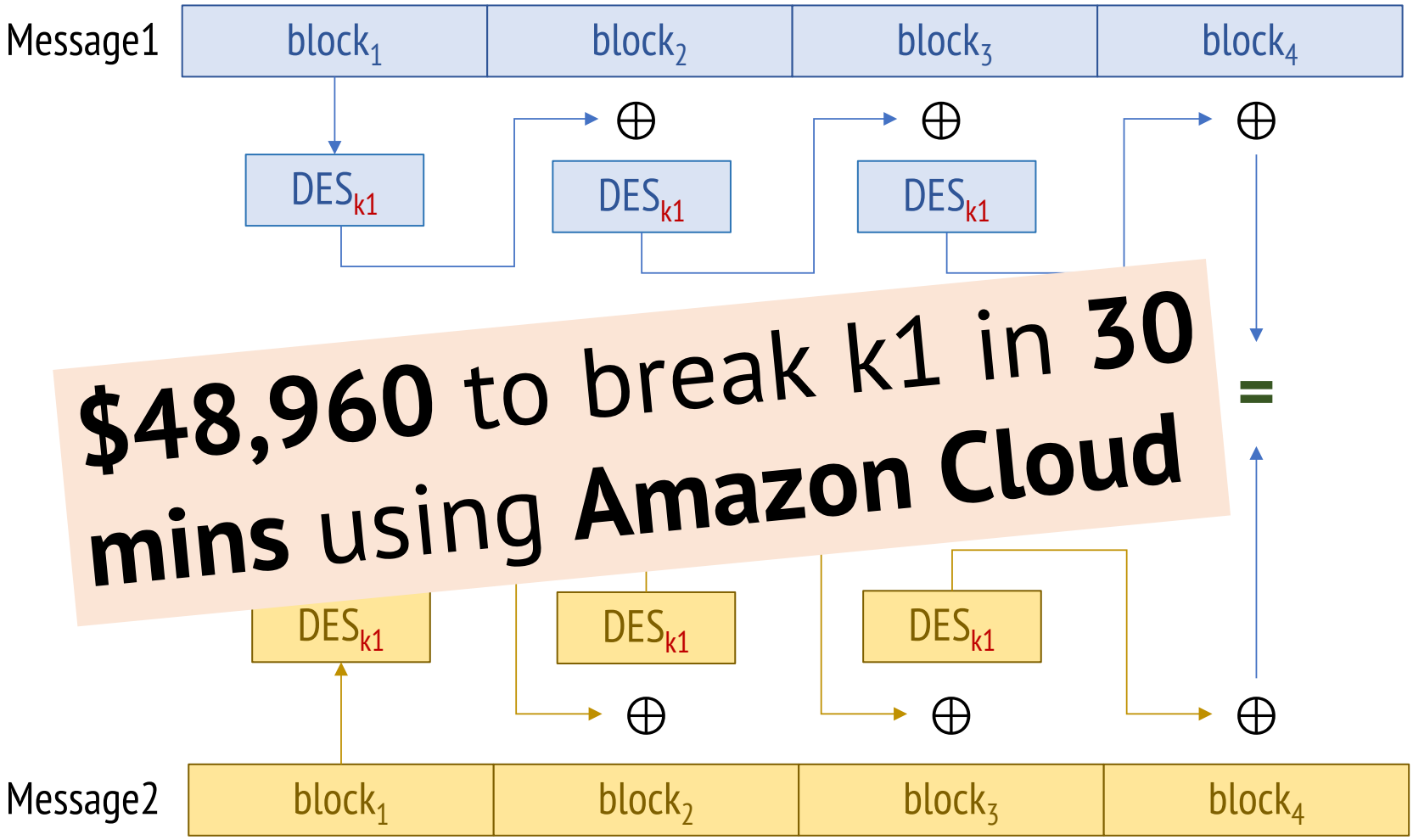
DES key recovery (when a collision happens)



DES key recovery (when a collision happens)

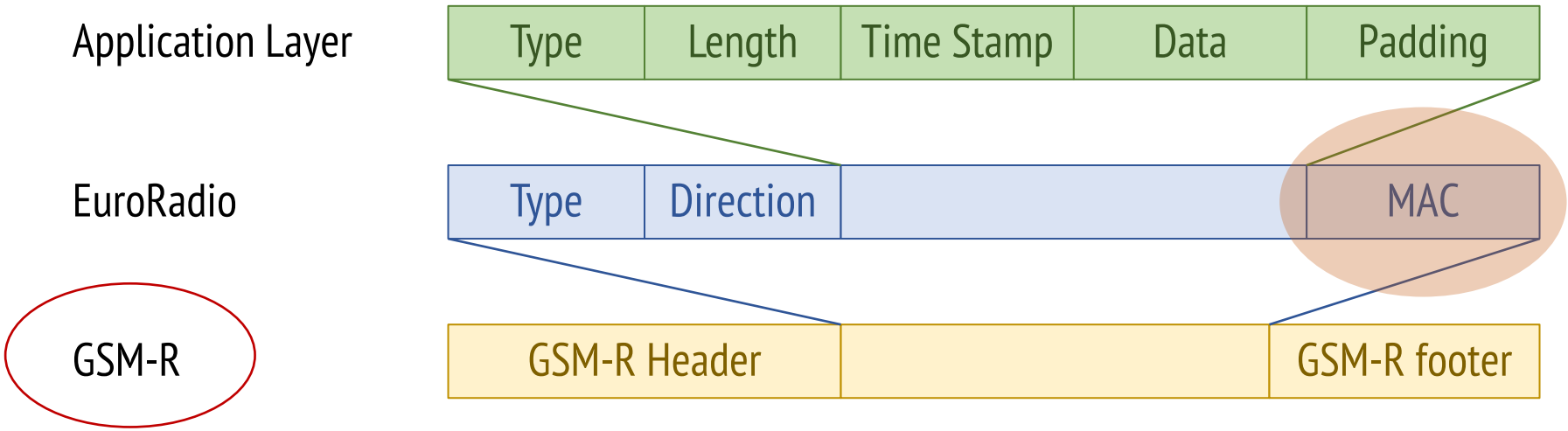


DES key recovery (when a collision happens)



