

Thwarting Selfish and Malicious Behavior in Wireless Networks

Mario Čagalj

Ecole Polytechnique Fédérale de Lausanne (EPFL)

January 16, 2006

This thesis is concerned with several security issues in wireless networks

- ▶ Selfish Behavior at the Medium Access Control (MAC) Layer
- ▶ Anti-Jamming Techniques in Sensor Networks
- ▶ Message Integrity Protection and Secure Key Agreement

Thesis Outline

This thesis is concerned with several security issues in wireless networks

- ▶ Selfish Behavior at the Medium Access Control (MAC) Layer
- ▶ Anti-Jamming Techniques in Sensor Networks
- ▶ Message Integrity Protection and Secure Key Agreement

This thesis is concerned with several security issues in wireless networks

- ▶ Selfish Behavior at the Medium Access Control (MAC) Layer
- ▶ Anti-Jamming Techniques in Sensor Networks
- ▶ Message Integrity Protection and Secure Key Agreement

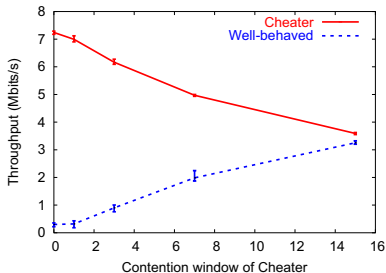
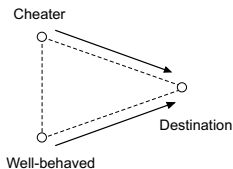
This thesis is concerned with several security issues in wireless networks

- ▶ Selfish Behavior at the Medium Access Control (MAC) Layer
- ▶ Anti-Jamming Techniques in Sensor Networks
- ▶ Message Integrity Protection and Secure Key Agreement

Selfish Behavior in CSMA/CA Networks

Introduction

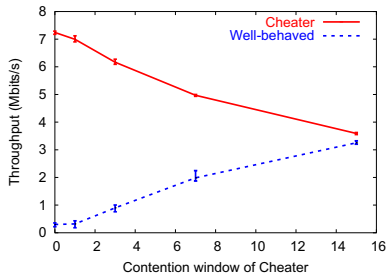
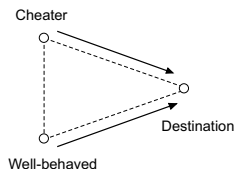
- ▶ CSMA/CA
 - ▷ The most popular MAC paradigm for wireless networks
 - ▷ Relies on a (fair) random deferment of packet transmission
 - ▷ Efficient if nodes follow predefined rules
- ▶ However, the users have a **rational motive to cheat**



- ▶ Understand the coexistence of a population of greedy users
- ▶ Derive the conditions for their stable and optimal functioning

Introduction

- ▶ CSMA/CA
 - ▷ The most popular MAC paradigm for wireless networks
 - ▷ Relies on a (fair) random deferment of packet transmission
 - ▷ Efficient if nodes follow predefined rules
- ▶ However, the users have a **rational motive to cheat**

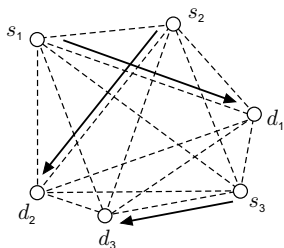


- ▶ Understand the coexistence of a population of greedy users
- ▶ Derive the conditions for their stable and optimal functioning

- ▶ Aloha
 - ▷ MacKenzie and Wicker '03 (perfect information)
 - ▷ Altman et al. '02 (a game with partial information)
 - ▷ Jin and Kesidis '02 (a heterogeneous setting)
- ▶ IEEE 802.11
 - ▷ Konorski '02 (misbehavior-resilient backoff algorithm)
 - ▷ Kyasanur and Vaidya '03 (the receiver assigns the backoff value to the sender)

Network Model and Assumptions

- ▶ N pairs, a subset \mathcal{I} of I sending nodes are **cheaters** ($|\mathcal{I}| = I$)
- ▶ IEEE 802.11, MAC layer authentication (one ID per stations)
- ▶ No hidden terminals (single collision domain)
- ▶ Nodes always have packets (of the same size) to transmit



Cheating Technique

- ▶ **Contention window size**-based cheating, that is, $\forall i \in \mathcal{I}$
 - ▷ No exponential backoff
 - ▷ Cheater i chooses $W_i \in \{1, 2, \dots, W_{max}, W_\infty\}$,
($W_{max} < \infty$, $W_i = W_\infty$ means cheater i chooses not to transmit)
 - ▷ Cheater i defers transmissions for the period proportional to a value chosen uniformly at random from $\{1, 2, \dots, W_i\}$ (for $W_i < W_\infty$)
- ▶ The cheating model reflects the real-life implementation

Game Theoretic Model

- ▶ CSMA/CA static game - $G_{\text{CSMA/CA}}$
 - ▶ Set of players \mathcal{I} and for every $i \in \mathcal{I}$
 - ▶ Pure-strategy set $S_i \stackrel{\text{def}}{=} \{1, 2, \dots, W_{\text{max}}, W_{\infty}\}$
 - ▶ Utility function $u_i(W) \stackrel{\text{def}}{=} r_i(W)$, where $W = (W_k)_{k=1}^N$
 - ▶ Move consists in choosing $W_i \in S_i$
- ▶ Solution concept to $G_{\text{CSMA/CA}}$ - **Nash equilibrium (NE)**
 - ▶ W is a NE point if no player $i \in \mathcal{I}$ can increase his/her payoff by unilaterally deviating from W ,
 - ▶ That is, $\forall i \in \mathcal{I}$, we have $u_i(\underbrace{W_i, W_{-i}}_W) \geq u_i(\underbrace{\widehat{W}_i, W_{-i}}_{\widehat{W}})$, $\forall \widehat{W}_i \in S_i$
- ▶ We often neglect “well-behaved” nodes (i.e., $N = I$)

