Selected Topics in Wireless Security

Bertinoro PhD. Summer School, July 2009

Radha Poovendran
Network Security Lab
Electrical Engineering Department
University of Washington, Seattle, WA
http://www.ee.washington.edu/research/nsl

Outline

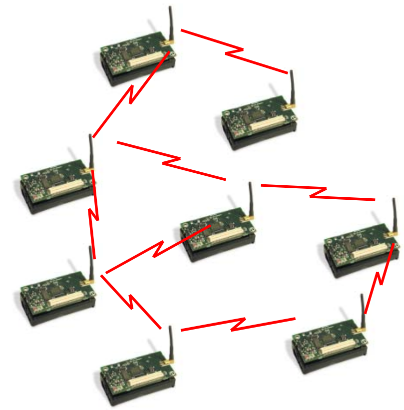
- Securing Ad-Hoc Network Assets
- Threats in Ad-Hoc Environments
- Elementary Security Properties
- Challenges in Realizing Security Properties
- Building Blocks of Defense Mechanisms
- Topic Covered: Control Channel Jamming with node capture attack

Ad Hoc Network Features

- **Interconnection of a (large) number of devices in the *absence of* infrastructure**

Vehicle networks

Personal Networks



Sensor Networks

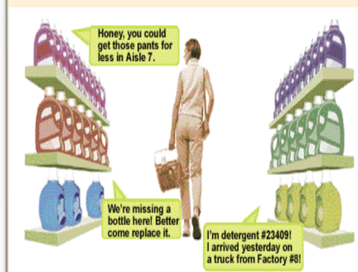
Resource Constraints (Energy, CPU, Memory)

  - **Rely on peer-to-peer communication and collaboration**
  - **Dynamic Network Topology – Mobility, Sleeping Patterns**
  - **Self-organized and Self-Adaptive to topology changes**
  - **Heterogeneous in device capabilities**

Ad Hoc Networks - Span of Applications

Home, Community and Enterprise Networking

Vehicular and Transporta-tion Networks



Inventory Tracking / Supply Chain Management

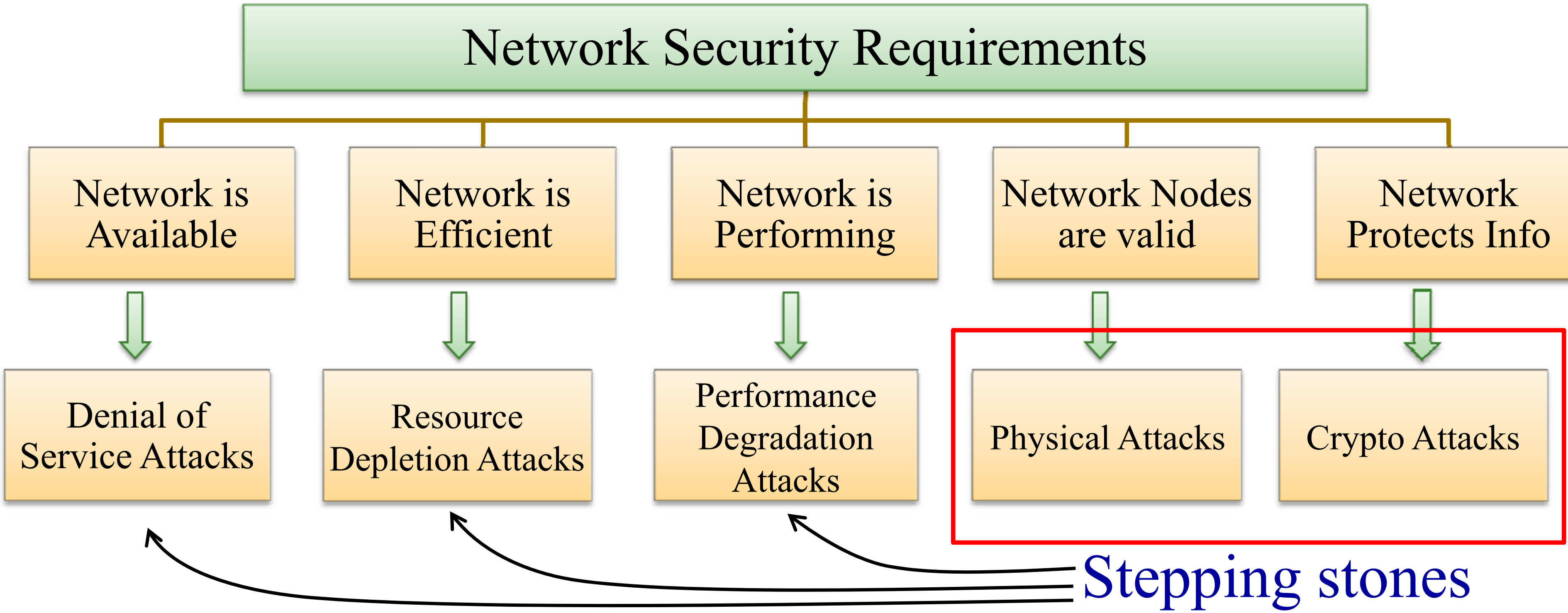
Health Monitoring

Surveillance Networks, Tactical Communica-tions

Network must be Available, Reliable and Secure

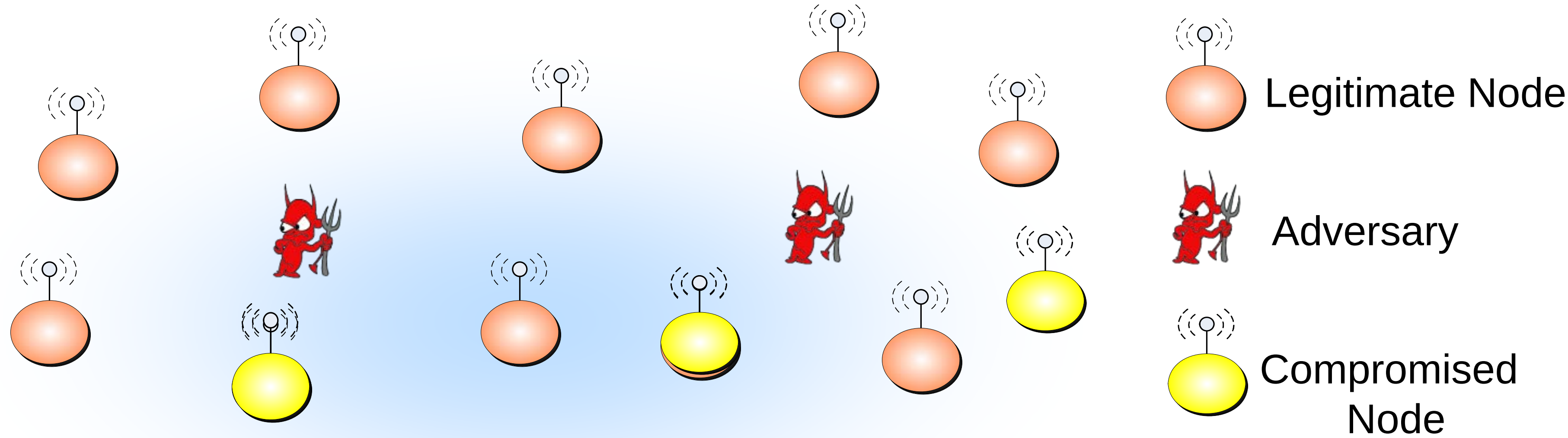
What does it mean to "***Secure***" the network?

Securing the Network Assets



1. **How does an adversary know when and where in the network to mount an attack?**
2. **How does an adversary mount these attacks?**
3. **How do we reason about attack primitives?**

Threats in the Ad hoc Environment



Tapping on the Open Wireless Medium

- Eavesdrop, block, modify, decompose, insert, replay messages

Physical Attacks on Unattended Devices

- Compromise, clone, move nodes, modify software/hardware

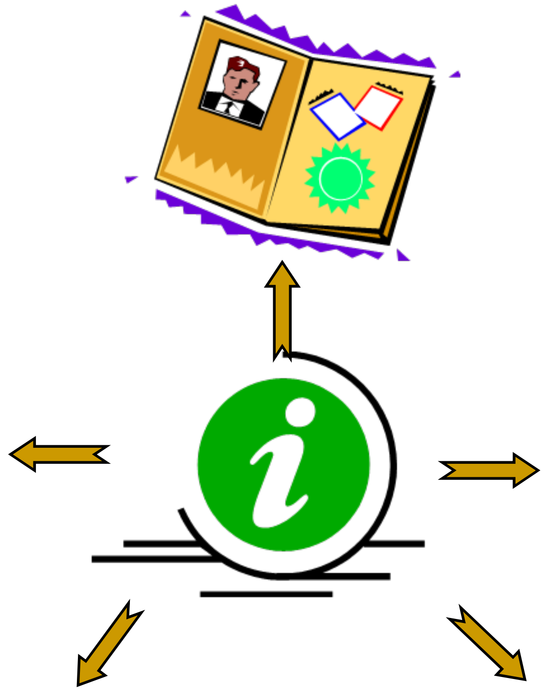
What security properties can we use to defend against these threats?

Elementary Security Properties

What is the source of the information?

Source Authenticity

Is the source trusted?



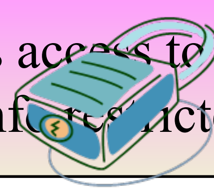
Freshness

Is th… esh?

Has the info been altered in transit?

Confidentiality

Is acc… to the inf… restricted?



Locality Verification

Is info used in …cal computa…ns indeed local?

