

Integrity (I) Codes: Message Integrity Protection and Authentication Over Insecure Channels

Mario Čagalj[†]

Srdjan Čapkun[§]

Ramkumar Rengaswamy[‡]

Ilias Tsigkogiannis[‡]

Mani Srivastava[‡]

Jean-Pierre Hubaux[†]

[†]EPFL

[§]Technical University of Denmark

[‡]UCLA

May 23, 2006

- ▶ Common wisdom
 - ▷ Any security system is only as secure as its weakest link
 - ▷ Weakest link commonly the user, given that the considered system is not user-friendly
- ▶ Folk theorem:

User-unfriendliness \Rightarrow security systems highly insecure

Problem Statement

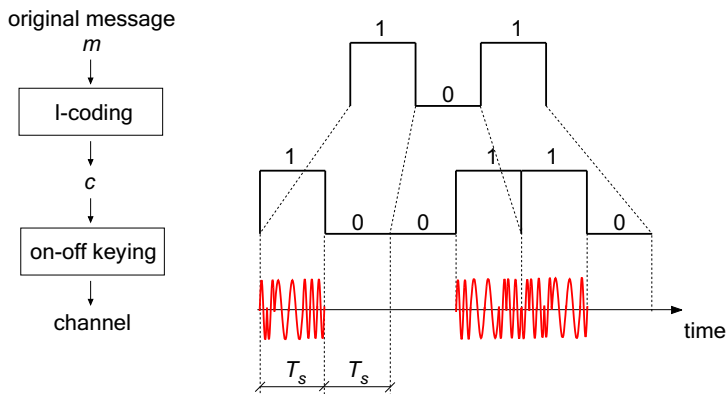
Alice $\xrightarrow{\text{message}}$ Bob

- ▶ “ $\xrightarrow{\text{message}}$ ” public (insecure) radio channel
- ▶ Alice and Bob within each others' transmission range
- ▶ Alice and Bob share neither secrets nor certified public keys
- ▶ How to preserve the integrity of the “message”, while minimizing the users' involvement?

Existing Approaches

- ▶ Users share prior context
 - ▷ Certified public keys
 - ▷ Passwords (Bellovin and Merritt - PAKE)
- ▶ No prior context
 - ▷ Physical contact (Stajano and Anderson)
 - ▷ Location limited infrared channel (Balfanz et al.)
 - ▷ Hash visualization (Perrig and Song)
 - ▷ Hash functions to readable words (Dohrmann and Ellison)
 - ▷ Seeing is believing (McCune, Perrig and Reiter)
 - ▷ Short string comparison (Čagalj, Čapkun and Hubaux)

Integrity Coding and a Radio Channel



- ▶ The **presence** or **absence** of energy in a given time slot of duration T_s conveys information

Definition

An integrity code is a triple $(\mathcal{S}, \mathcal{C}, e)$, where the following conditions are satisfied:

- 1 \mathcal{S} is a finite set of possible source states (plaintext)
- 2 \mathcal{C} is a finite set of codewords
- 3 e is a source encoding rule $e : \mathcal{S} \rightarrow \mathcal{C}$, satisfying the following:
 - ▷ e is an injective function
 - ▷ it is not possible to convert codeword $c \in \mathcal{C}$ to another codeword $c' \in \mathcal{C}$, such that $c' \neq c$, without changing at least one bit 1 of c to bit 0.

I-code Example: Complementary Encoding

- ▶ Complementary encoding rule (Manchester) e :

$$1 \longrightarrow 10$$

$$0 \longrightarrow 01$$

- ▶ $\mathcal{S} = \{00, 01, 10, 11\} \xrightarrow{e} \mathcal{C} = \{0101, 0110, 1001, 1010\}$

$$0101 \longrightarrow 0111$$

$$0101 \longrightarrow 1101$$

$$0101 \longrightarrow 1111$$

$$0110 \longrightarrow 0111$$

$$0110 \longrightarrow 1111$$

$$0110 \longrightarrow 1110$$

► Assumptions

- 1 Sender and receiver are in synch wrt. the beginning and the end of c
- 2 Adversary cannot block (annihilate) signal 1 (except with ε)

Theorem

The adversary cannot trick the receiver into accepting the message \hat{m} when $m \neq \hat{m}$ is sent, except with ε probability.