Game Theoretic Model

- ▶ CSMA/CA static game - $G_{\text{CSMA/CA}}$
 - ▶ Set of players \mathcal{I} and for every $i \in \mathcal{I}$
 - ▶ Pure-strategy set $S_i \stackrel{\text{def}}{=} \{1, 2, \dots, W_{\max}, W_{\infty}\}$
 - ▶ Utility function $u_i(W) \stackrel{\text{def}}{=} r_i(W)$, where $W = (W_k)_{k=1}^N$
 - ▶ Move consists in choosing $W_i \in S_i$
- ▶ Solution concept to $G_{\text{CSMA/CA}}$ - **Nash equilibrium (NE)**
 - ▶ W is a NE point if no player $i \in \mathcal{I}$ can increase his/her payoff by unilaterally deviating from W ,
 - ▶ That is, $\forall i \in \mathcal{I}$, we have $u_i(\underbrace{W_i, W_{-i}}_W) \geq u_i(\underbrace{\widehat{W}_i, W_{-i}}_{\widehat{W}})$, $\forall \widehat{W}_i \in S_i$
- ▶ We often neglect “well-behaved” nodes (i.e., $N = I$)

Characterization of Utility Functions U_i

▶ Bianchi's model of IEEE 802.11

- ▷ Every player $i \in \mathcal{I}$ controls its **access probability**

$$\tau_i = \frac{2}{W_i + 1}$$

- ▷ Player $i \in \mathcal{I}$ receives the payoff (ignoring well-behaved nodes)

$$u_i(\tau) \stackrel{\text{def}}{=} r_i(\tau) = \frac{\tau_i c_i^{(1)}(\tau_{-i})}{\tau_i c_i^{(2)}(\tau_{-i}) + c_i^{(3)}(\tau_{-i})}$$

- ▷ $u_i(\cdot)$ is an increasing (decreasing) concave (convex) function in τ_i (W_i)

Lemma

For any W that constitutes a NE in $G_{\text{CSMA}/\text{CA}}$, $\exists i \in \mathcal{I}$ such that $W_i = 1$.

Theorem

The game $G_{\text{CSMA}/\text{CA}}$ admits exactly $(W_{\max} + 1)^I - W_{\max}^I$ (pure) NE.

- ▶ Two families of equilibria ($\mathcal{D} \stackrel{\text{def}}{=} \{i : W_i = 1, \forall i \in \mathcal{I}\}$)
 - 1 Only one player receives a non-null payoff, $|\mathcal{D}| = 1$
 - 2 The tragedy of the commons, $|\mathcal{D}| > 1$
- ▶ Examples
 - 1 $W = (1, W_{\infty}, \dots, W_{\infty})$ (Pareto-optimal NE)
 - 2 $W = (1, 1, \dots, 1)$, $W = (W_1, 1, \dots, 1)$ with $W_1 < W_{\infty}$

Lemma

For any W that constitutes a NE in $G_{\text{CSMA}/\text{CA}}$, $\exists i \in \mathcal{I}$ such that $W_i = 1$.

Theorem

The game $G_{\text{CSMA}/\text{CA}}$ admits exactly $(W_{\max} + 1)^I - W_{\max}^I$ (pure) NE.

- ▶ Two families of equilibria ($\mathcal{D} \stackrel{\text{def}}{=} \{i : W_i = 1, \forall i \in \mathcal{I}\}$)
 - 1 Only one player receives a non-null payoff, $|\mathcal{D}| = 1$
 - 2 The tragedy of the commons, $|\mathcal{D}| > 1$
- ▶ Examples
 - 1 $W = (1, W_\infty, \dots, W_\infty)$ (Pareto-optimal NE)
 - 2 $W = (1, 1, \dots, 1)$, $W = (W_1, 1, \dots, 1)$ with $W_1 < W_\infty$

Robustness of the Nash Equilibria

- ▶ Unlikely to know u_i exactly (the effect on the NE of $G_{\text{CSMA/CA}}$?)
- ▶ Define an approximate game $\widehat{G}_{\text{CSMA/CA}}$ to $G_{\text{CSMA/CA}}$, with

$$\widehat{u}_i(W) = u_i(W) - \begin{cases} \varepsilon, & \text{if } W_i < W_\infty; \\ 0, & \text{if } W_i = W_\infty, \end{cases} \quad (0 < \varepsilon \ll 1)$$

Definition (informal)

A Nash equilibrium W of $G_{\text{CSMA/CA}}$ is robust (essential) if there exists a Nash equilibrium \widehat{W} of $\widehat{G}_{\text{CSMA/CA}}$ that is *arbitrarily close* to W . The game is essential if all its equilibrium points are robust (essential).

Theorem

The Nash equilibrium $W = (W_i = 1)_{i \in \mathcal{I}}$ of the $G_{\text{CSMA/CA}}$ is not robust, and therefore the $G_{\text{CSMA/CA}}$ is *nonessential*.

Robustness of the Nash Equilibria

- ▶ Unlikely to know u_i exactly (the effect on the NE of $G_{\text{CSMA/CA}}$?)
- ▶ Define an approximate game $\widehat{G}_{\text{CSMA/CA}}$ to $G_{\text{CSMA/CA}}$, with

$$\widehat{u}_i(W) = u_i(W) - \begin{cases} \varepsilon, & \text{if } W_i < W_\infty; \\ 0, & \text{if } W_i = W_\infty, \end{cases} \quad (0 < \varepsilon \ll 1)$$

Definition (informal)

A Nash equilibrium W of $G_{\text{CSMA/CA}}$ is robust (essential) if there exists a Nash equilibrium \widehat{W} of $\widehat{G}_{\text{CSMA/CA}}$ that is *arbitrarily close* to W . The game is essential if all its equilibrium points are robust (essential).

Theorem

The Nash equilibrium $W = (W_i = 1)_{i \in \mathcal{I}}$ of the $G_{\text{CSMA/CA}}$ is not robust, and therefore the $G_{\text{CSMA/CA}}$ is *nonessential*.

How to Avoid Undesirable Outcomes?