Challenges in Realizing Security Properties

- **No Centralized Trusted Entity**
  - **Lack of infrastructure; node mobility**
  - **Need for collaboration among the nodes**
- **Heterogeneity in Resource Constraints**
  - **Computation/communication efficient security mechanisms**
- **Nodes Have no Global View of the Network**
  - **Have to rely on limited local information and collaborate**
- **Susceptible to Physical/Side-Channel Attacks**
  - **Cryptography alone is not enough to secure the network**

Building Blocks of Defense Mechanisms

- Over-deploy Nodes
- Aggregate Data from Multiple Sources
- Disseminate Data via Multiple Paths

Information Redundancy

- Use Consistency Checks based on Invariant Properties
- E.g. Time, Communication Range

Multiple Modalities

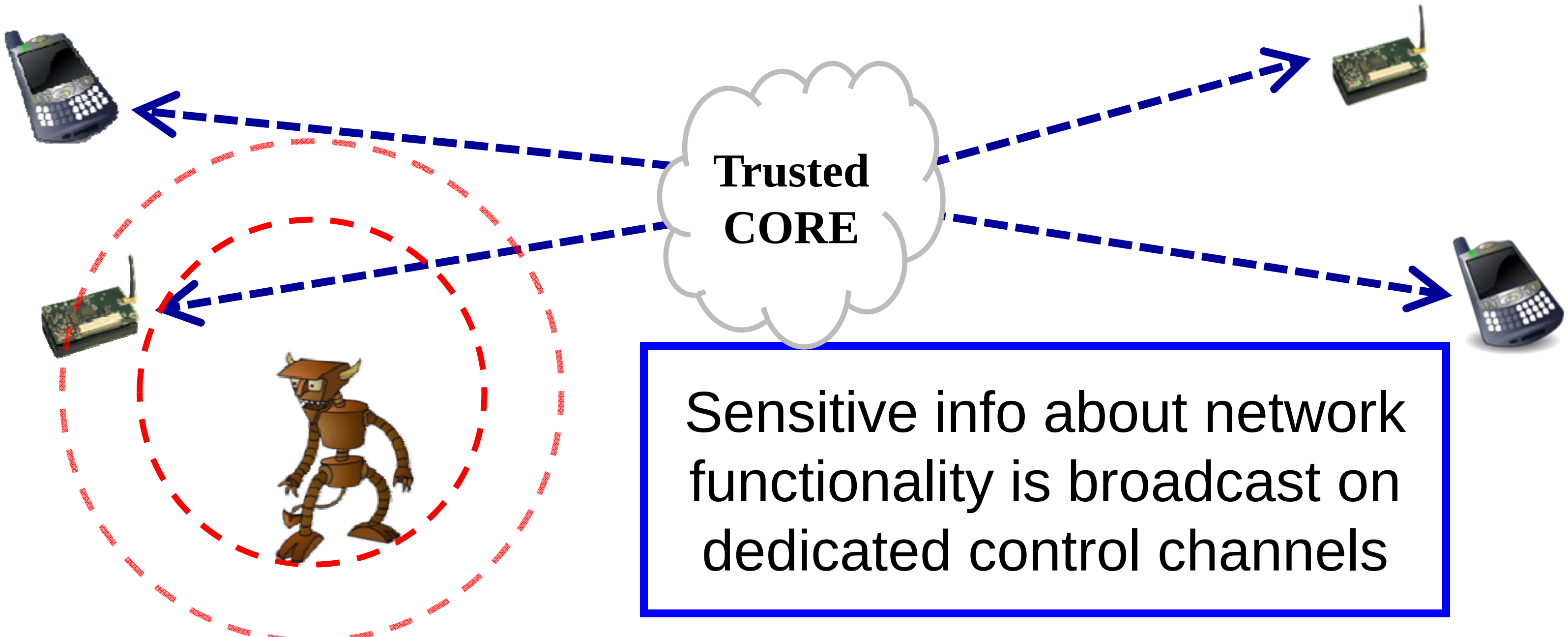
- Crypto Mechanisms
- Distributed trust - Threshold Schemes

Integrate Security and Robustness

1. **How to use the building blocks to detect, isolate and defend against the attacks encountered?**
2. **What type of approaches are suitable for such problems?**
3. **What can be done when the attacker model is not known?**

Today: Mitigation of Control Channel Jamming with node capture Attack

Impact of Jamming Control Channels



Sensitive info about network functionality is broadcast on dedicated control channels

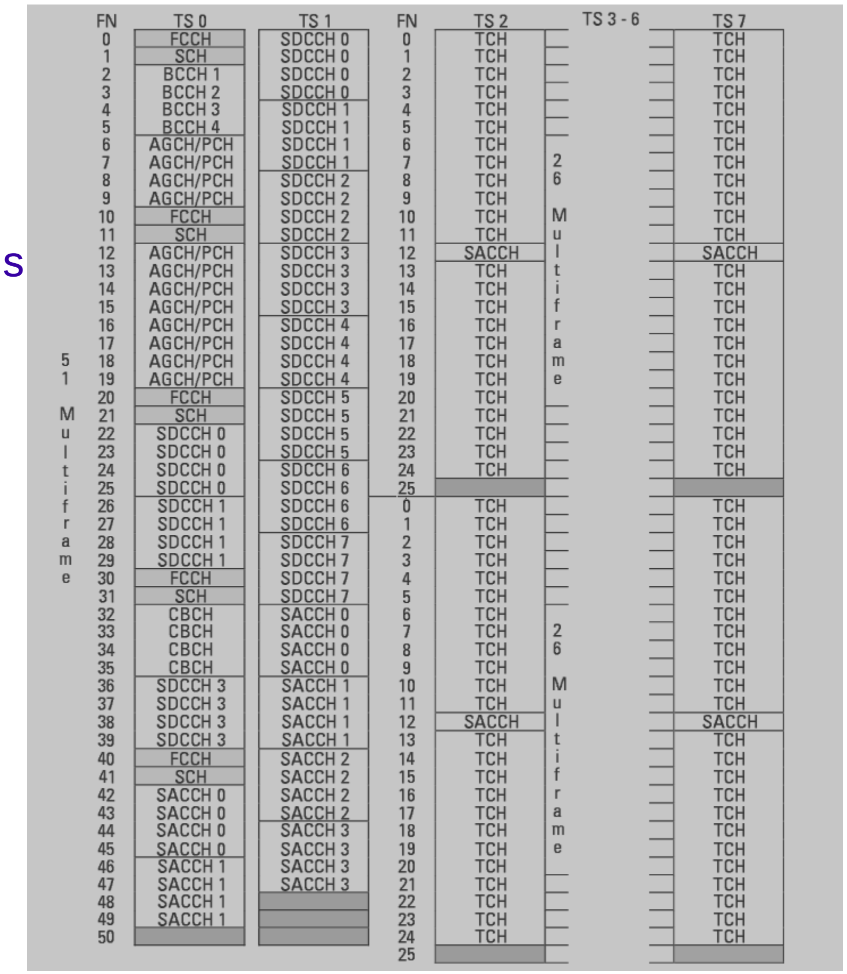
Jamming prevents reception of control messages and degrades network functionality

A control channel becomes the critical point-of-failure for any supported network functionality

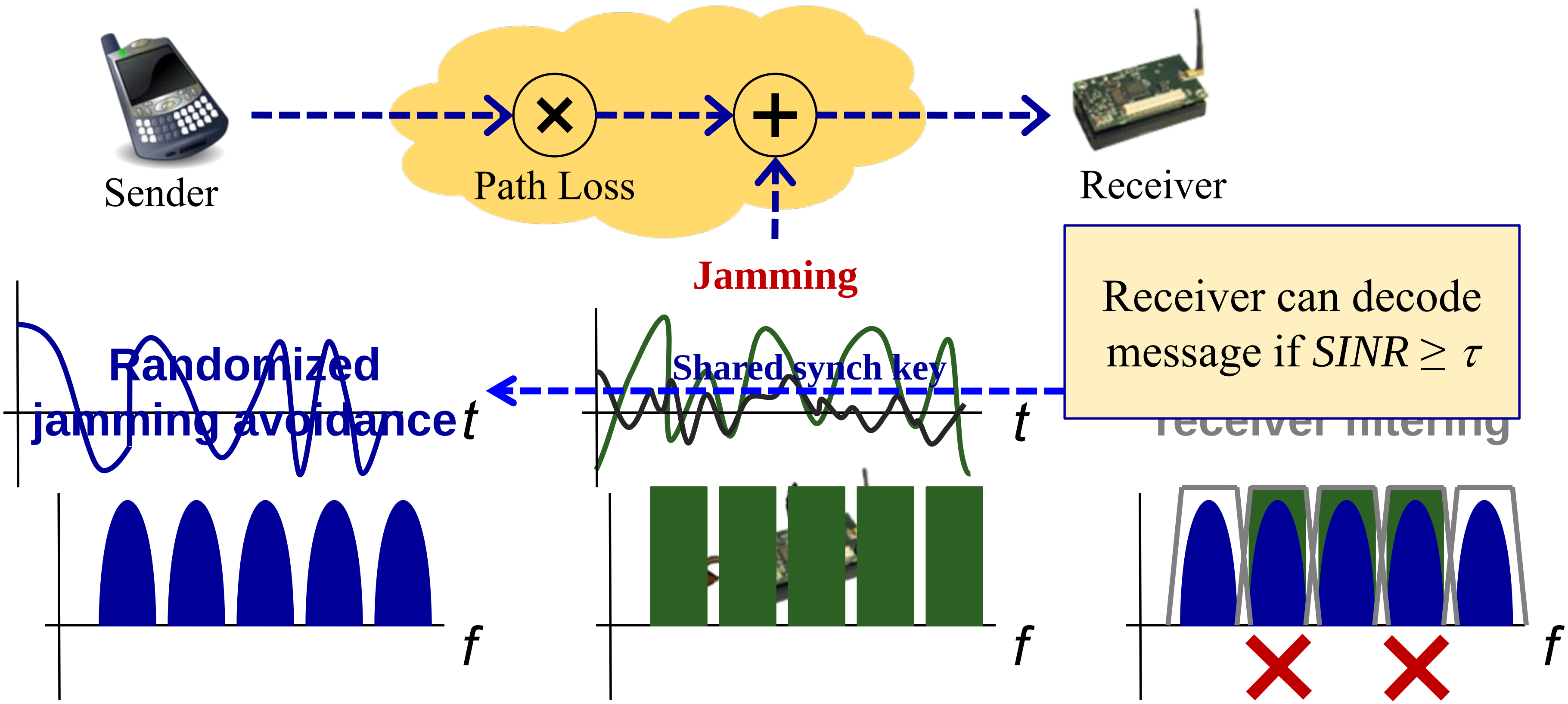
Why Control Channel?