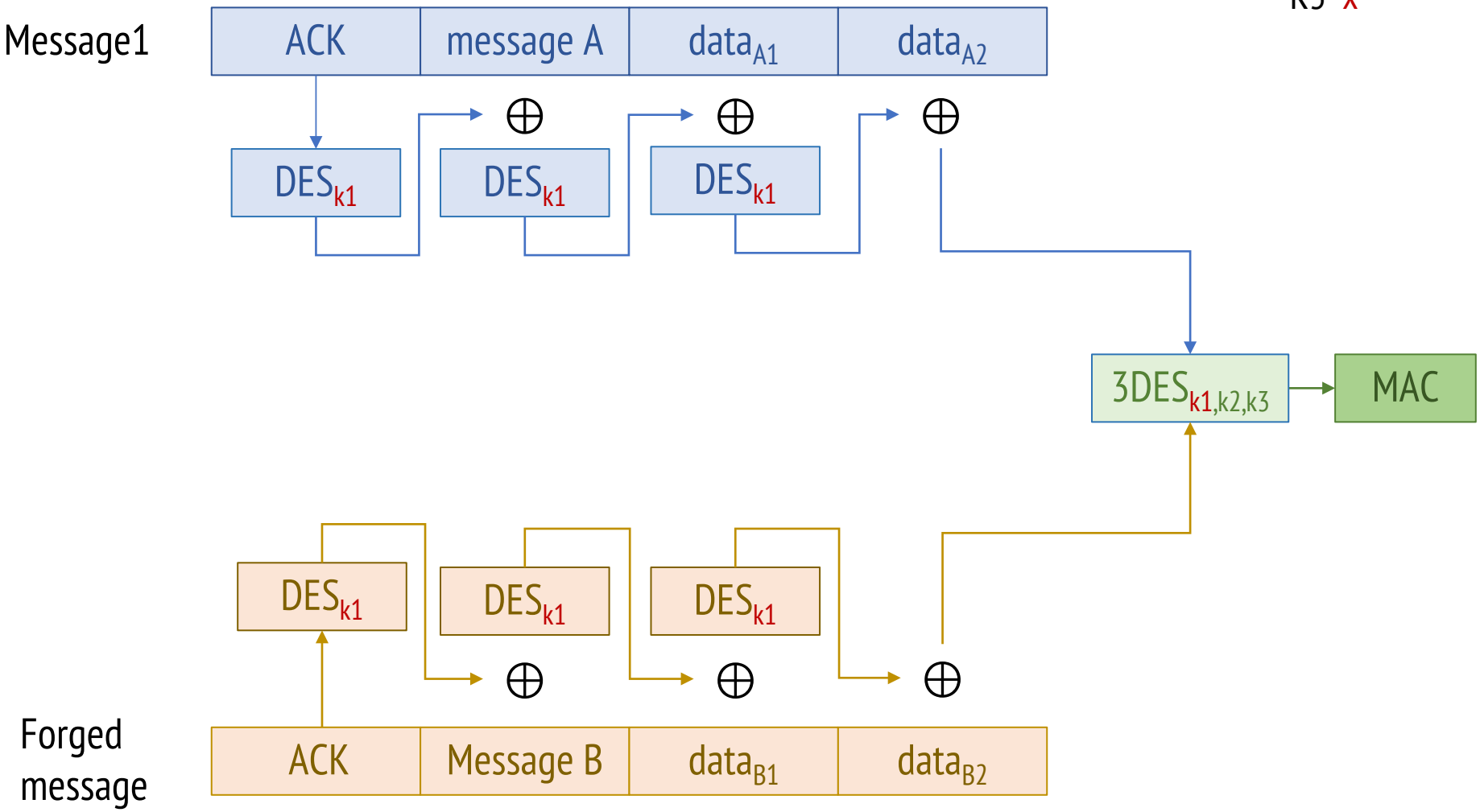
$48,960 to break k1 in **30 mins** using **Amazon Cloud**