- ▶ $G_{\text{CSMA/CA}}$ equilibria: multiple, highly unfair or highly inefficient
- ▶ $G_{\text{CSMA/CA}}$ is nonessential (hard to predict the outcome)
- ▶ Desirable solution
 - ▷ Uniqueness
 - ▷ Fairness
 - ▷ Pareto-optimality

Uniqueness, Fairness and Pareto-optimality

- ▶ Use **Nash bargaining framework**

$$\begin{array}{ll} \Pi_1 : \text{maximize} & \prod_{i \in \mathcal{I}} (u_i - u_i^\circ) \\ \text{subject to} & u \in U \\ & u \geq u^\circ . \end{array} \quad \Rightarrow \quad \begin{array}{ll} \Pi_2 : \text{maximize} & \sum_{i \in \mathcal{I}} \log u_i(\tau) \\ \text{subject to} & 0 \leq \tau \leq 1 . \end{array}$$

- ▶ U - set of feasible points, $u^\circ \stackrel{\text{def}}{=}} (u_i^\circ = 0)_{i \in \mathcal{I}}$ - **disagreement point**

Theorem

The problem Π_2 admits the unique solution $(\tau_i = \tau^*)_{i \in \mathcal{I}}$, with $\tau^* \in (0, 1)$.

Conjecture

The problem Π_1 admits a unique, fair and Pareto-optimal solution satisfying $W_i = W^*$, $(W^* \in S_i)$, $\forall i \in \mathcal{I}$.

Uniqueness, Fairness and Pareto-optimality

- ▶ Use Nash bargaining framework

$$\begin{array}{ll} \Pi_1 : \text{maximize} & \prod_{i \in \mathcal{I}} (u_i - u_i^\circ) \\ \text{subject to} & u \in U \\ & u \geq u^\circ . \end{array} \quad \Rightarrow \quad \begin{array}{ll} \Pi_2 : \text{maximize} & \sum_{i \in \mathcal{I}} \log u_i(\tau) \\ \text{subject to} & 0 \leq \tau \leq 1 . \end{array}$$

- ▶ U - set of feasible points, $u^\circ \stackrel{\text{def}}{=}} (u_i^\circ = 0)_{i \in \mathcal{I}}$ - disagreement point

Theorem

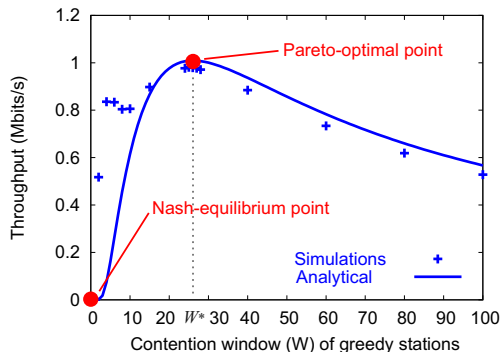
The problem Π_2 admits the unique solution $(\tau_i = \tau^*)_{i \in \mathcal{I}}$, with $\tau^* \in (0, 1)$.

Conjecture

The problem Π_1 admits a unique, fair and Pareto-optimal solution satisfying $W_i = W^*$, $(W^* \in S_i)$, $\forall i \in \mathcal{I}$.

Pareto-optimal but not Nash Equilibrium

- ▶ “ns-2”-simulations: cheaters have the same W_i ($I = 10, 2 \text{ Mb/s}$)



- ▶ Apply the theory of **repeated games** to transform PO point into NE

Repeated Game ($G_{\text{CSMA/CA}}^\infty$) Model

- ▶ $G_{\text{CSMA/CA}}^\infty$: the game $G_{\text{CSMA/CA}}$ played repeatedly over time
 - ▶ Utility function

$$u_i^\infty = \liminf_{T \rightarrow \infty} \frac{1}{T} \sum_{t=1}^T u_i^t(\tau)$$

- ▶ Stage t payoff

$$u_i^t(\tau) = r_i^t(\tau) - p_i^t(\tau)$$

- ▶ Penalty function

$$p_i^t(\tau) = \begin{cases} \varphi_i^t(\tau), & \tau^* < \tau_i^t \leq 1; \\ 0, & 0 \leq \tau_i^t \leq \tau^*, \end{cases}$$

with $\tau^* \in (0, 1)$ and $\frac{\partial}{\partial \tau_i} \varphi_i^t(\tau) > \frac{\partial}{\partial \tau_i} r_i^t(\tau)$

- ▶ Solution concept - **Subgame Perfect Nash Equilibrium (SPNE)**

Definition (SPNE)

Strategy profile $\tau = (\tau_i^t)_{i \in \mathcal{I}, t = \{1, \dots, T\}}$ is a SPNE if it induces a NE in every *subgame* of the $G_{\text{CSMA/CA}}^\infty$.

- ▶ If $(\tau_i^t)_{i \in \mathcal{I}, t = \{1, \dots, T\}}$ is a NE of the $G_{\text{CSMA/CA}}^\infty$, then $(\tau_i^t)_{i \in \mathcal{I}, t = \{k, \dots, T\}}$ is a NE of the subgame $G_{\text{CSMA/CA}}^{k, \infty}$ for every k

Theorem

Strategy profile $(\tau_i^t = \tau^*)_{i \in \mathcal{I}, t = \{1, \dots, T\}}$ is a SPNE of the $G_{\text{CSMA/CA}}^\infty$.

- ▶ Solution concept - **Subgame Perfect Nash Equilibrium (SPNE)**

Definition (SPNE)

Strategy profile $\tau = (\tau_i^t)_{i \in \mathcal{I}, t = \{1, \dots, T\}}$ is a SPNE if it induces a NE in every *subgame* of the $G_{\text{CSMA/CA}}^\infty$.

- ▶ If $(\tau_i^t)_{i \in \mathcal{I}, t = \{1, \dots, T\}}$ is a NE of the $G_{\text{CSMA/CA}}^\infty$, then $(\tau_i^t)_{i \in \mathcal{I}, t = \{k, \dots, T\}}$ is a NE of the subgame $G_{\text{CSMA/CA}}^{k, \infty}$ for every k

Theorem

Strategy profile $(\tau_i^t = \tau^*)_{i \in \mathcal{I}, t = \{1, \dots, T\}}$ is a SPNE of the $G_{\text{CSMA/CA}}^\infty$.