► Proof:

- ▷ $\hat{m} \neq m \Rightarrow \hat{c} \neq c$ (I-code)
- ▷ $c \rightarrow \hat{c}$ implies at least one bit 1 of c to bit 0 (I-code)
- ▷ Adversary has to annihilate some of the emitted signals (with ε prob.)
q.e.d.

Synchronization via Incongruous (i) Delimiters

Definition (informal)

Given \mathcal{C} , i -delimiter is a *minimum-length* bit string such that any valid codeword $c \in \mathcal{C}$ received between two consecutive i -delimiters is authentic.

- ▶ Example (complementary encoding)

$$\mathcal{S} = \{0, 1, 00, 01, \dots, \underbrace{11 \dots 1}_k\}, \quad \mathcal{C} = \{01, 10, 0101, 0110, \dots, \underbrace{1010 \dots 10}_{2k}\}$$

$$\dots \underbrace{111000}_{i\text{-delimiter}} \overbrace{1010011001}^c \underbrace{111000}_{i\text{-delimiter}} \overbrace{1010011001}^c \underbrace{111000}_{i\text{-delimiter}} \dots$$

- ▶ Receiver does not have to know the length of the c in advance
- ▶ “Correct” c , received between two subsequent i -delimiters is authentic

Synchronization via Incongruous (i) Delimiters

Definition (informal)

Given \mathcal{C} , i -delimiter is a *minimum-length* bit string such that any valid codeword $c \in \mathcal{C}$ received between two consecutive i -delimiters is authentic.

- ▶ Example (complementary encoding)

$$\mathcal{S} = \{0, 1, 00, 01, \dots, \underbrace{11 \dots 1}_k\}, \quad \mathcal{C} = \{01, 10, 0101, 0110, \dots, \underbrace{1010 \dots 10}_{2k}\}$$

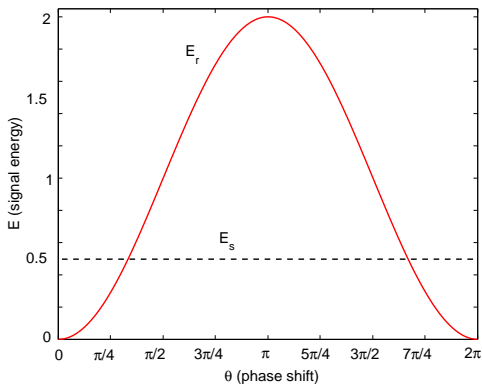
$$\dots \underbrace{111000}_{i\text{-delimiter}} \overbrace{1010011001}^c \underbrace{111000}_{i\text{-delimiter}} \overbrace{1010011001}^c \underbrace{111000}_{i\text{-delimiter}} \dots$$

- ▶ Receiver does not have to know the length of the c in advance
- ▶ “Correct” c , received between two subsequent i -delimiters is authentic

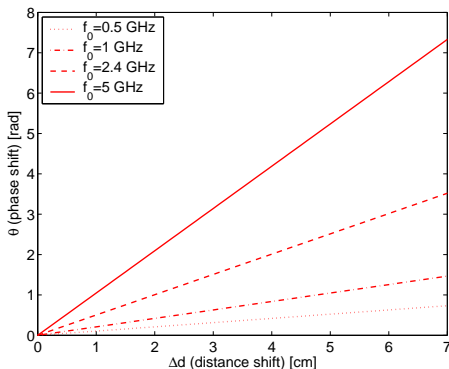
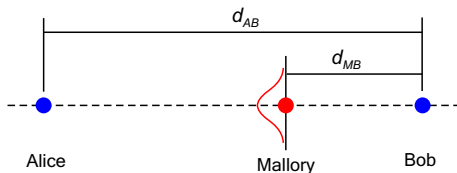
Anti-blocking Property of a Radio Channel ($1 \rightarrow 0$)

$$\underbrace{r(t)}_{\text{receiver}} = \underbrace{\cos(\omega_0 t)}_{\text{sender}} - \underbrace{\cos(\omega_0 t - \theta)}_{\text{adversary}}, \text{ where } \theta \in [0, 2\pi)$$

$$E_r = \int_0^{T_s} r^2(t) dt$$
$$\approx 2T_s \sin^2\left(\frac{\theta}{2}\right)$$



Anti-blocking Property of a Radio Channel ($1 \rightarrow 0$)



Anti-blocking Property of a Radio Channel ($1 \rightarrow 0$)