- GSM:
  - FDMA:
- Carrier channels of 200KHz
    - Very few Beacon Frequencies
  - TDMA:
    - 8 time slots
    - TS0: carries most control traffic
  - Super Frame Structure:
    - Critical information such as FCCH, BCCH1 is only scheduled 1/51 frames

⇒ 1 pulse every 400 timeslots on a 200KHz band prevents all communication

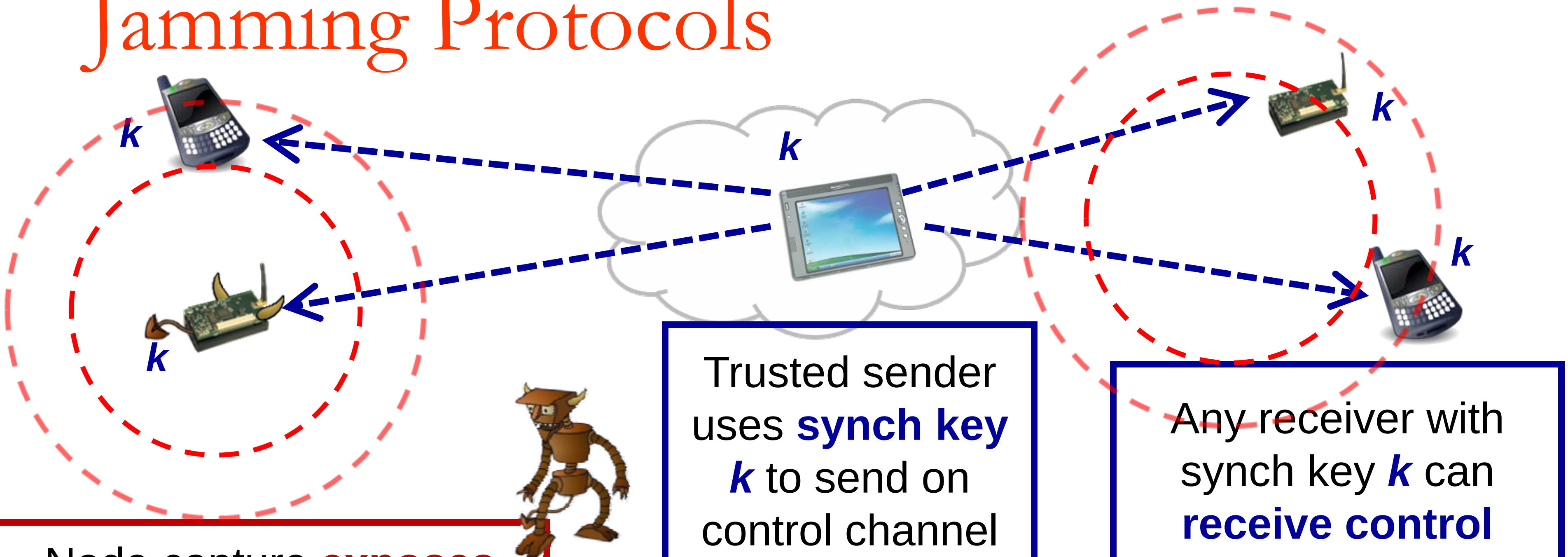


Control Channel Anti-Jamming



Synchronization keys *must remain secret* for effective anti-jamming

Impact of Node Capture on Anti-Jamming Protocols



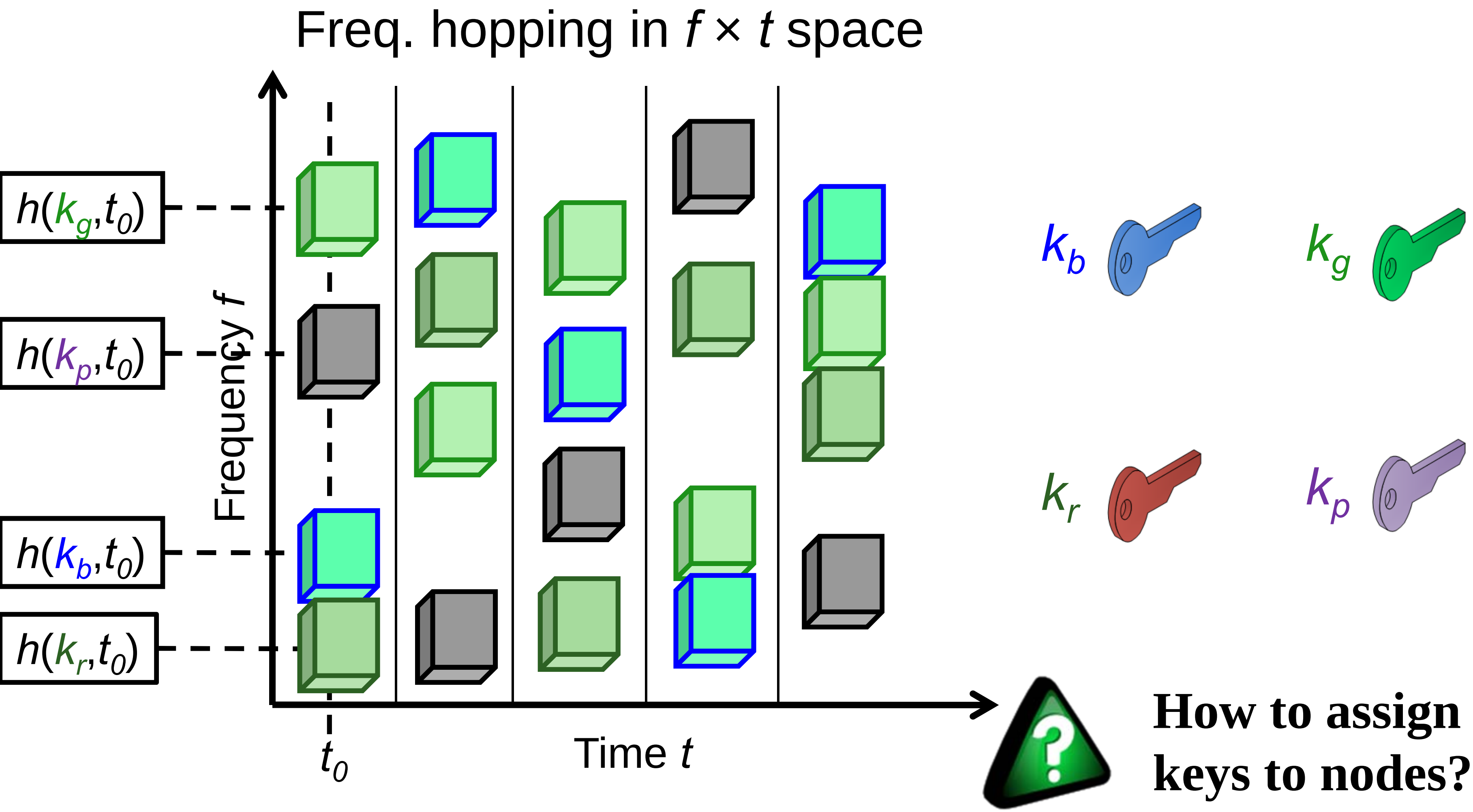
Trusted sender uses **synch key *k*** to send on control channel

Any receiver with synch key ***k*** can **receive control message**

Node capture **exposes synch key *k***, allows for **efficient jamming**

How can we provide control availability in the presence of jamming using exposed synch keys?

Main Idea: Channel Redundancy



How to assign keys to nodes?

Dynamic Jamming Mitigation for Wireless Broadcast Networks

Jerry Chiang and Yih-Chun Hu

Electrical and Computer Engineering

University of Illinois at Urbana-Champaign

Results from the Infocom 2008 paper as well as the Mobicom 2007 papers

Outline

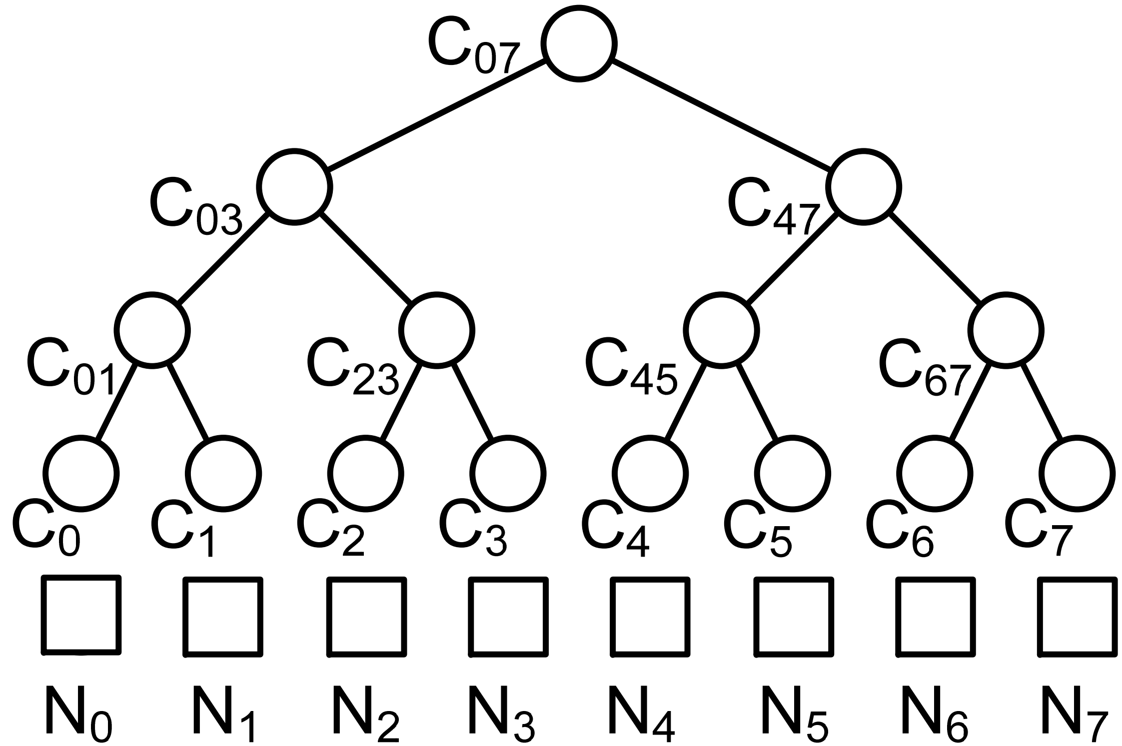
- **Background**
  - **Jamming attack**
  - **Spread spectrum**
  - **Code tree method**
  - **Tree remerging optimization**
  - **Theoretical results**