Practical Penalty Function p_i

- ▶ Player $k \in \mathcal{I}$ **selectively jams** $i \in \mathcal{I} \setminus \{k\}$ for which $r_i(\tau) > r_k(\tau)$
- ▶ Penalty evaluation

$$p_i^t(\tau) = \begin{cases} r_i(\tau) - r_k(\tau), & \text{if } r_i(\tau) > r_k(\tau); \\ 0, & \text{otherwise .} \end{cases}$$

- ▶ Implications

- ▶ $\tau^* = \min_{k \in \mathcal{I}} \{\tau_k\}$ is a **SPNE**
- ▶ Equal payoffs for all the players, i.e., $r_i(\tau) = r_k(\tau)$, $\forall i, k \in \mathcal{I}$

- ▶ Implementation

$$T^{jam} = T^{obs} \times \frac{\bar{r}_i(t, T^{obs}) - \bar{r}_k(t, T^{obs})}{\bar{r}_k(t + T^{obs}, T^{jam})}$$

Practical Penalty Function p_i

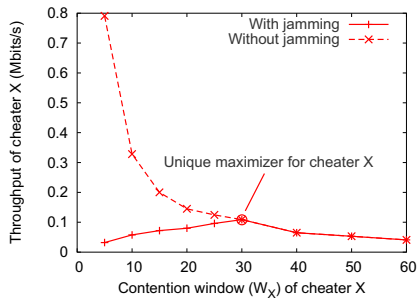
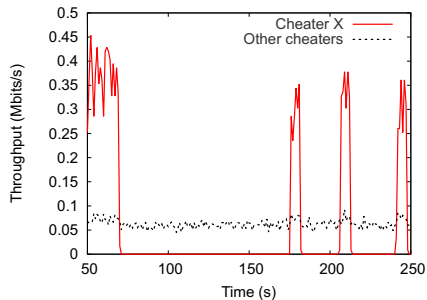
- ▶ Player $k \in \mathcal{I}$ **selectively jams** $i \in \mathcal{I} \setminus \{k\}$ for which $r_i(\tau) > r_k(\tau)$
- ▶ Penalty evaluation

$$p_i^t(\tau) = \begin{cases} r_i(\tau) - r_k(\tau), & \text{if } r_i(\tau) > r_k(\tau); \\ 0, & \text{otherwise .} \end{cases}$$

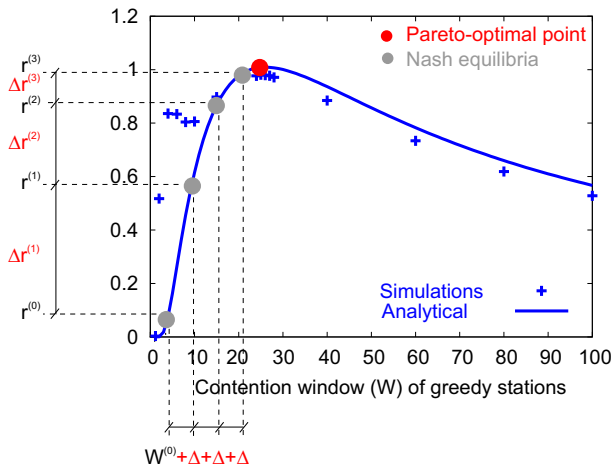
- ▶ Implications
 - ▷ $\tau^* = \min_{k \in \mathcal{I}} \{\tau_k\}$ is a **SPNE**
 - ▷ Equal payoffs for all the players, i.e., $r_i(\tau) = r_k(\tau)$, $\forall i, k \in \mathcal{I}$
- ▶ Implementation

$$T^{jam} = T^{obs} \times \frac{\bar{r}_i(t, T^{obs}) - \bar{r}_k(t, T^{obs})}{\bar{r}_k(t + T^{obs}, T^{jam})}$$

Example: Penalization



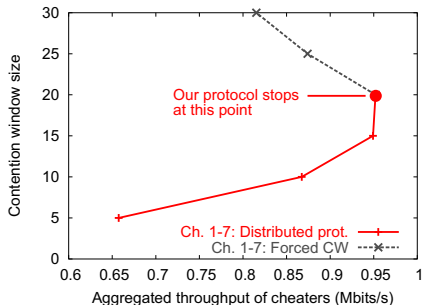
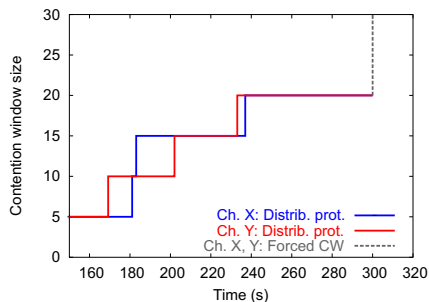
Transforming the Pareto-optimal Point to a NE



- ▶ Continue the game until $|\Delta r^{(t)}| > \epsilon$

Fully Distributed Implementation

- “ns-2”-simulations: $N = 20$, $I = 7$ and step size $\Delta = 5$



Summary

- ▶ CSMA/CA game $G_{\text{CSMA/CA}}$ admits $(W_{\text{max}} + 1)^I - W_{\text{max}}^I$ pure NE
 - ▷ (1st family) Only one player receives non-null payoff
 - ▷ (2st family) The tragedy of the commons
- ▶ $G_{\text{CSMA/CA}}$ is nonessential
 - ▷ The tragedy of the commons NE are not robust
- ▶ Unique Pareto-optimal point exhibiting efficiency and fairness
 - ▷ Identified within the Nash Bargaining Framework
 - ▷ Corresponds to the unique Nash Bargaining Solution
- ▶ Transformation of the Pareto-optimal point to a SPNE
 - ▷ Repeated games
 - ▷ Selective jamming

Message Integrity Protection and Secure Key Agreement in Wireless Networks

Optimal Message Transfer (MT) Authenticator

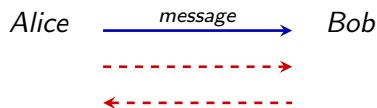
Integrity (I) Codes

Introduction



- ▶ “ $\xrightarrow{\text{message}}$ ” **high-bandwidth** public (insecure) channel
 - ▷ Radio channel, Internet
- ▶ “----->” **low-bandwidth** authenticated channel
 - ▷ Voice, phone, SMS, friends
 - ▷ No secrecy required (only integrity)
- ▶ *Alice* and *Bob* share neither secrets nor certified public keys
- ▶ How to preserve the integrity of the *message* transmitted over the public channel, while minimizing the users' involvement?