ERTMS stack

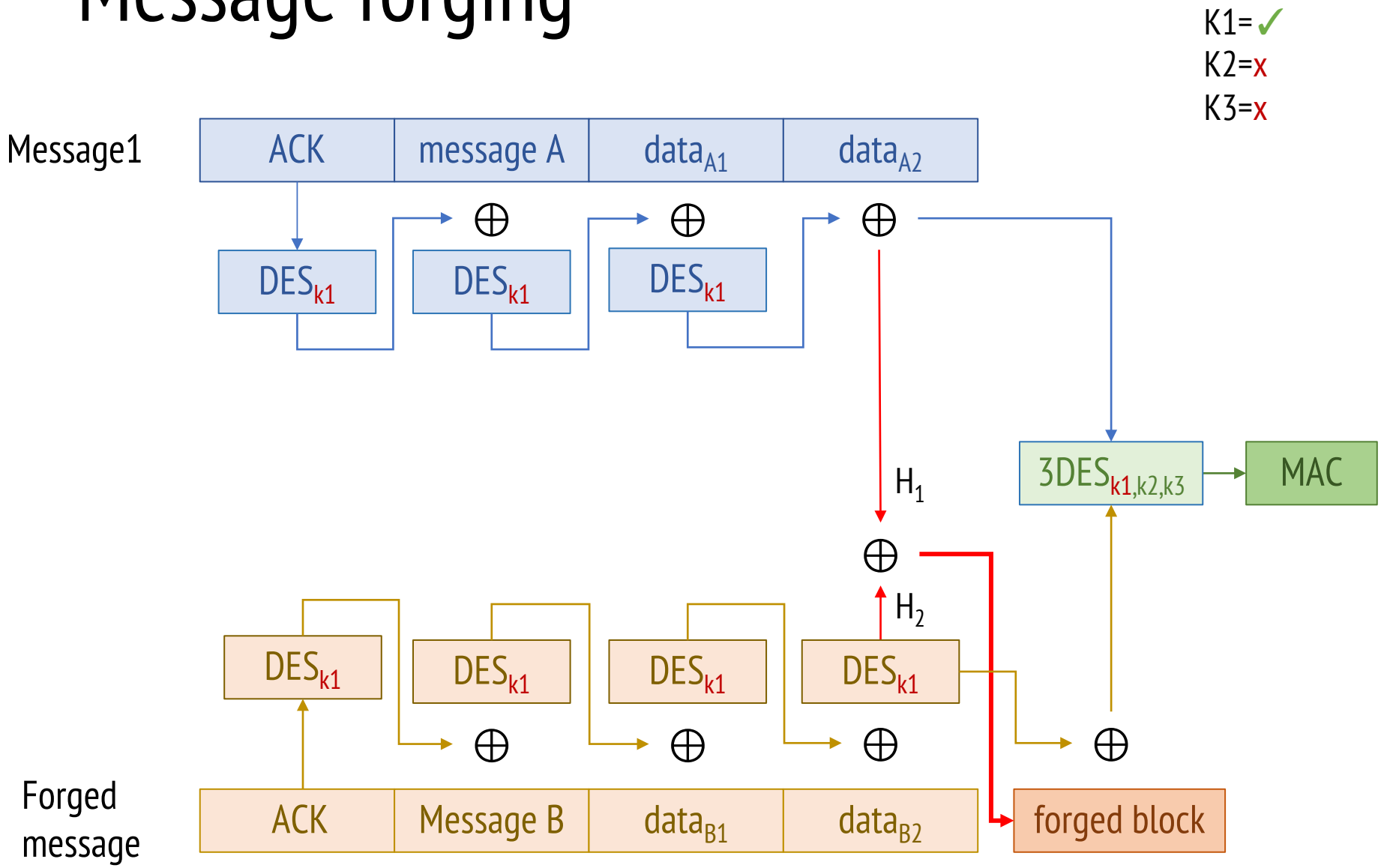

Application Layer
Type
Length
Time Stamp
Data
Padding
EuroRadio
Type
Direction
MAC
GSM-R
GSM-R Header
GSM-R footer