Broadcast System

- **A *broadcast system* has one transmitter and many receivers**
- **Hard to efficiently extend point-to-point anti-jamming capability of spread spectrum to broadcast systems**

Tree Keying Scheme

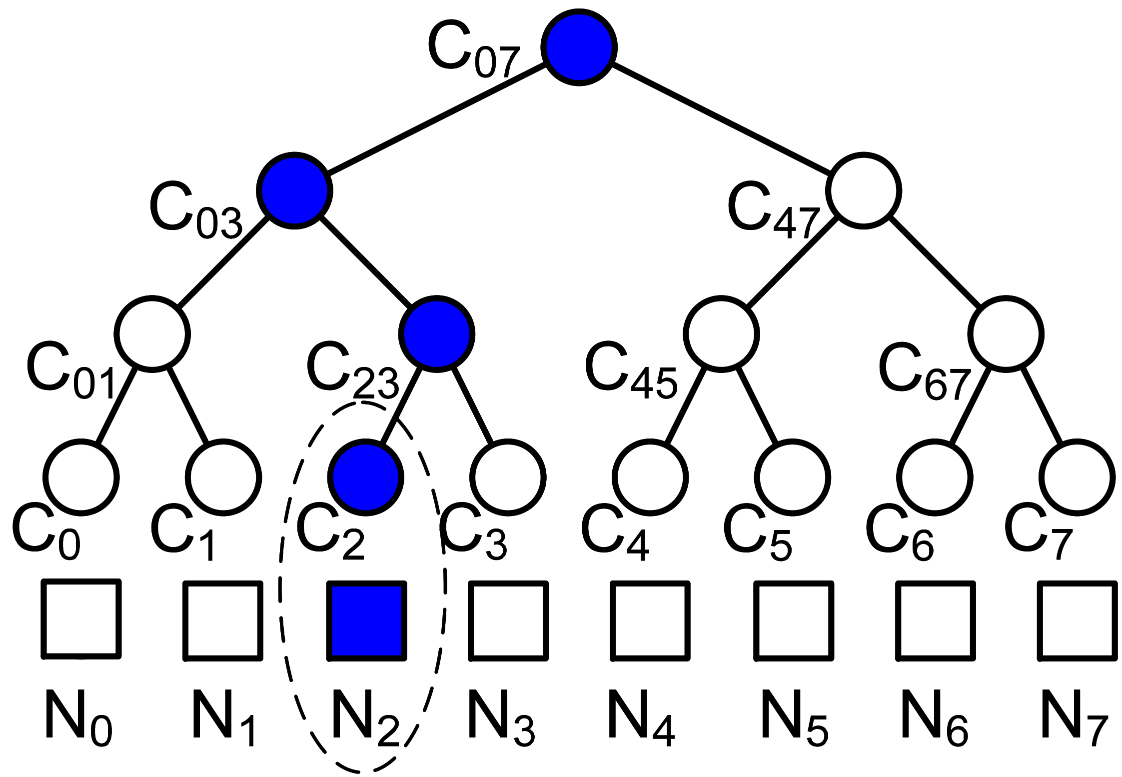
- **Each node of the tree corresponds to a spread spectrum code**



[Chiang and Hu, Cross-layer jamming detection and mitigation in wireless broadcast networks, MobiCom 2007]

Tree Keying Scheme

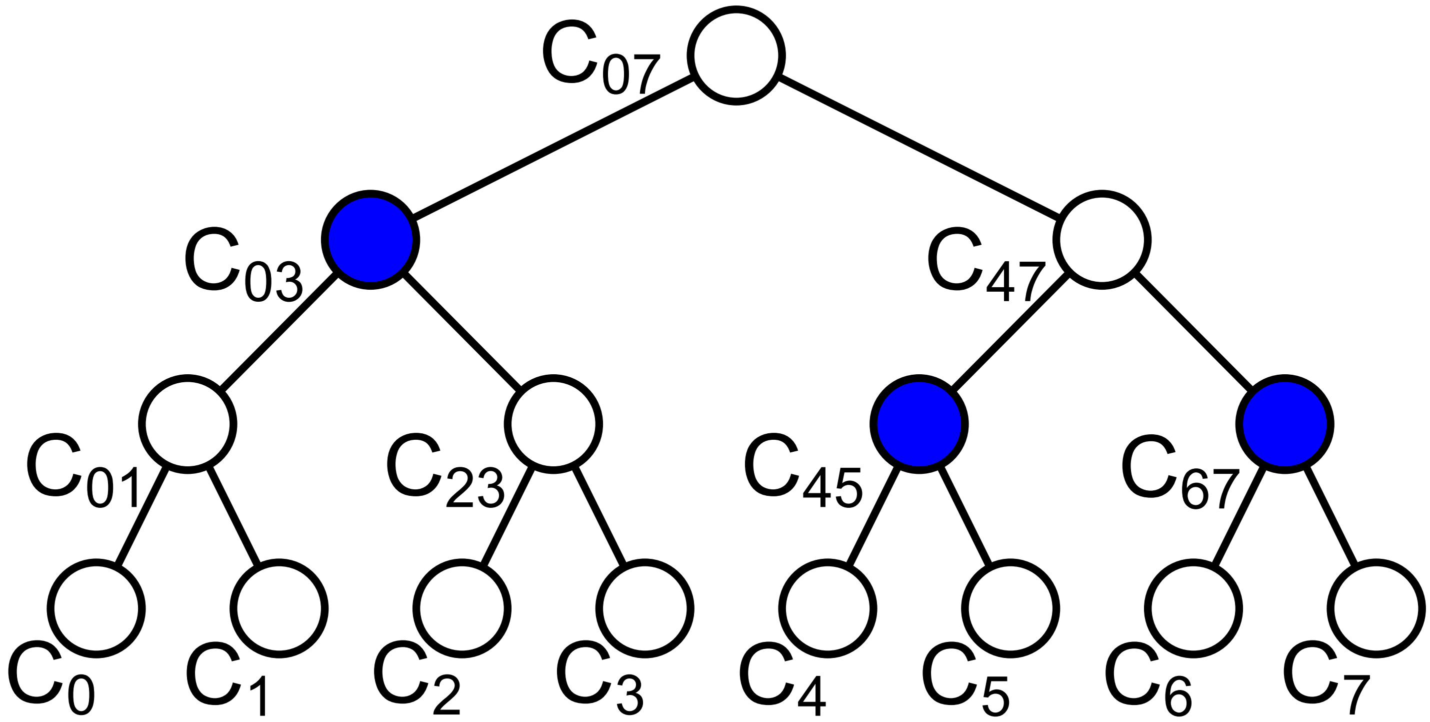
- **Each user holds the codes corresponding to a leaf and its ancestors**



[Chiang and Hu, Cross-layer jamming detection and mitigation in wireless broadcast networks, MobiCom 2007]

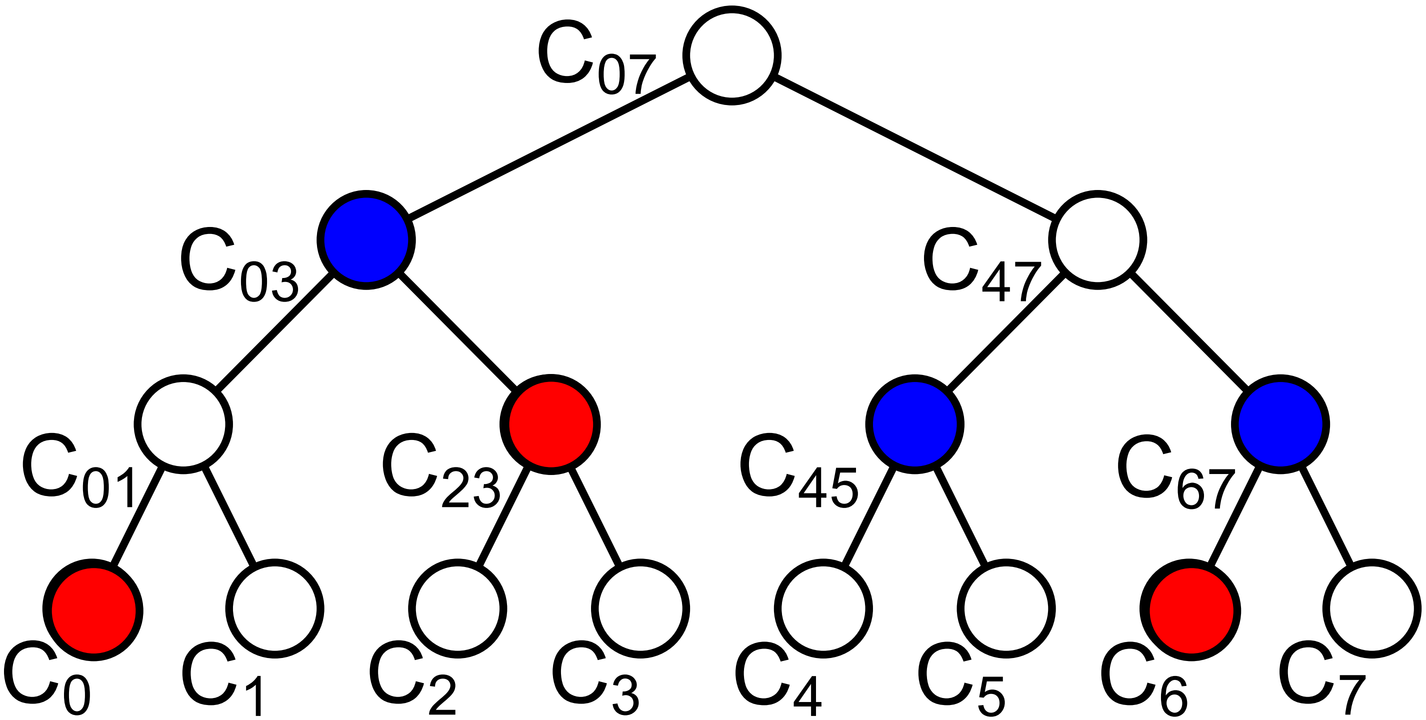
Cover

- A ***cover*** is a set of codes such that each user can decode using at least one spreading code