Introduction



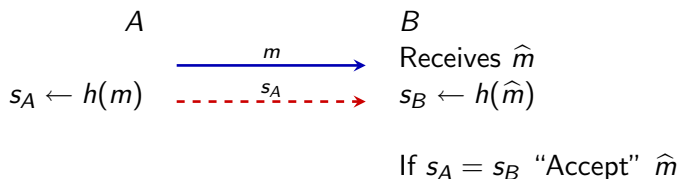
- ▶ “ $\xrightarrow{\hspace{1cm}}$ ” **high-bandwidth** public (insecure) channel
 - ▷ Radio channel, Internet
- ▶ “ $\xrightarrow{\hspace{1cm}}$ ” **low-bandwidth** authenticated channel
 - ▷ Voice, phone, SMS, friends
 - ▷ No secrecy required (only integrity)
- ▶ *Alice* and *Bob* share neither secrets nor certified public keys
- ▶ How to preserve the integrity of the *message* transmitted over the public channel, while minimizing the users' involvement?

Existing Paradigms and Approaches

- ▶ Users share prior context
 - ▷ Passwords (Bellovin and Merritt - PAKE)
 - ▷ Certified public keys
- ▶ 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)
 - ▷ “Folklore” protocols (suboptimal, not delay-tolerant)

Motivation

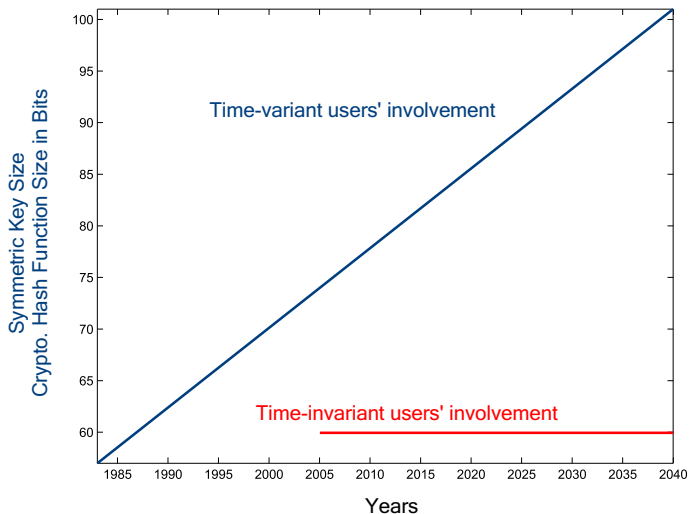
- ▶ Straightforward solution



- ▶ Today, 2nd preimage resistant $h(\cdot)$ implies at least 80-bit s_A
 - ▷ Tomorrow, perhaps 81 bit
 - ▷ In 10 years?
- ▶ Users' involvement **increases** with time
 - ▷ Capacity of the "----->" does not change

Time Invariant Solution

- ▶ Lenstra and Verheul, *Selecting Cryptographic Key Sizes*, 1999



Commitments Schemes

▶ Notation

$$(c, d) \leftarrow \text{commit}(m)$$

$$m \leftarrow \text{open}(c, d)$$

▶ Transforms a value m into a commitment/opening pair (c, d)

▷ c reveals no information about m

▷ (c, d) together reveal m

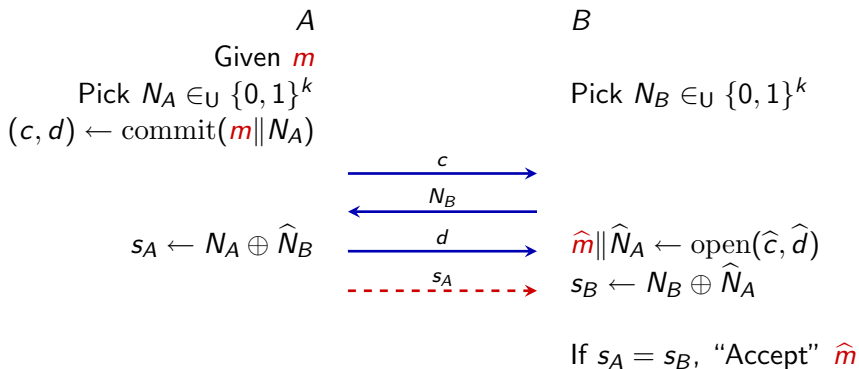
▷ Infeasible to find \hat{d} such that (c, \hat{d}) reveal $\hat{m} \neq m$

▶ Semantic

▷ A user who commits to m (by sending out c) cannot change m afterwards (**binding** property)

▷ m is hidden from the receiver until he/she receives d (**hiding** property)

Optimal Message Transfer (MT) Authenticator



Security of the Optimal MT-authenticator

- ▶ ε - the probability that $\text{commit}(\cdot)$ is broken in time T
- ▶ γ - the maximum number of sessions per user (abortive or successful)
- ▶ Attacker computationally bounded

Theorem

The probability that an attacker succeeds against a targeted user in time T is bounded by $\gamma 2^{-k} + \varepsilon$.

Security of the Optimal MT-authenticator

- ▶ ε - the probability that $\text{commit}(\cdot)$ is broken in time T
- ▶ γ - the maximum number of sessions per user (abortive or successful)
- ▶ Attacker computationally bounded

Theorem

The probability that an attacker succeeds against a targeted user in time T is bounded by $\gamma 2^{-k} + \varepsilon$.