Message forging

K1=✓
K2=x
K3=x

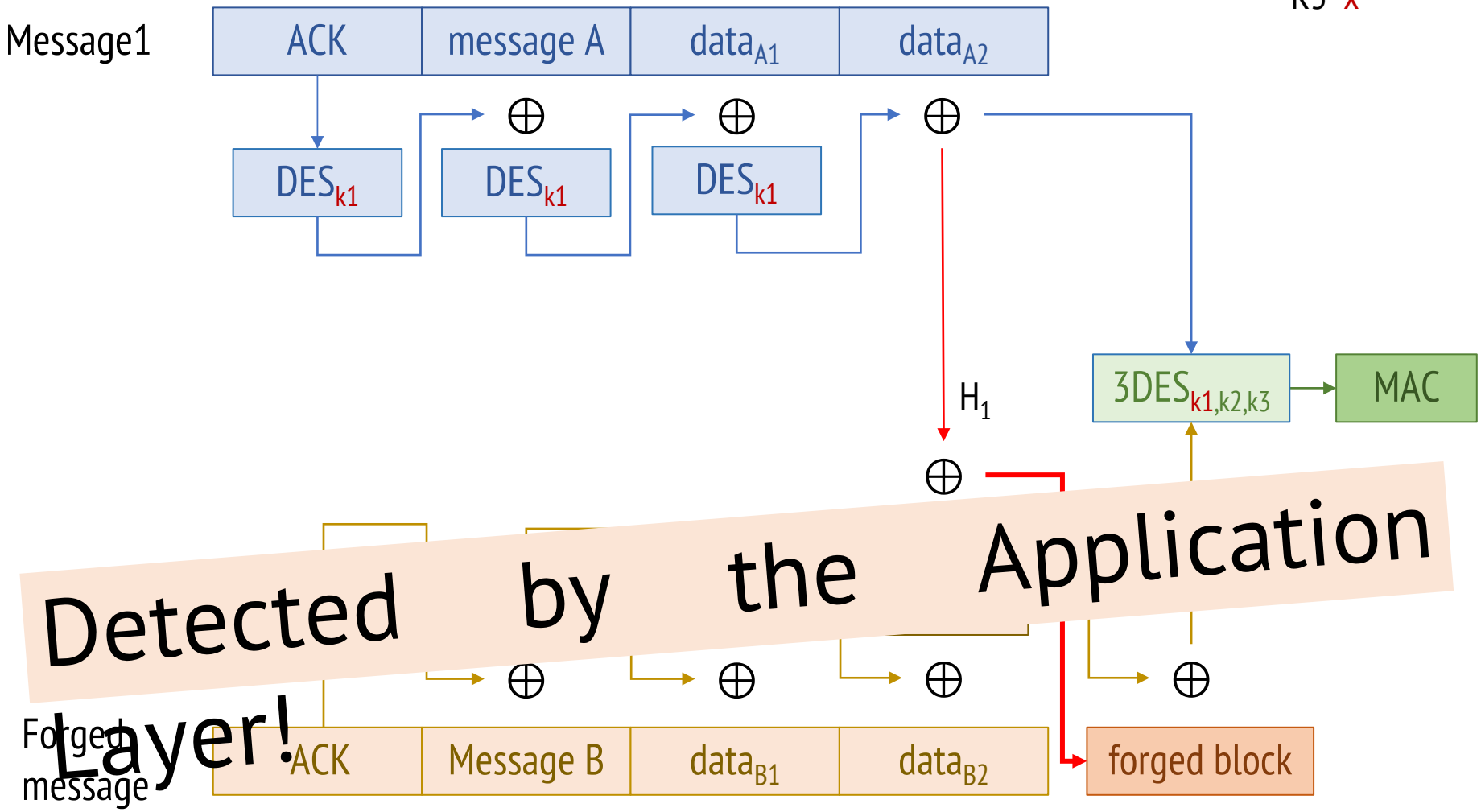


Message forging



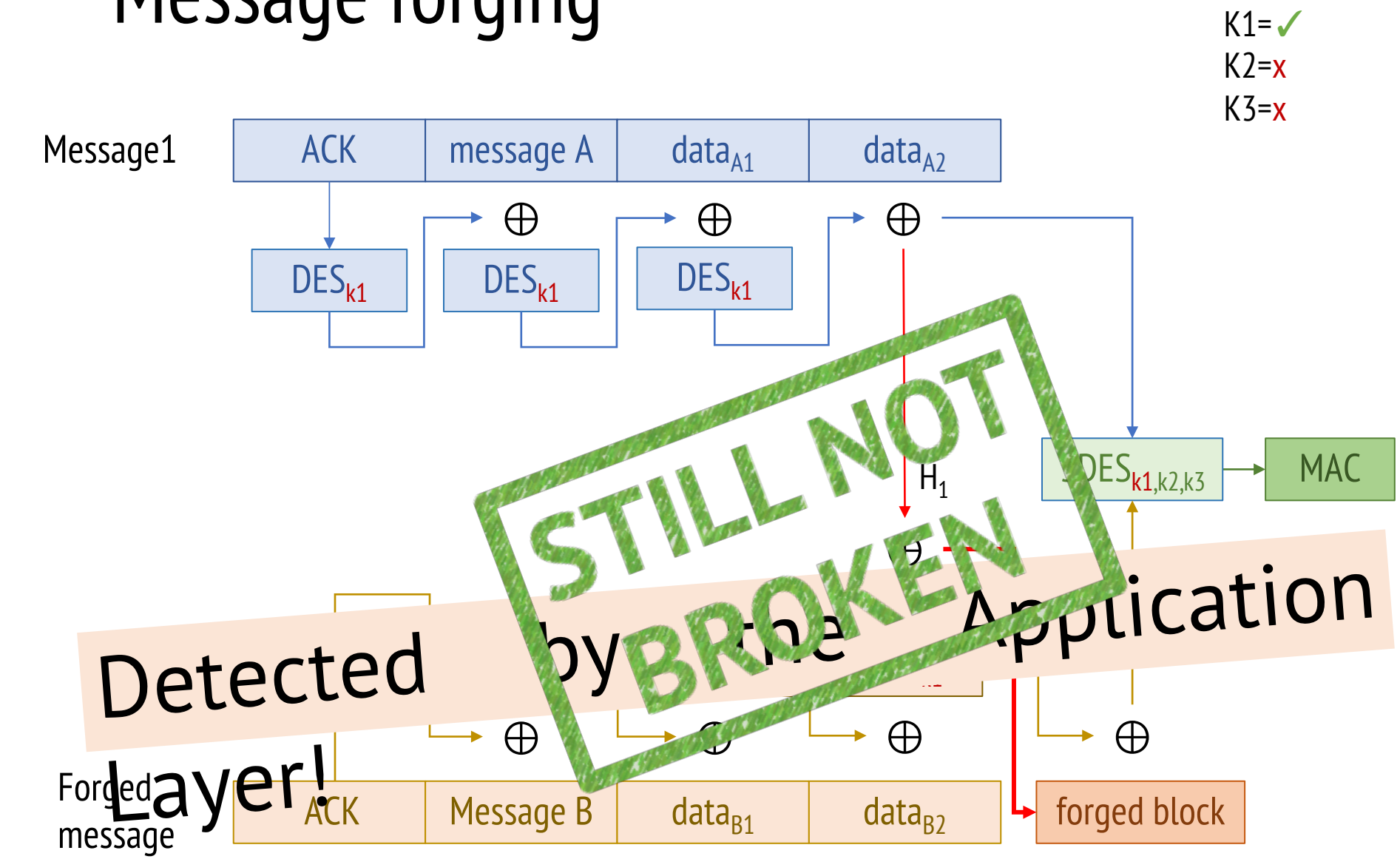
Message forging

K1=✓
K2=x
K3=x



Detected by the Application Layer!

Message forging

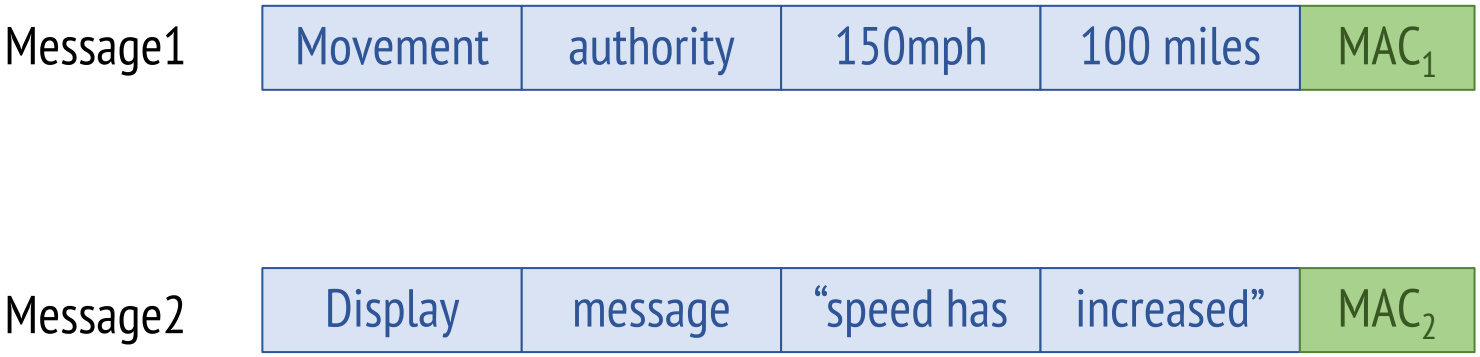


ERTMS - Application Layer

- Transmits train control messages and signalling
- Messages can be of multiple types
  - Movement authorities
  - Display message
  - Acknowledgment message

Application layer

K1= ✓
K2=x
K3=x



Application layer

K1=✓
K2=x
K3=x

Message1	Movement	authority	150mph	100 miles	MAC_1
Message2	Display	message	“speed has	increased”	MAC_2

Message1 Message2

Movement	authority	150mph	100miles	Display	message	“speed has	increased”	MAC_3

Application layer

K1=✓
K2=x
K3=x

Message1	Movement	authority	150mph	100 miles	MAC_1
Message2	Display	message	“speed has	increased”	MAC_2