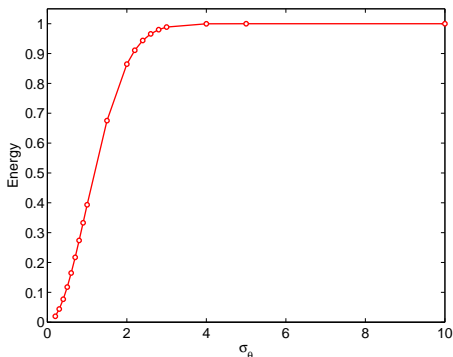
$$\underbrace{R(t)}_{\text{receiver}} = \underbrace{\cos(\omega_0 t + \Phi)}_{\text{sender}} - \underbrace{\cos(\omega_0 t - \Theta)}_{\text{adversary}}, \quad \Phi \in_{\mathcal{U}} [0, 2\pi)$$

- ▶ Θ a random variable (example, $\Phi = 0$)
 - ▷ Energy content $\mathcal{E}_R = \mathbb{E} \left[\int_0^T R^2(t) dt \right] \approx T$, for uniform Θ
 - ▷ Gaussian Distribution of Θ with zero mean and variance σ_θ^2

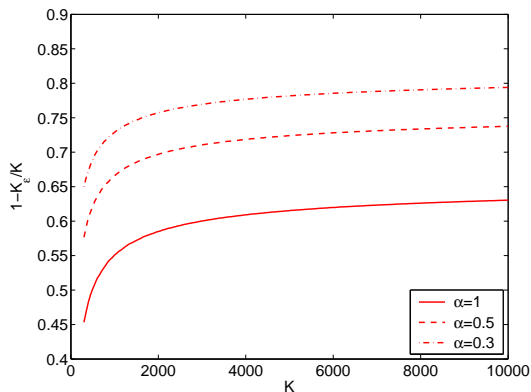
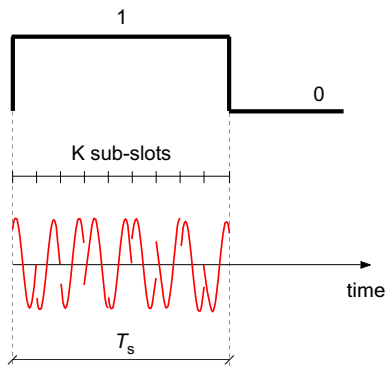
$$\sigma_\theta^2 = (2\pi f_0/c)^2 \sigma_d^2$$

$$f_0 = 5\text{GHz},$$

$$\sigma_\theta = 1.189 \text{ rad} \Leftrightarrow \sigma_d = 1.14 \text{ cm}$$



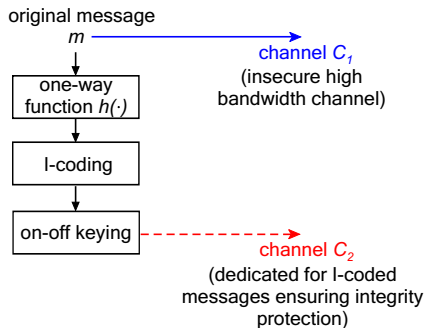
Randomization at the Sender



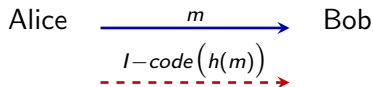
$$\mathbb{P}[K_{\text{attenuated}} \leq K_\epsilon] \geq 1 - \epsilon, \quad \epsilon = 10^{-14}$$

Applications of I-codes

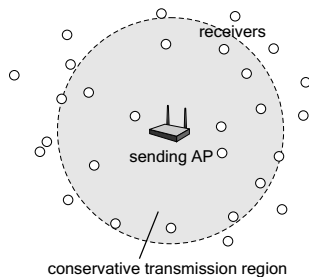
► Authentication through presence (radio channel)