Security Analysis: Proof

- ▶ $C \stackrel{def}{=} \{\text{commit}(\cdot) \text{ broken by anybody in time } T\}$, $Pr[C] \leq \varepsilon \ll 1$
- ▶ \bar{C} complementary event to C
- ▶ $S \stackrel{def}{=} \{\text{the attacker successful against the given user } A \text{ in time } T\}$

$$\begin{aligned} Pr[S] &= Pr[S|C]Pr[C] + Pr[S|\bar{C}]Pr[\bar{C}] \\ &\leq Pr[C] + Pr[S|\bar{C}] \\ &\leq \varepsilon + Pr[S|\bar{C}] \end{aligned} \tag{1}$$

- ▶ $S|\bar{C}$ - the semantics of $\text{commit}(\cdot)$ preserved

$$\begin{aligned} Pr[S|\bar{C}] &= Pr[N_A = N_B \oplus \hat{N}_A \oplus \hat{N}_B] \\ &= Pr[N_B = N_A \oplus \hat{N}_A \oplus \hat{N}_B] \\ &\leq \gamma 2^{-k} \end{aligned} \tag{2}$$

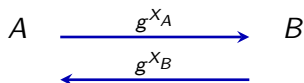
- ▶ (1) and (2) $\Rightarrow Pr[S] \leq \gamma 2^{-k} + \varepsilon$ q.e.d.

Choice of the Parameters γ and k

- ▶ “ $10^{-9} (< 2^{-30})$ satisfactorily small probability” - Lenstra and Verheul, *Selecting Cryptographic Key Sizes*, 1999
- ▶ Example
 - ▷ $\gamma = 2^{20}$ (32 times/day during approximately 89 years)
 - ▷ $k = 50$ implies $P[S] \leq 2^{20} \times 2^{-50} + \epsilon \approx 2^{-30}$
 - ▷ Users' involvement “only” 50 bits (time-invariant)
 - ▷ All the 50 bits contribute to the uncertainty of the attacker (optimality)

From Secure MT-auth. to Secure Key Agreement

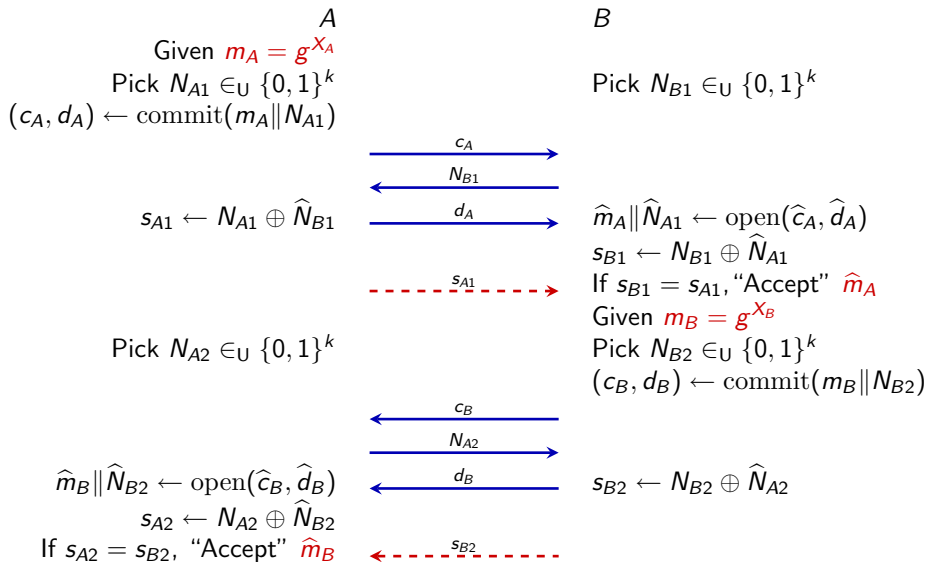
- ▶ Diffie-Hellman (DH) key agreement protocol is “secure” in the **ideal world** (passive attacks)



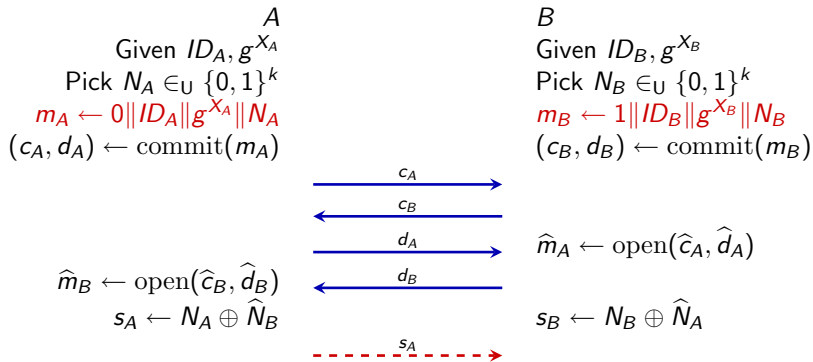
$$K_{AB} = g^{X_A X_B} = \left(g^{X_B}\right)^{X_A} = \left(g^{X_A}\right)^{X_B}$$

- ▶ “Compile” the DH protocol using the optimal MT-authenticator
- ▶ Results in a secure DH protocol in the **real world** (Bellare et al., 1998)