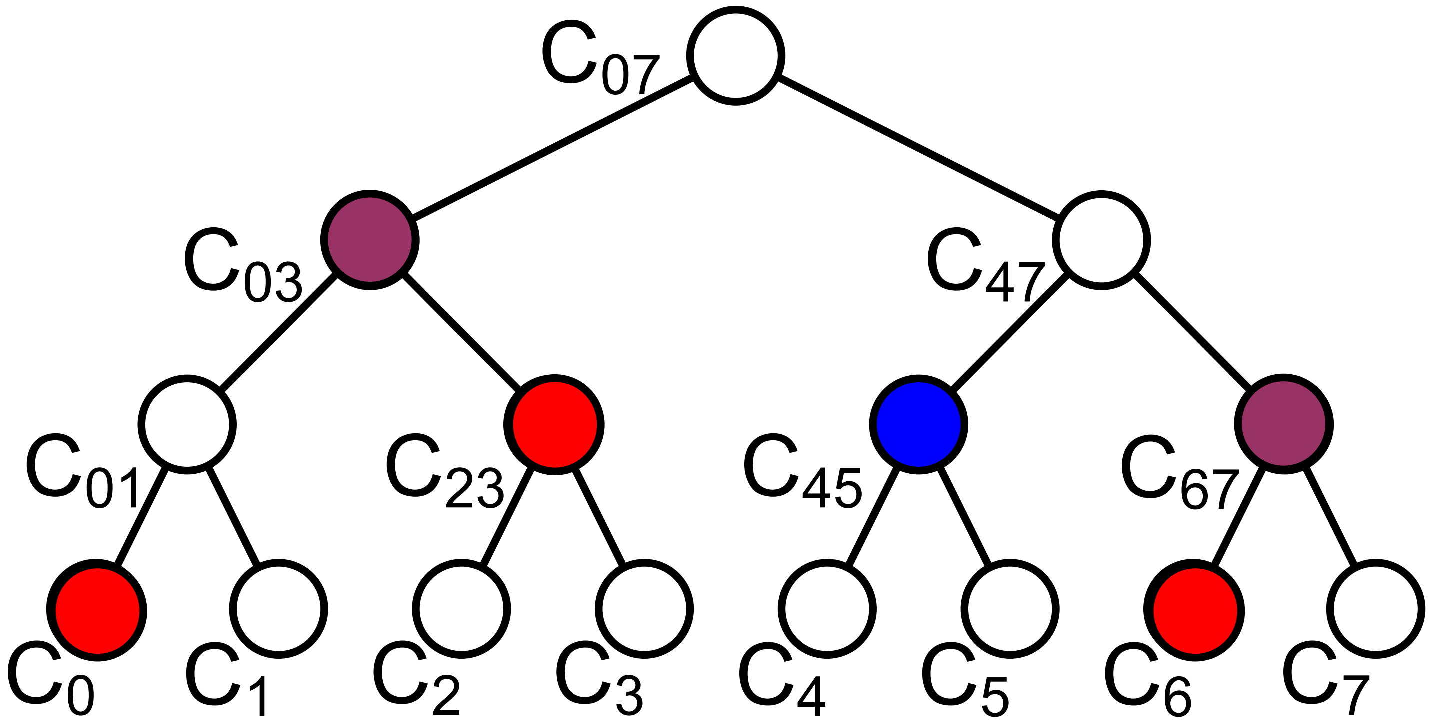
Test Codes

- A set of codes are called ***test codes*** if they are chosen from descendents of the cover



Detectable Codes

- The ancestors of the test codes in the cover are called ***detectable codes***



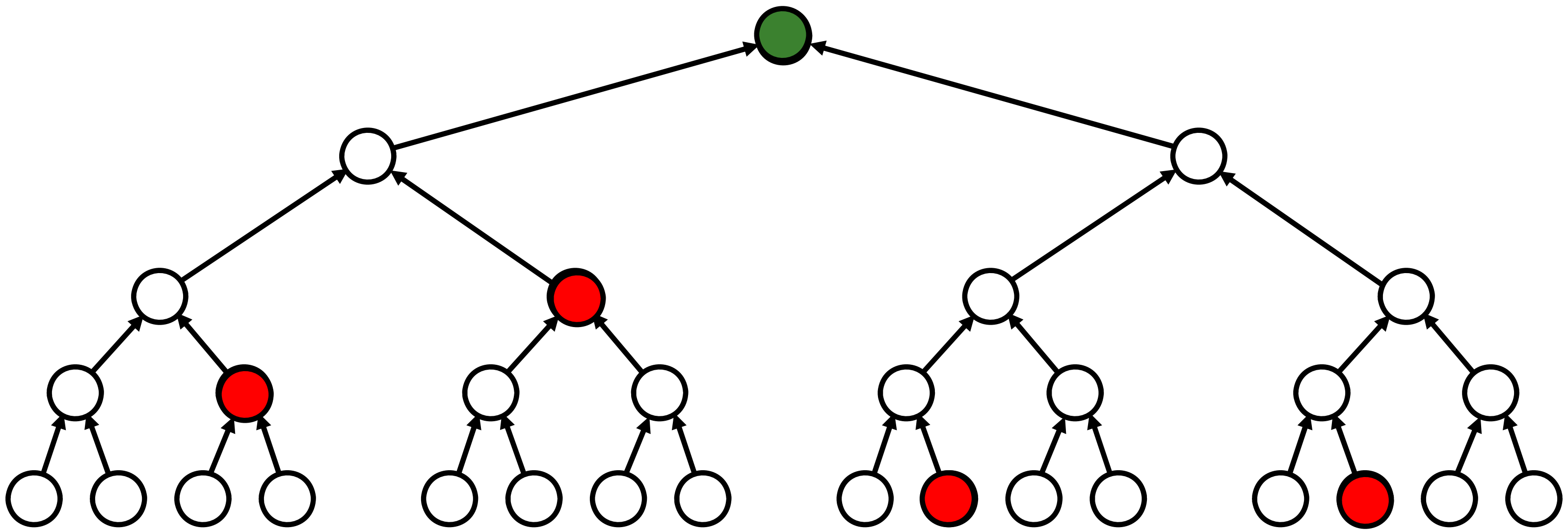
Jamming Detection

- **Control entity and the user nodes have to collaborate on detection of possible jamming**
- **Each node needs to check if it received same control information via two channels**
- **Transmitter simultaneously sends message on both the current minimal safe cover and a set of test codes**
- **Jamming detected when reception happens on test codes but not detectable codes**

Response to Jamming Detection

- Jamming is detected on code C

- Replace C in the cover with its two children



Broadcast Control Channel Jamming: Resilience and Identification of Traitors

Agnes Chan, Xin Liu,
Guevara Noubir, Bishal Thapa
@ College of Computer & Information Science
Northeastern University, Boston

Problem Definition

- Traitor: A malicious user **inside** the system whose intension is to prevent the delivery of broadcast control information
- Goal:
  - Fully Traitor-*Resilient* Control Channel Broadcast
  - Identify **all the traitors**
  - Revoke the bad guys
- Resiliency: Ability to deliver control messages successfully to all users **at least once during a bounded period of time**

Outline

- Model
- Traitor Resilient Scheme
  - 1-Traitor Scheme
  - T-Traitor Scheme
- Performance Evaluation
  - Communication Cost
  - Delay
- Conclusion and Future Work

Model

- Network Model
  - Static: N users and T or less traitors
  - One-Time Preassigned Key Distribution
  - Server sends information over multiple channels
  - Channels are distributed over frequency & time
  - Users use a cryptographic hash function with keys as input to acquire channel information
- Adversary Model
  - **Persistent Traitors/Jammers**
  - Follow the key sequence prescribed
  - Can only jam one channel at a time
  - Server knows the jammed channels(only for ID)

TERM DEFINITION

T	Number of Traitors
N	Total Number of Network users
p	A Communication Frame divided into p timeslots
q	Number of control channels used in a timeslot
k_i^j	a message(key) assigned to an user j at timeslot i. A channel $CH = f(k, i)$
K_i	Set of Keys assigned to users at timeslot i
F	Set of all possible keys assigned to users (Key Pool). $\|F\| = p * q$.
C	Communication Cost

One-Traitor Resilient Scheme

- Binomial Based

Algorithm 1: BBK

Setup: N users, 1 traitor.
Result: distribution matrix $K = (K_i^{(j)})_{N \times \lceil \log_2 N \rceil}$.
begin
  $F = \{k_1, k_2, \cdots, k_{\lceil \log_2 N \rceil}, k'_1, k'_2, \cdots, k'_{\lceil \log_2 N \rceil}\}$
  for $j = 0$ **to** $N-1$ **do**
    $j \leftarrow (j_1 j_2 \cdots j_{\lceil \log_2 N \rceil})$ // binary encoding
    for $i=1$ **to** $\lceil \log_2 N \rceil$ **do**

$$K_i^{(j)} = \begin{cases} k_i, & if \quad j_i = 0 \\ k'_i, & if \quad j_i = 1 \end{cases}$$