► Solving our initial problem

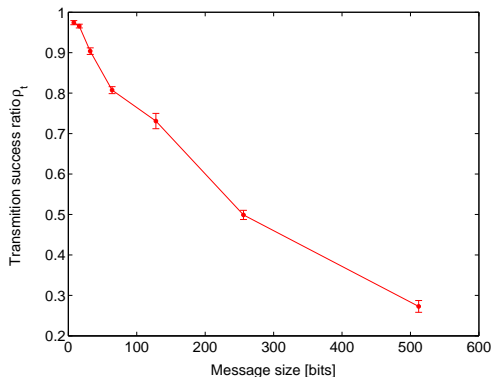


- ▶ Broadcast Authentication
 - ▶ Access Point Authentication

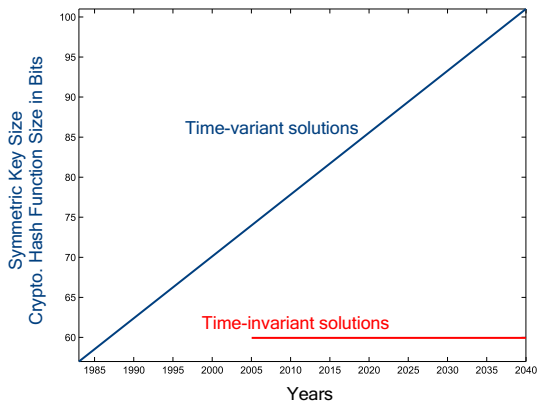


Implementation of I-codes

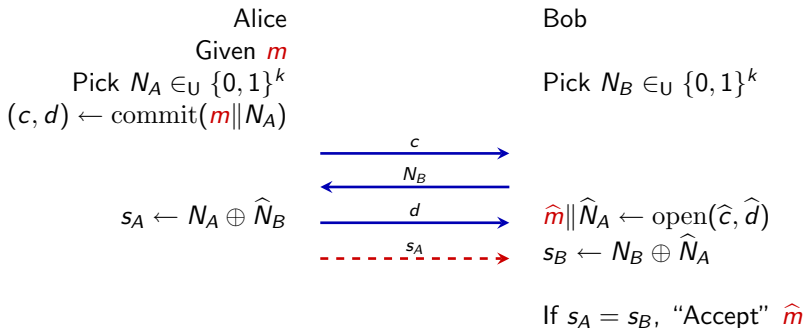
- ▶ Mica2 sensor networking platform (UCLA SOS operating system)
 - ▷ Frequency Shift Keying, output power -20 to 10 dBm
- ▶ Complementary encoding
 - ▷ Every bit 1 transmitted as an 48-bit packet ($T_s = 10$ ms)
 - ▷ Every bit 0 transmitted as an absence of signal ($T_s = 10$ ms)



Time-invariance



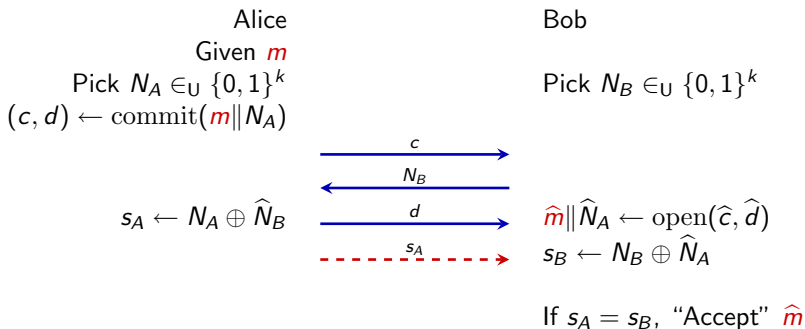
Optimal Message Transfer (MT) Authenticator¹



- ▶ Transmit s_A using I-codes
- ▶ Free choice of the size of s_A (e.g., 50 bits)
- ▶ **Time-invariant solution**

¹Čagalj, Čapkun and Hubaux. "Key Agreement in Peer-to-Peer Wireless Networks". *Proceedings of the IEEE (Special Issue on Cryptography and Security)*, 2006.

Optimal Message Transfer (MT) Authenticator¹



- ▶ Transmit s_A using I-codes
- ▶ Free choice of the size of s_A (e.g., 50 bits)
- ▶ **Time-invariant solution**

¹Čagalj, Čapkun and Hubaux. "Key Agreement in Peer-to-Peer Wireless Networks". *Proceedings of the IEEE (Special Issue on Cryptography and Security)*, 2006.

Summary and Future Work

- ▶ Integrity and authentication without shared keys/certificates (over insecure radio channels)
 - ▷ Anti-blocking property of a radio channel
 - ▷ Location awareness
- ▶ Applications
 - ▷ Walk-in scenarios (AP authentication)
 - ▷ Broadcast authentication with low-power devices (Mica2 sensor platform)
 - ▷ P2P and group key establishment
- ▶ Authentication through presence

Future work: Application of I-codes to a wired channel?