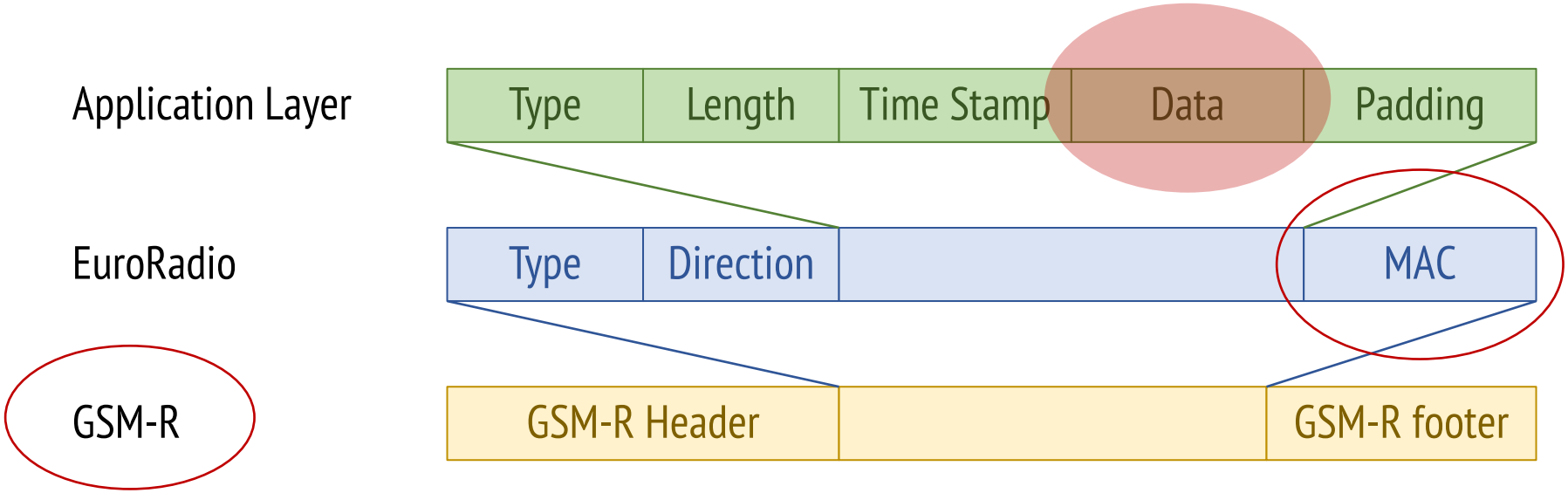
Display message accepts unicode characters!

Message1

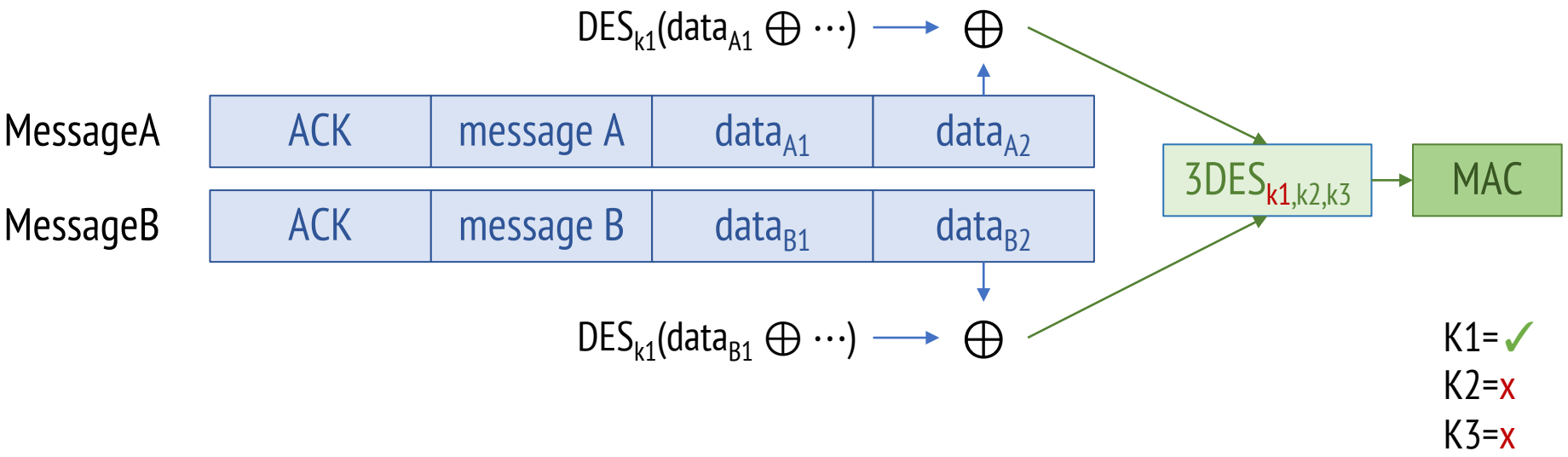
Movement	authority	150mph	100miles	Display	message	“speed has	increased”	MAC_3