    Assign keys from j^{th} row of K to user j
end

Algorithm 2: Transmission for One Traitor Case

System Server:
$i \leftarrow 1$
for *timeslot* i **do**
  Channel-send$_1$ = $f(k_{(i \bmod \lceil \log_2 N \rceil)}, i)$
  Channel-send$_2$ = $f(k'_{(i \bmod \lceil \log_2 N \rceil)}, i)$
  Send control information on two channels
  $i \leftarrow i + 1$
User: For each user $j \in \{0, 1, \cdots, N-1\}$
$i \leftarrow 1$
for *timeslot* i **do**
  Channel-listen = $f(K^{(j)}_{(i \bmod \lceil \log_2 N \rceil)}, i)$
  j listens to that channel
  $i \leftarrow i + 1$

One-Traitor Resilient Scheme

- Example:

Node	Bit-Representation	Key Assignment
0	000	$k_1\ k_2\ k_3$
1	100	$k_1'\ k_2\ k_3$
2	010	$k_1\ k_2'\ k_3$
3	110	$k_1'\ k_2'\ k_3$
4	001	$k_1\ k_2\ k_3'$
5	101	$k_1'\ k_2\ k_3'$
6	011	$k_1\ k_2'\ k_3'$
7	111	$k_1'\ k_2'\ k_3'$

TABLE I

KEY ASSIGNMENT FOR A 8-USER NETWORK WITH ONE TRAITOR.

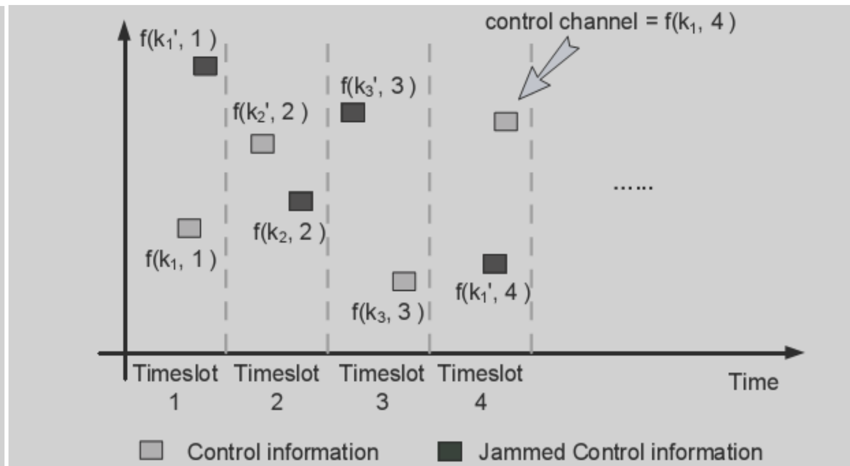


Fig. 1. Channel mapping for the 8-user network example. User 5 is the traitor. Network is 1-resilient.

- Communication Cost: $2\log_2 N$

Optimal One-Traitor Scheme

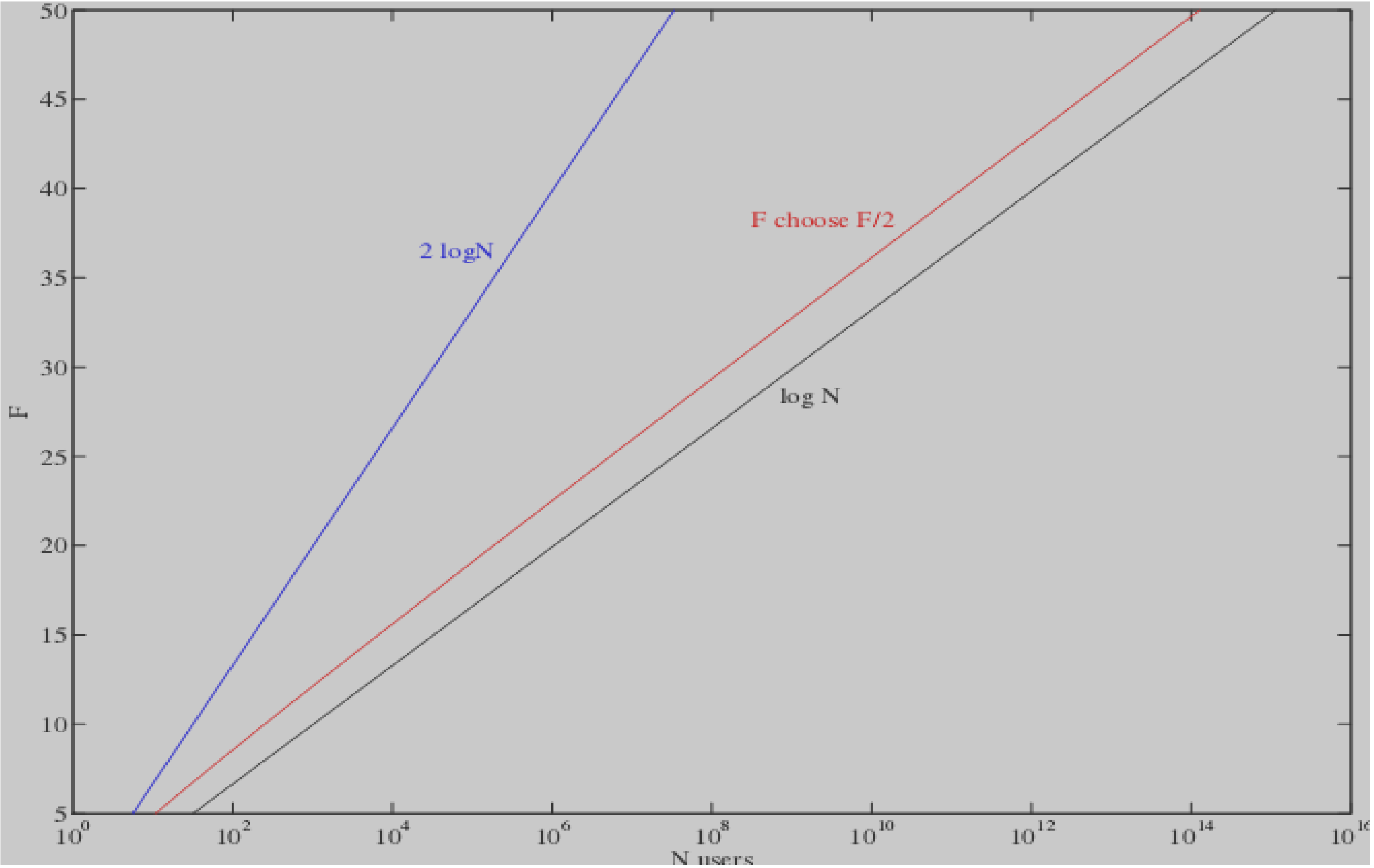
- *Sperner's Lemma*: Given F, choosing $\lfloor \frac{|F|}{2} \rfloor$-subset of F gives the largest Anti-chain of F
- Key Distribution: Given N, pick F such that

$$N \leq \binom{|F|}{\lfloor \frac{|F|}{2} \rfloor}$$

- Communication Cost, F: (sterling's approx.)
- Optimality:

  We know the lower bound, $\lceil \log_2 N \rceil$

One-Traitor Resilient Scheme



T-Traitor Resilient Scheme

- Polynomial Based:

Algorithm 3: PBK-T

Setup: N, key pool F
Result: a $N \times p$ key-distribution matrix K noted K_{ji} or $K_i^{(j)}$
begin
  Initialize $K \leftarrow [0]_{N \times p}$
  S = { (c+1)-vector in GF(q) }
  for $j = 0$ **to** $N-1$ **do**
    Pick unique $s_j \in S$
    for $i = 0$ **to** $p-1$ **do**
      $\gamma = \sum_{k=0}^{c} s_k^{(j)} i^k$
      $K_i^{(j)} = k_i^{(\gamma)}$
  Send $\{K_0^{(j)}, K_1^{(j)}, \cdots, K_{p-1}^{(j)}\}$ to user j
end

Algorithm 4: Transmission for Multi-Traitor Case

System Server:
$i \leftarrow 1$
for *timeslot* i **do**
  $l = i \bmod p$
  for $j = 0$ **to** $q-1$ **do**
    Channel-send = $f(K_l^{(j)}, i)$
    Send access information on this channel
  $i \leftarrow i+1$
User: **for user** $j \in \{0, 1, \cdots, N-1\}$
$i \leftarrow 1$
for *timeslot* i **do**
  $l = i \bmod p$
  Channel-listen = $f(K_l^{(j)}, i)$
  Listen to that channel
  $i \leftarrow i+1$

T-Traitor Resilient Scheme

- Example:

Node j	Polynomial Identifier	Eval $u_j(0)$	Eval $u_j(1)$	Eval $u_j(2)$	Key Assignment
0	0	0	0	0	$k_0^0\ k_1^0\ k_2^0$
1	1	1	1	1	$k_0^1\ k_1^1\ k_2^1$
2	2	2	2	2	$k_0^2\ k_1^2\ k_2^2$
3	x	0	1	2	$k_0^0\ k_1^1\ k_2^2$
4	$1+x$	1	2	0	$k_0^1\ k_1^2\ k_2^0$
5	$2+x$	2	0	1	$k_0^2\ k_1^0\ k_2^1$
6	$2x$	0	2	1	$k_0^0\ k_1^2\ k_2^1$
7	$1+2x$	1	0	2	$k_0^1\ k_1^0\ k_2^2$
8	$2+2x$	2	1	0	$k_0^2\ k_1^1\ k_2^0$

TABLE II

KEY ASSIGNMENT FOR A 9-NODE NETWORK WITH 2 TRAITORS.