Secure DH Key Agreement Protocol



Secure DH Key Agreement Protocol

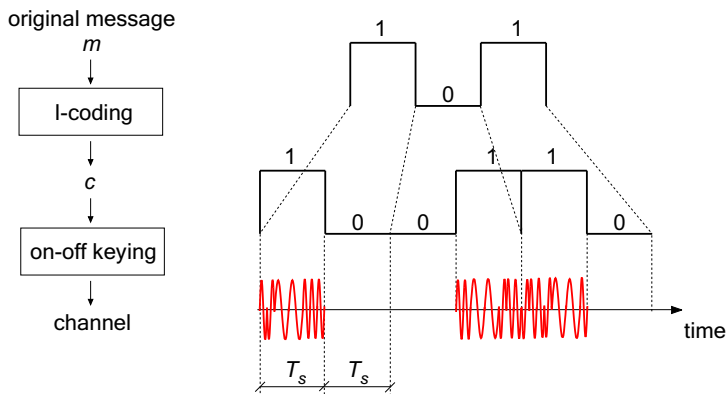


If $s_A = s_B$, "Accept" \hat{m}_A and \hat{m}_B

Summary: Optimal MT-authenticator

- ▶ Novel and re-usable *message transfer* authenticator (MT-SC)
- ▶ Time-invariant solution
- ▶ Optimal trade-off between the security and the user's involvement
- ▶ Novel Diffie-Hellman key agreement protocol (application of MT-SC)

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 e :

1 \longrightarrow 10

0 \longrightarrow 01

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

0101 \longrightarrow 0111

0110 \longrightarrow 0111

0101 \longrightarrow 1101

0110 \longrightarrow 1111

0101 \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:

- 1 $\hat{m} \neq m \Rightarrow \hat{c} \neq c$ (I-code)
- 2 $c \rightarrow \hat{c}$ implies at least one bit 1 of c to bit 0 (I-code)
- 3 Adversary has to annihilate some of the emitted signals (with ε prob.)
q.e.d.

Synchronization via Incongruous (*i*) Delimiters

Definition

Given \mathcal{C} , *i*-delimiter is a *minimum-length* bit string that cannot be transformed to any substring (of subsequent bits) of $c \in \mathcal{C}$ and vice versa.

▶ Example (complementary encoding)

- ▶ $\mathcal{S} = \{0, 1, 00, 01, \dots, \underbrace{11 \dots 1}_k\}$, for $k < \infty$
- ▶ $\mathcal{C} = \{01, 10, 0101, 0110, \dots, \underbrace{1010 \dots 10}_{2k}\}$
- ▶ *i*-delimiter: **111000**



- ▶ 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

Given \mathcal{C} , *i*-delimiter is a *minimum-length* bit string that cannot be transformed to any substring (of subsequent bits) of $c \in \mathcal{C}$ and vice versa.

▶ Example (complementary encoding)

▶ $\mathcal{S} = \{0, 1, 00, 01, \dots, \underbrace{11 \dots 1}_k\}$, for $k < \infty$

▶ $\mathcal{C} = \{01, 10, 0101, 0110, \dots, \underbrace{1010 \dots 10}_{2k}\}$

▶ *i*-delimiter: **111000**

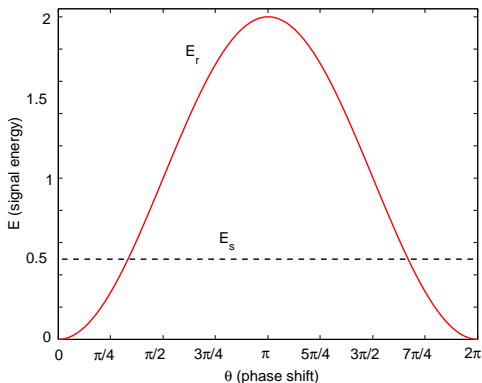
$$\dots \underbrace{111000}_{i\text{-delimiter}} \overbrace{1010011001}^c \underbrace{111000}_{i\text{-delimiter}} \overbrace{1010011001}^c \underbrace{111000}_{i\text{-delimiter}} \dots$$

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

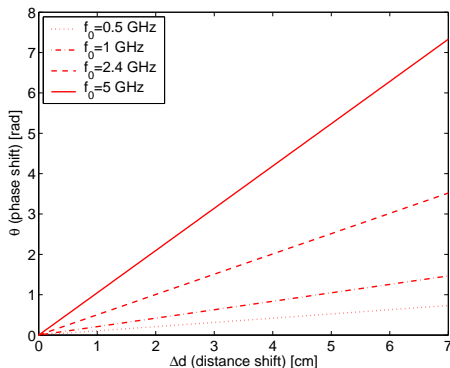
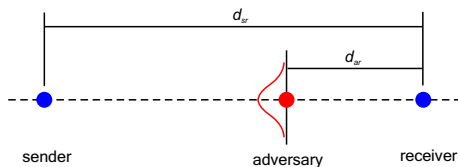
Anti-blocking Property of a Radio Channel

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

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



Anti-blocking Property of a Radio Channel



Anti-blocking Property of a Radio Channel

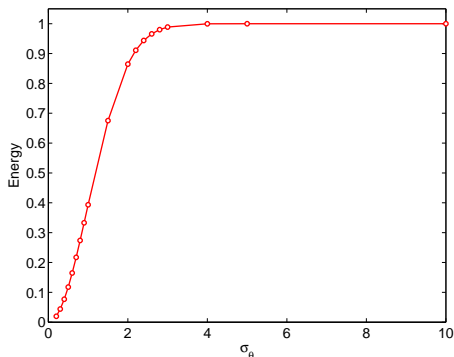
$$\underbrace{R(t)}_{\text{receiver}} = \underbrace{\cos(\omega_0 t + \Phi)}_{\text{sender}} - \underbrace{\cos(\omega_0 t - \Theta)}_{\text{adversary}}, \quad \Phi \in_U [0, 2\pi)$$