ERTMS stack

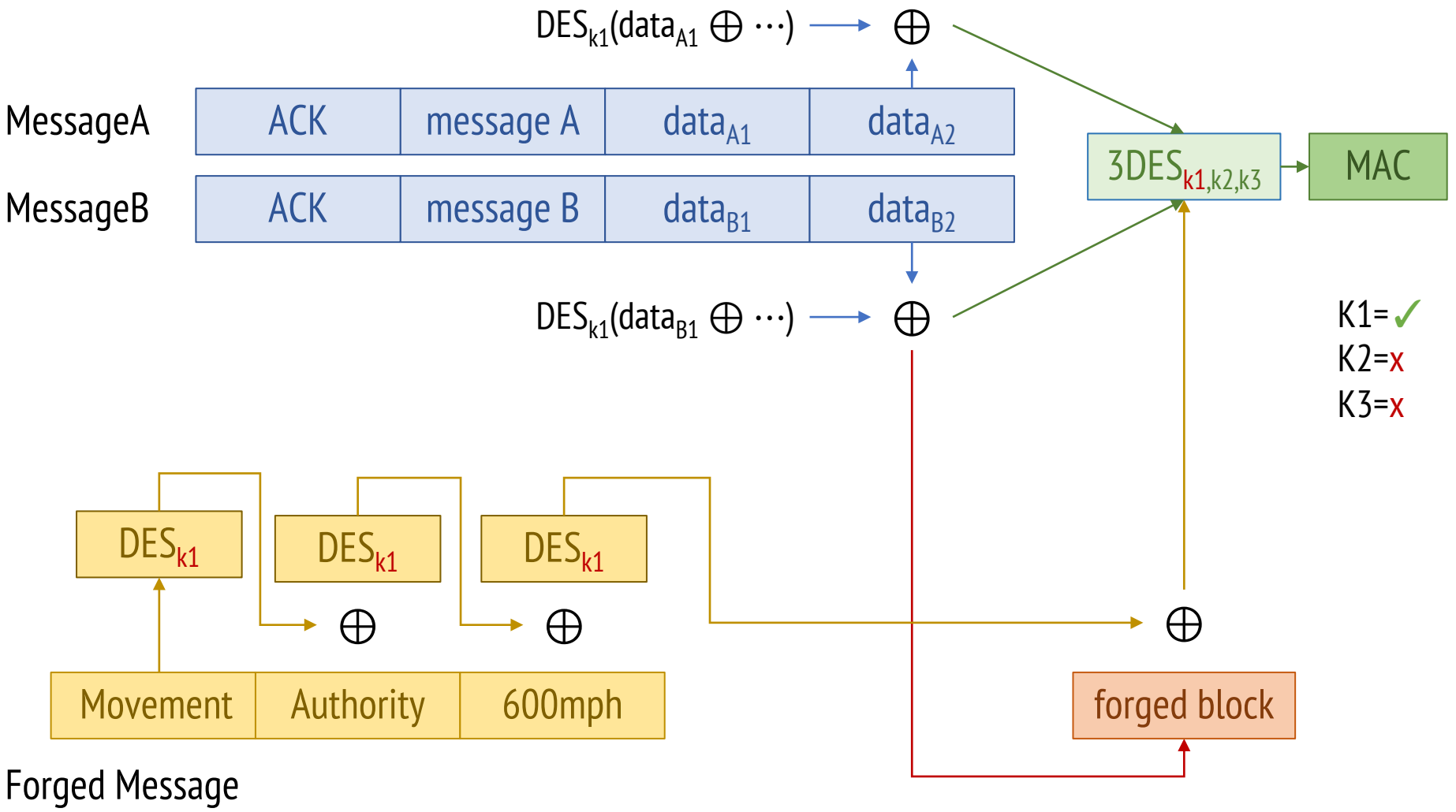
K1=✓
K2=x
K3=x



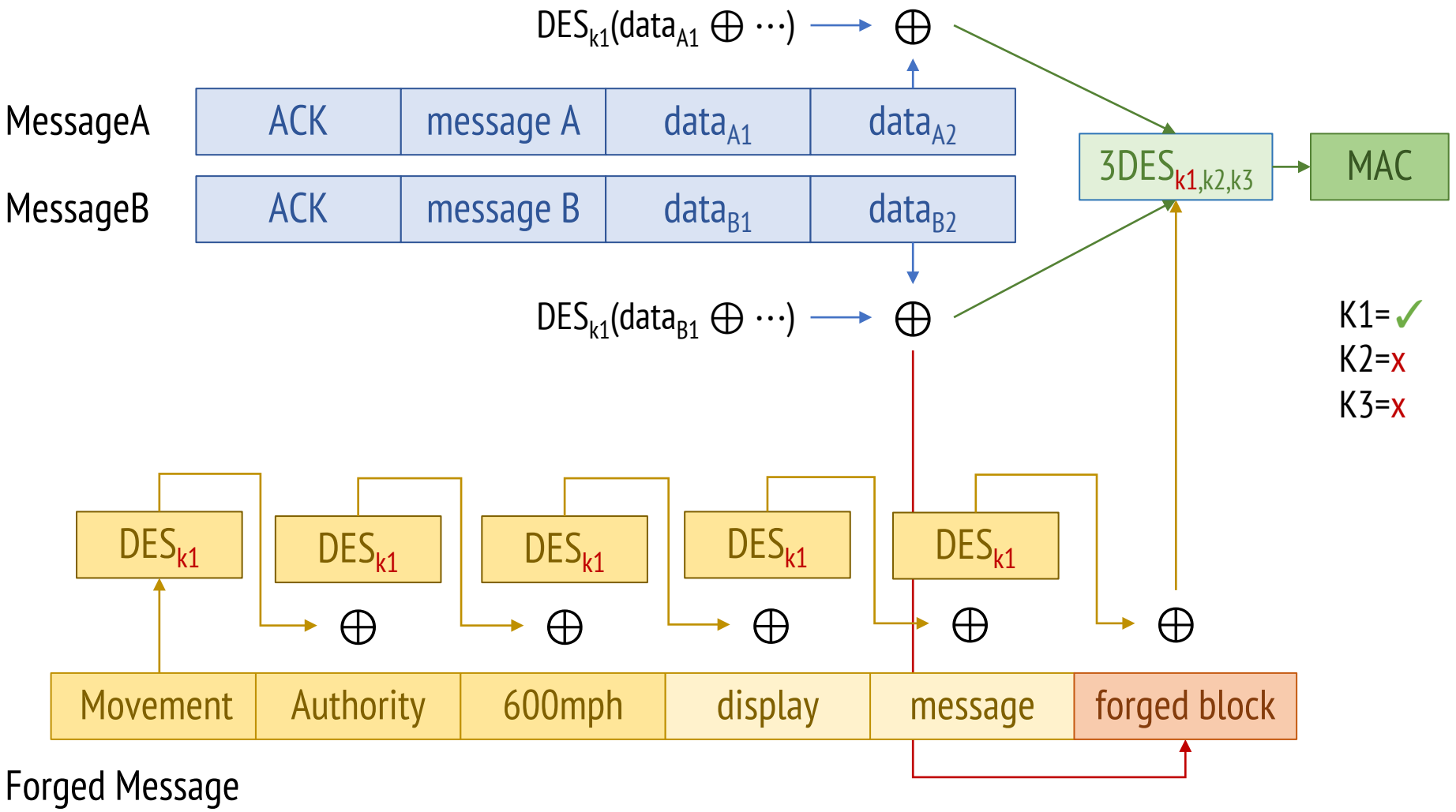
Leveraging collisions



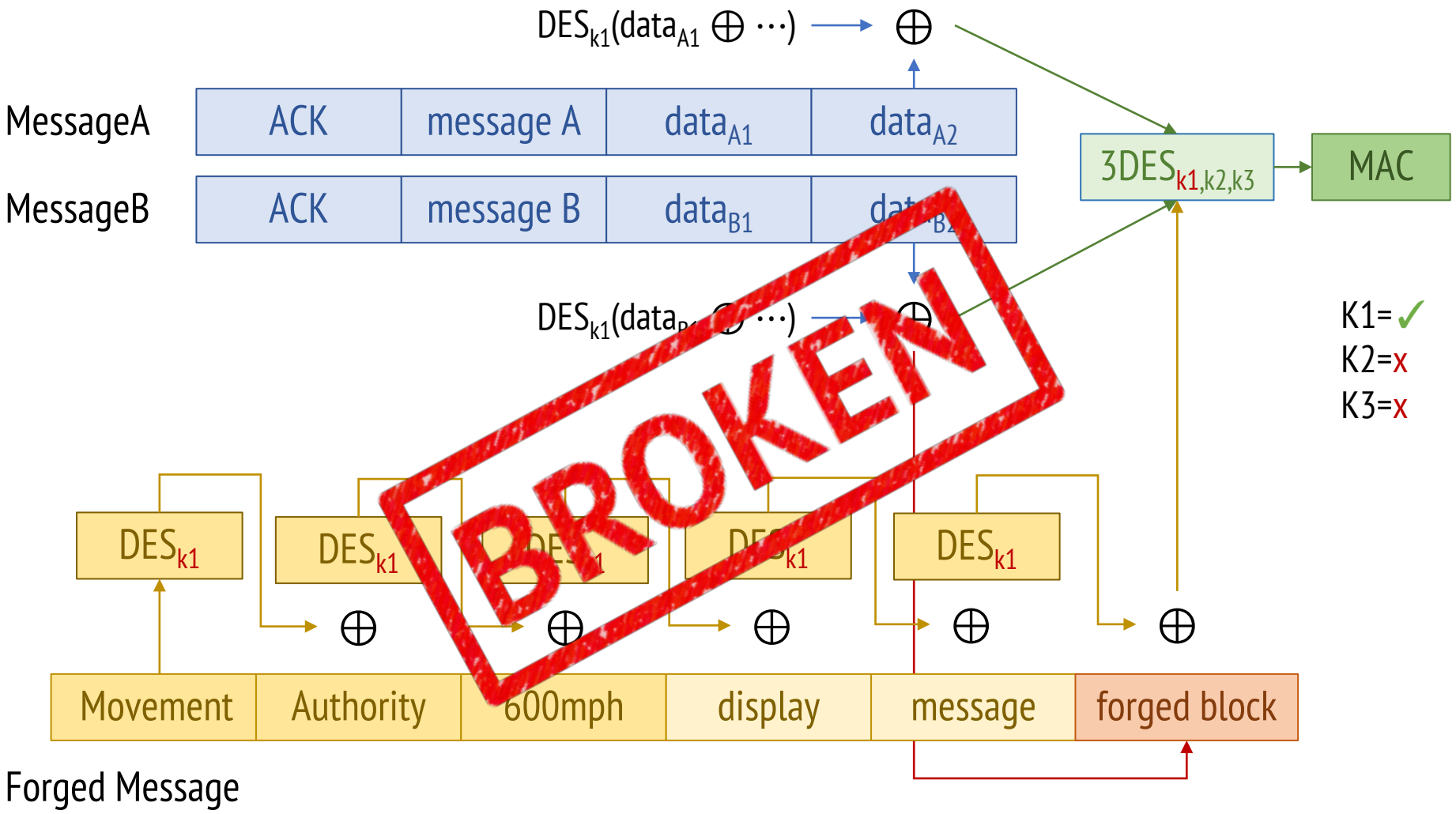
DES key recovery



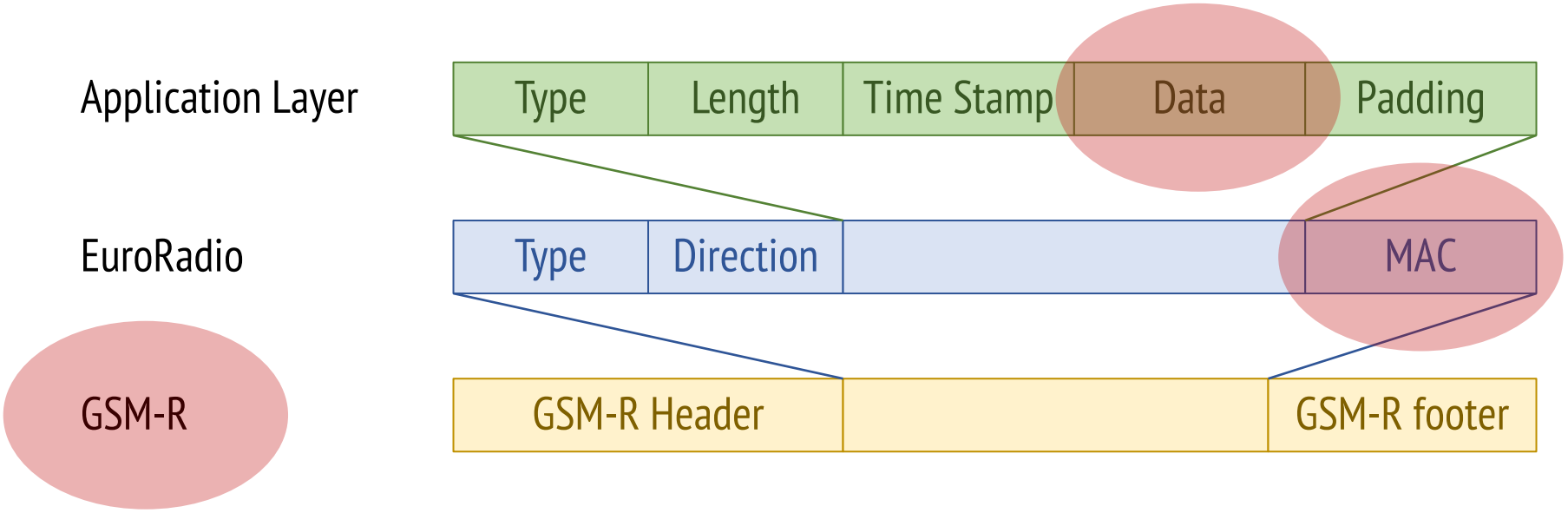
Message concatenation



Message concatenation



ERTMS stack vulnerabilities



ACK message collision

Two acknowledgement messages:

00120000020A9203A2105E048000062105DFD0000000000

MAC: 80B7557F31566DBB

00120000020A9203AAE360078000006AE360000000000000

MAC: 80B7557F31566DBB

Forged movement authority

Variable	Length (bits)	Value	Description
NID_PACKET	8	0000 1111	Level 2/3 movement authority (only RBC)
Q_DIR	2	10	Both directions
L_PACKET	13	0 0000 0111 0001	113 bits
Q_SCALE	2	10	10 m
V_LOA	7	111 1000	600 km/h
T_LOA	10	11 1111 1111	Unlimited
N_ITER	5	0 0000	0 iterations
L_ENDSECTION	15	111 1111 1111 1111	327670 meter
Q_SECTIONTIMER	1	0	No section timer information
Q_ENDTIMER	1	0	No end section timer information
Q_DANGERPOINT	1	0	No danger point information
Q_OVERLAP	1	1	Overlap information to follow
D_STARTOL	15	000 0000 0000 0000	0 meter
T_OL	10	00 0000 0000	0 sec
D_OL	15	000 0000 0000 0000	0 meter
V_RELEASEOL	7	111 1110	Use onboard calculated release speed