- For user j at TS i, assign $k_i^j = polynom_j(i)$

T-Traitor Resilient Scheme

- Correctness: PBK-T resilient Scheme satisfies the sufficient conditions:

$$q^{c+1} \geq N \quad (1)$$

$$q \geq p \quad (2)$$

$$p > T \times c \quad (3)$$

- Cost: p*q

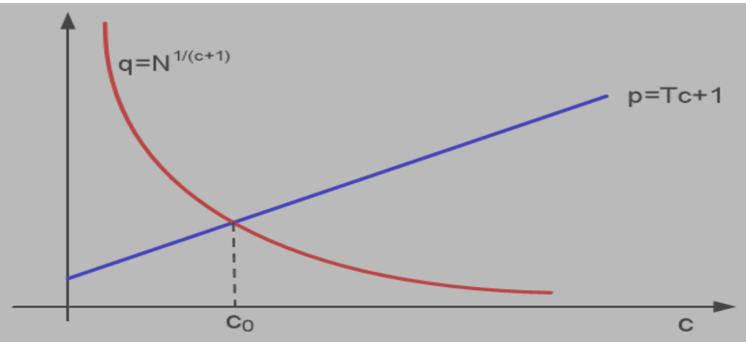


Fig. 2. p(c) and q(c)

T-Traitor Resilient Scheme

- Identification:
  - T-resilience => Unique Identification of all Traitors
  - The assumption that server knows all the jammed channel information is used here
  - Cost: table lookups, where *c* is the maximum degree of identifying polynomials

Conclusion and Future Work

- Extend Combinatorial Scheme of 1-Traitor Scheme to T-Traitor Scheme
- Study the optimal T-Traitor resilient scheme
- Probabilistic Method of defining a resilient scheme and identification for non-persistent traitors
- Suggestions…

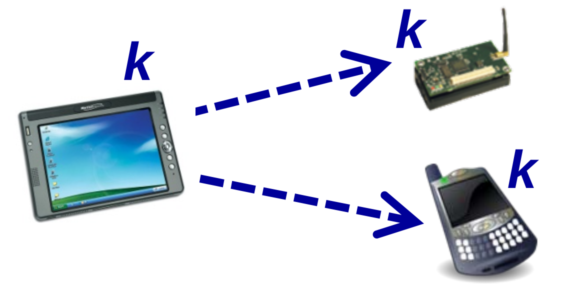
Mitigating Control Channel Jamming using Random Key Assignment

Patrick Tague, Radha Poovendran

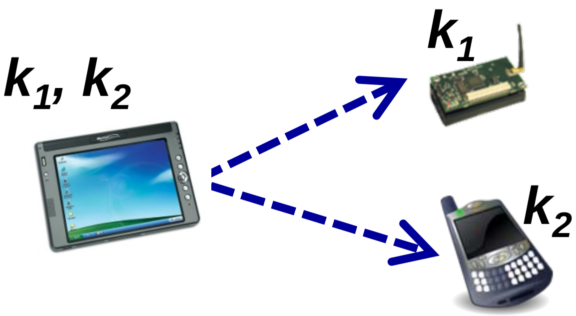
Network Security Lab (NSL)
Department of Electrical Engineering
University of Washington, Seattle

In collaboration with:
Mingyan Li, Boeing Research & Technology

Control Channel Key Assignment



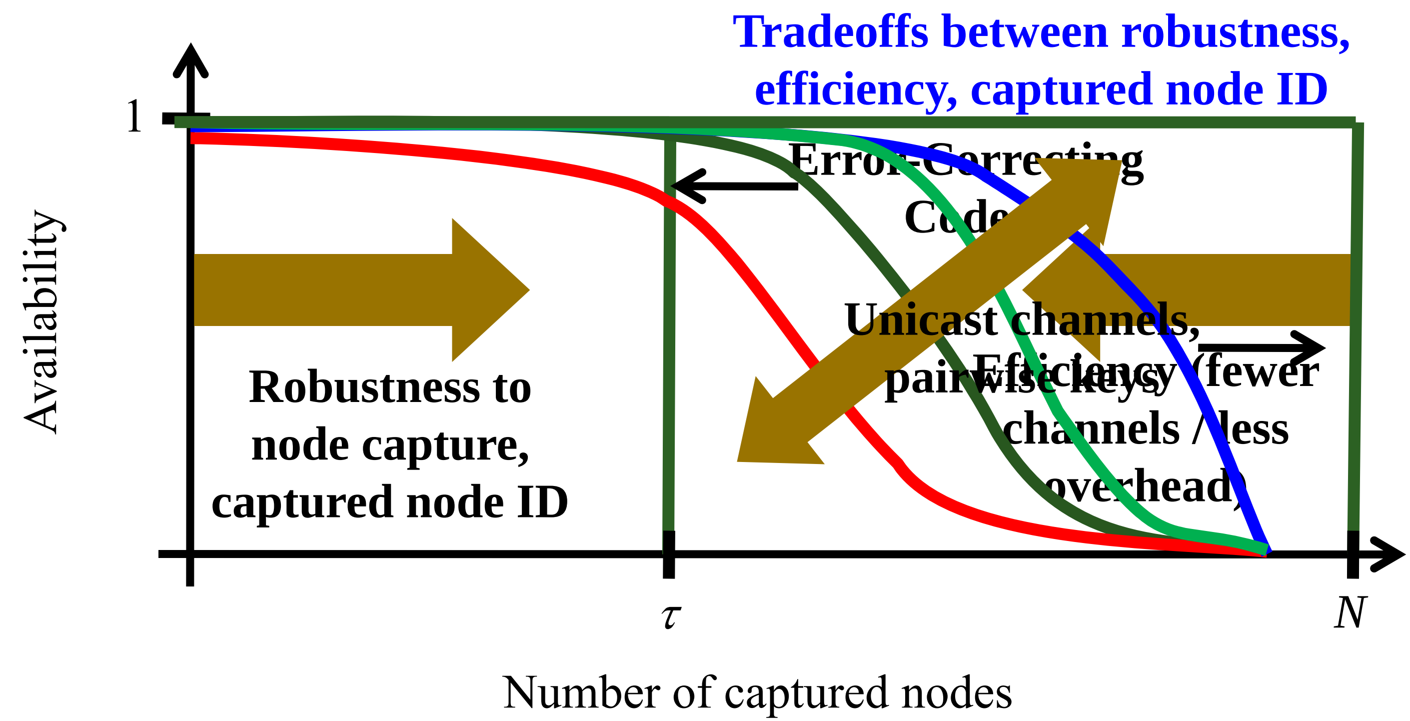
Global key *k*: capture of single node exposes *k*, compromises control channel anti-jamming



Unique key k_i per node: node capture has no effect on other nodes, but number of control channels is *N* (large)

Problem: design key assignment that balances trade-off between *number of channels* and *robust anti-jamming*

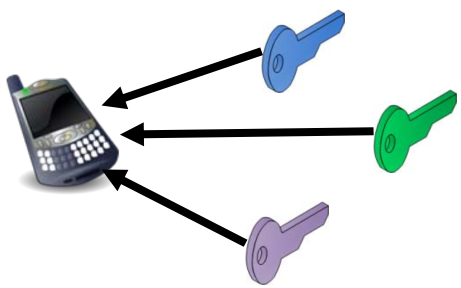
Design for Graceful Degradation



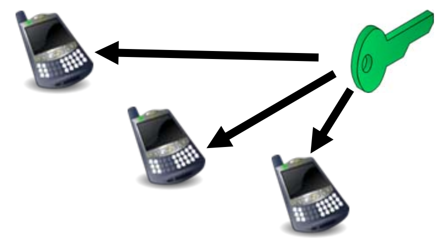
How to assign keys for graceful degradation instead of threshold behavior?

Our Approach: Random Key Assignment

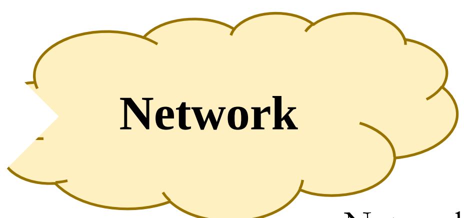
Redundancy in channels available to each node



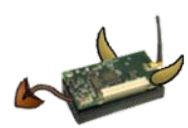
Ability to constrain/control number of nodes with each key



Nodes can join/leave network without control channel re-configuration



No deterministic structure to allow for strategic node capture attacks



Random Control Channel Key Assignment

$k_{t,1}$ $k_{t,2}$

$k_{t,3}$ $k_{t,4}$

$k_{t,5}$ $k_{t,6}$

***K**^{t}*: keys for time slot *t*

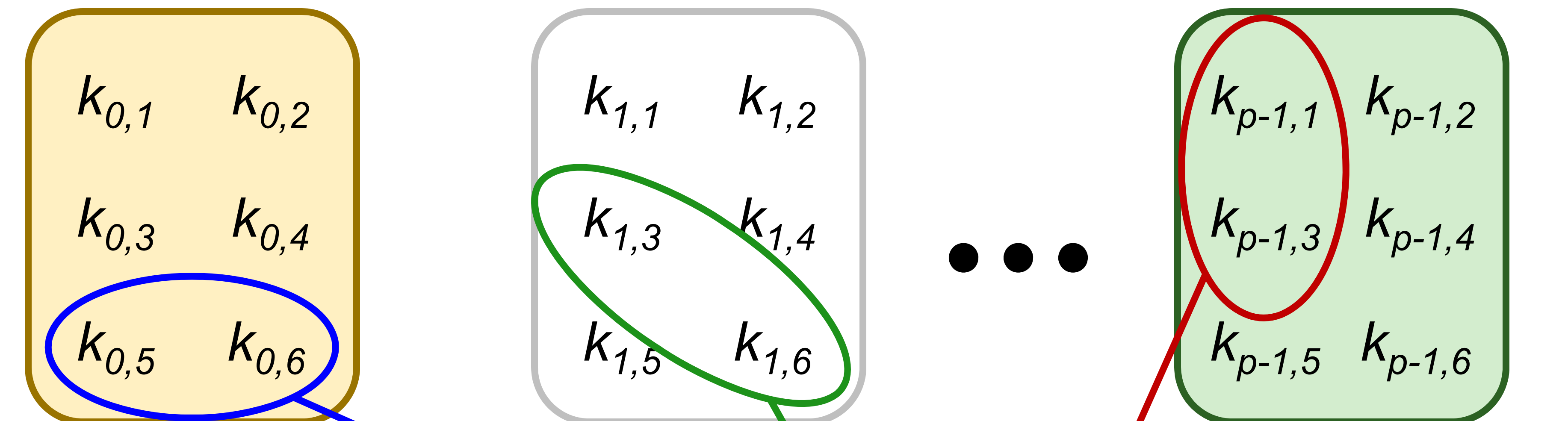
Randomly assign a subset of keys to each node