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

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

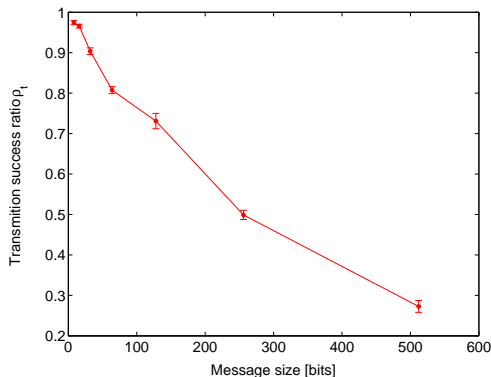
$$f_0 = 5\text{GHz},$$

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



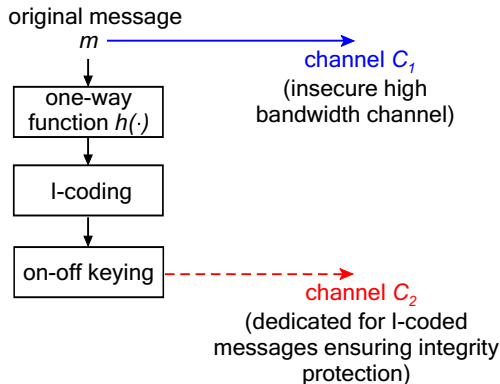
Implementation of I-codes

- ▶ Mica2 sensor networking platform (UCLA SOS operating system)
 - ▷ FSK, output power -20 to 10 dBm, receiver sensitivity -110 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)



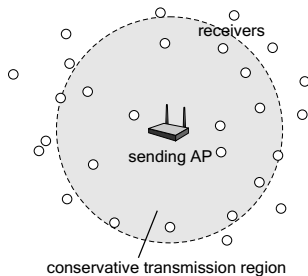
Applications of I-codes

► Authentication through presence (radio channel)



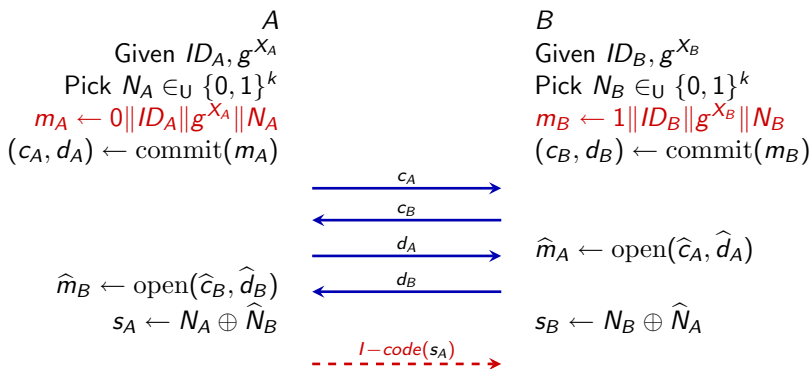
Applications of I-codes

- ▶ Broadcast Authentication
 - ▷ Sensor Networks
 - ▷ Access Point Authentication



Applications of I-codes

► Key Establishment over Insecure Channels



If $s_A = s_B$, "Accept" \hat{m}_A and \hat{m}_B

Summary: I-codes

- ▶ Integrity protection based on message coding
- ▶ Authentication through presence
- ▶ Application of *I*-codes to broadcast authentication and key agreement
- ▶ Implementation of *I*-codes on the Mica2 wireless sensor platform

Selfish Behavior at the Medium Access Control (MAC) Layer

- ▶ A formalism for systematic study of selfish behavior in CSMA/CA networks (game theory)
- ▶ The CSMA/CA *game* admits $(W_{max} + 1)^I - W_{max}^I$ Nash equilibria
- ▶ The *tragedy of the commons* Nash equilibria are *nonessential*
- ▶ Using the Nash Bargaining Framework the Pareto optimal point of operation is identified
- ▶ Transformation of the Pareto optimal point into a Subgame Perfect Nash Equilibrium (repeated games)

Anti-Jamming Techniques in Sensor Networks

- ▶ *Probabilistic wormholes* - the reactive mechanism ensuring timely data delivery
- ▶ Wired pairs of sensor nodes
- ▶ Coordinated frequency-hopping pairs
- ▶ Uncoordinated channel-hopping (requires no synchronization)
- ▶ Appropriate mathematical models

Message Integrity Protection and Secure Key Agreement

- ▶ Novel and re-usable *message transfer* authenticator (MT-SC)
- ▶ MT-SC - optimal trade-off between security and user's involvement
- ▶ Novel Diffie-Hellman key agreement protocol (application of MT-SC)
- ▶ Novel security property called the *integrity region*
- ▶ *Integrity (I) codes* - integrity protection based on message coding
- ▶ Application of *I*-codes to broadcast authentication and key agreement
- ▶ Implementation of *I*-codes on the Mica2 wireless sensor platform

Publications

- ▶ M. Čagalj, S. Čapkun, and J.-P. Hubaux. “**Key agreement in peer-to-peer wireless networks**”. *Proceedings of the IEEE (Special Issue on Security and Cryptography)*, February, 2006.
- ▶ M. Čagalj, J.-P. Hubaux, and C. Enz. “**Energy-Efficient Broadcasting in All-Wireless Networks**”. *Wireless Networks (WINET)*, 11:177–188, 2005.
- ▶ S. Čapkun, M. Čagalj, and M. Srivastava “**Securing Localization With Hidden and Mobile Base Stations**”. *IEEE INFOCOM '06*.
- ▶ M. Čagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux. “**On Selfish Behavior in CSMA/CA Networks**”. *IEEE INFOCOM '05*.
- ▶ M. Čagalj, J.-P. Hubaux, and C. Enz. “**Minimum-Energy Broadcast in All-Wireless Networks: NP-Completeness and Distribution Issues**”. *MOBICOM '02*.

Submitted for publishing

- ▶ M. Čagalj, S. Čapkun, and J.-P. Hubaux. “**Wormhole Defense: New Anti-Jamming Techniques in Sensor Networks**”, 2005.
- ▶ M. Čagalj, S. Čapkun, and J.-P. Hubaux. “**Integrity (*I*) codes: Message Integrity Protection and Authentication Over Insecure Channels**”, 2005.
- ▶ S. Čapkun, M. Čagalj, and J.-P. Hubaux. “**Uncoordinated Frequency Hopping: Anti-jamming Communication Without a Shared Secret Key**”, 2005.

Directions for Future Work

- ▶ Selfish behavior in wireless networks of general topology
- ▶ Implementation of anti-jamming techniques for sensor networks
- ▶ Extension of the Optimal MT-authenticator to group settings
- ▶ Implementation of I-codes for IEEE 802.11 networks