Forged display message

Variable	Length (bits)	Value	Description
NID_PACKET	8	0100 1000	Packets for sending plain text messages
Q_DIR	2	00	Reverse
L_PACKET	13	0 0000 1101 1100	220 bits
Q_SCALE	2	10	10 m
Q_TEXTCLASS	2	00	Auxiliary
Q_TEXTDISPLAY	1	0	no, as soon until events fulfilled
D_TEXTDISPLAY	15	111 1111 1111 1110	327660 Meter
M_MODETEXTDISPLAY	4	1001	System failure
M_LEVELTEXTDISPLAY	3	000	Level 0
L_TEXTDISPLAY	15	000 0000 0000 0000	0 Meter
T_TEXTDISPLAY	10	00 0000 0000	0 sec
M_MODETEXTDISPLAY	4	1001	System failure
M_LEVELTEXTDISPLAY	3	000	Level 0
Q_TEXTCONFIRM	2	00	No confirmation required
L_TEXT	8	0001 0000	16 Chars
X_TEXT	128	...	Text messsage...

Encoded messages example

ACK M1: 00120000020A9203A2105E048000062105DFD0000000000

MAC: 80B7557F31566DBB

ACK M2: 00120000020A9203AAE360078000006AE360000000000000

MAC: 80B7557F31566DBB

FORG M: continue at 600km/h; display “Z|1MB\%<w*RRf)8n/”

030CD3C677A100000021F01C651FF809C4080000000007E4801
B90FFFD2000000120105A7C314D42253C772A525266293 86E2F

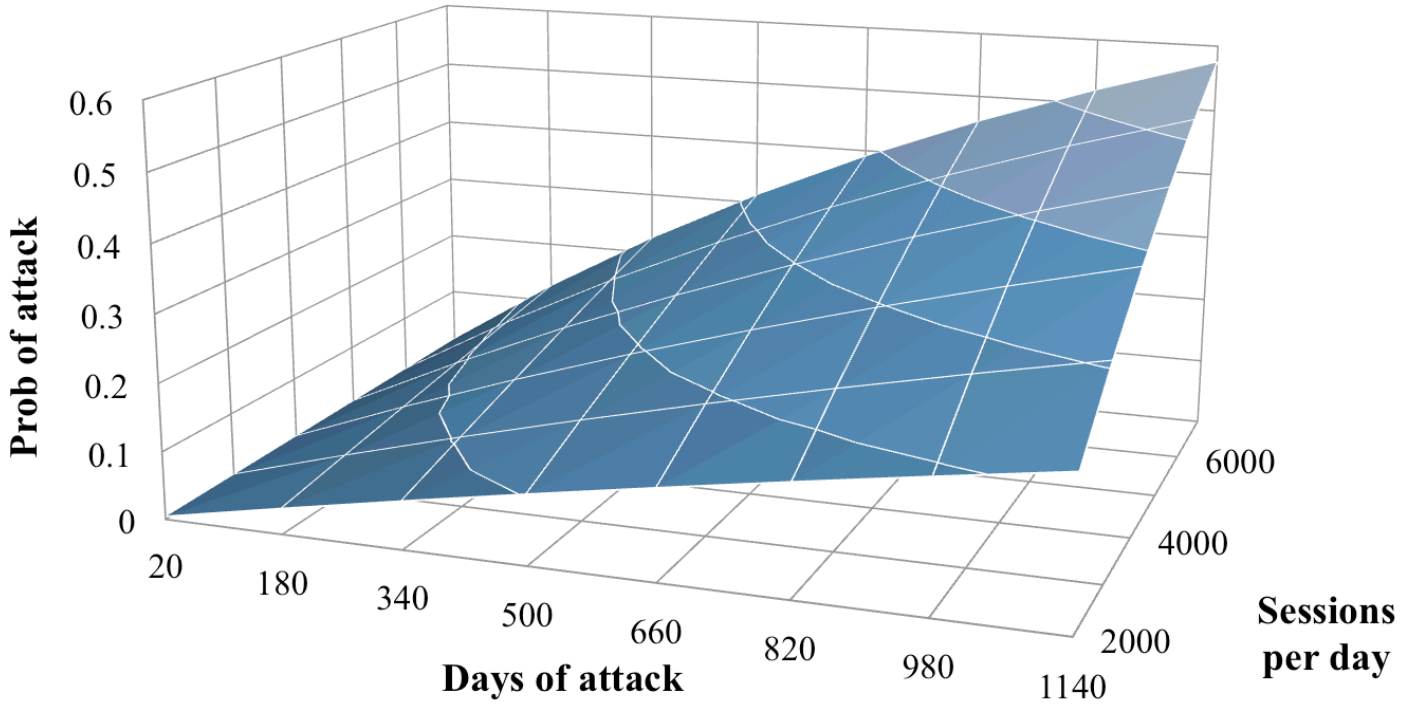
MAC: 80B7557F31566DBB

Likelihood

1. The attack depends on the ability to discover a collision (assuming that the key used by DES can be brute-forced).

2. Cipher collisions depends on the ability to capture the right amount of traffic.

Likelihood



$$P_{collision} = 1 - \prod_{i=1}^{M-1}\left(1 - \frac{i}{N}\right)^{S} \approx 1 - e^{\frac{-M(M-1)}{2N}\cdot S}, N = 2^{64}$$

Likelihood assumptions

- Message collision chance: 1%
- Average message length 32 bytes
- GSM-R speed 10Kbps (14Kbps max)
- UK rail network:
  - 4000 trains per day
  - 10h sessions

Data capture

- 1% chance of collision requires ~600,000,000 messages.
  - *32 byte messages, 10 Kbps bandwidth*
- Safe limit for a EuroRadio session: 19 GB.
- This would require a single session lasting 22 days!
- No threat to current trains.

Data capture

- 1% chance of collision requires ~600,000,000 messages.
  - *32 byte messages, 10 Kbps bandwidth*
- If we could monitor next generation UK rail backbone(s).
  - 4000 trains per day, 10 hour sessions.
- 1% chance of attack in 45 days. 50% chance ~ 8 years
  - This *might* be a problem.

Conclusions

- Every protocol layer of ERTMS has a security flaw
- The specification fails to meet its own safety standards

- Not a problem yet, there are easier ways to crash a train!

- ERTMS is the next gen in rail technology, but has been designed with obsolete ciphers.

Thank you!

Email: m.ordean@cs.bham.ac.uk