Node *n*:
$\boldsymbol{K}^t_n = \{k_{t,5}, k_{t,6}\}$

Node *n* can access (or jam) channels #*5* and #*6*

- **Number of keys $q_t = |K^t|$ determines overhead**
- **Subset size $m_t = |K^t_n|$ and ratio m_t / q_t determine resilience to jamming at time *t***

Periodic Key Reuse



$\boldsymbol{K}^0$: keys for time slots $t \equiv 0 \bmod p$

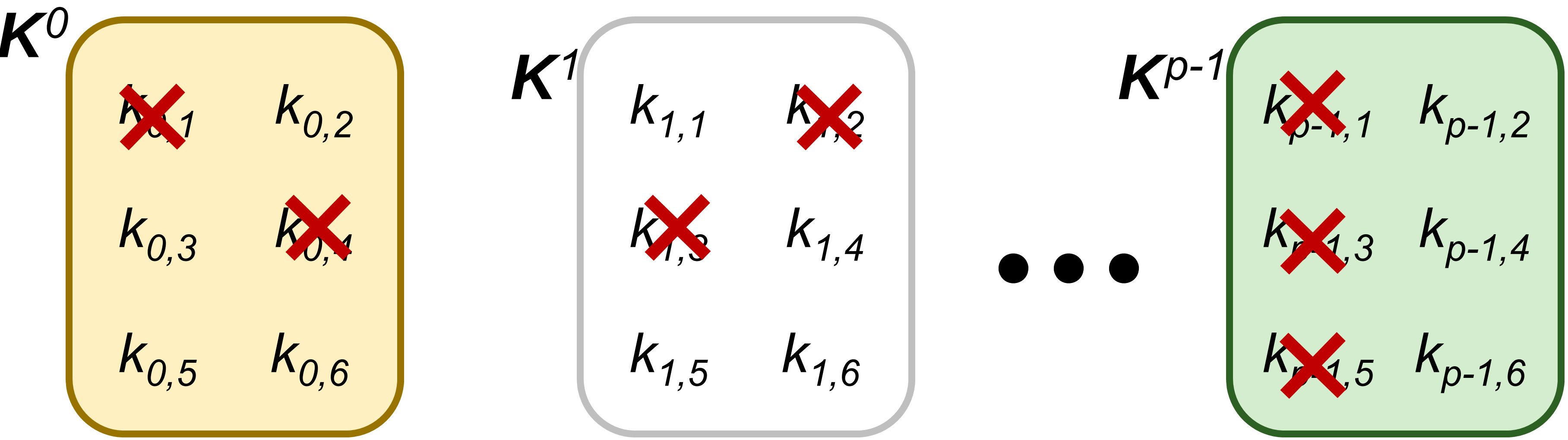
$\boldsymbol{K}^1$: keys for time slots $t \equiv 1 \bmod p$

$\boldsymbol{K}^{p-1}$: keys for time slots $t \equiv p-1 \bmod p$

Node n: $\boldsymbol{K}_n = (\boldsymbol{K}^0{}_n, \boldsymbol{K}^1{}_n, \ldots, \boldsymbol{K}^{p-1}{}_n)$

- **Resilience increases with *p***
- **Overhead and delay increase with *p***

Elimination of Captured Nodes



$\boldsymbol{J}^0 = \{k_{0,1}, k_{0,4}\}$ $\boldsymbol{J}^1 = \{k_{1,2}, k_{1,3}\}$ $\boldsymbol{J}^{p-1} = \{k_{p-1,1}, k_{p-1,3}, k_{p-1,5}\}$

Detection of control channel jamming yields ($\boldsymbol{J}^0$, $\boldsymbol{J}^1$,…, $\boldsymbol{J}^{p-1}$)

How effectively can the source *revoke captured nodes* based on detected jamming?

Identifying Captured Nodes

Node ID	Assigned Keys
1	$(\boldsymbol{K}^0{}_1, \boldsymbol{K}^1{}_1, \ldots, \boldsymbol{K}^{p-1}{}_1)$
2	$(\boldsymbol{K}^0{}_2, \boldsymbol{K}^1{}_2, \ldots, \boldsymbol{K}^{p-1}{}_2)$
…	…
N	$(\boldsymbol{K}^0{}_N, \boldsymbol{K}^1{}_N, \ldots, \boldsymbol{K}^{p-1}{}_N)$

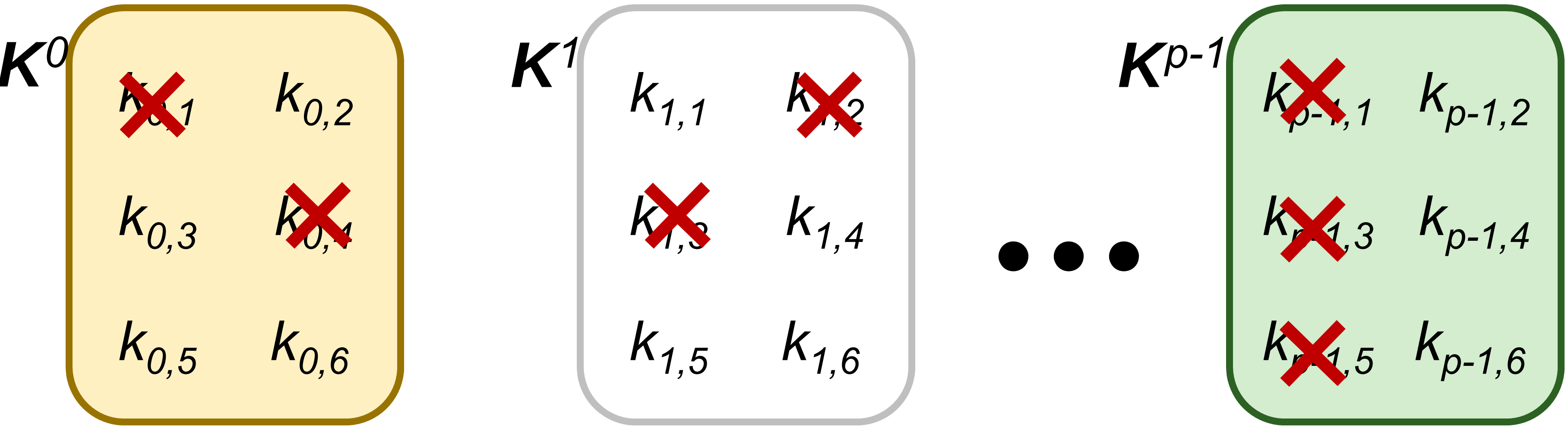
Time Slot	Jammed Channels
0	$\boldsymbol{J}^0 = \{k_{0,1}, k_{0,4}\}$
1	$\boldsymbol{J}^1 = \{k_{1,2}, k_{1,3}\}$
…	
p-1	$\boldsymbol{J}^{p-1} = \{k_{p-1,1}, k_{p-1,3}, k_{p-1,5}\}$

Captured node identification:

- ***Estimate*** **the set of captured nodes** ***C*** **given the jamming evidence {J^i : $i=0,\ldots,p-1$}**

How to estimate the captured node set? How accurate is this estimation process?

Captured Node Estimation



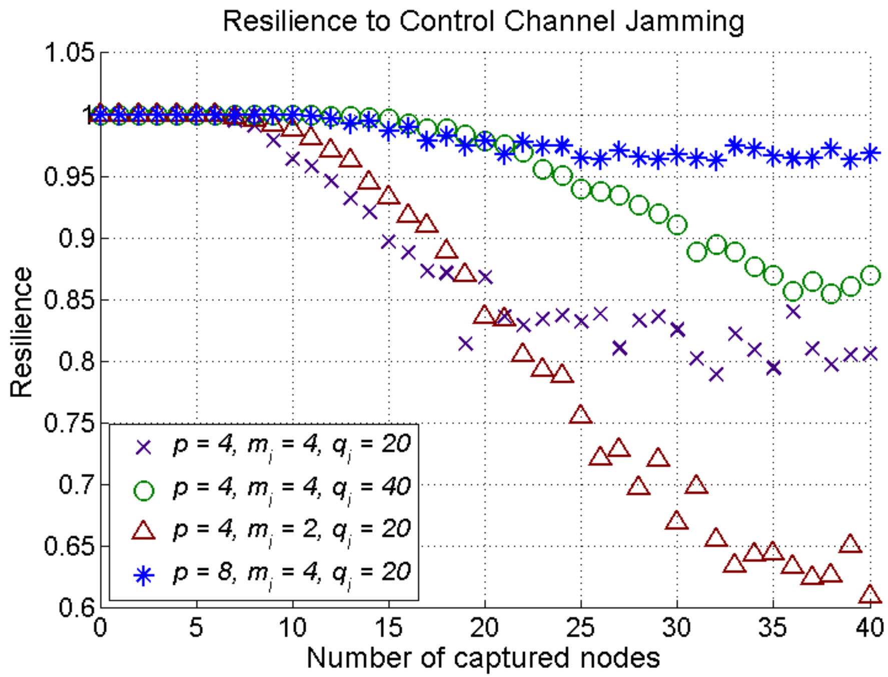
$\boldsymbol{J}^0 = \{k_{0,1}, k_{0,4}\}$ $\boldsymbol{J}^1 = \{k_{1,2}, k_{1,3}\}$ $\boldsymbol{J}^{p-1} = \{k_{p-1,1}, k_{p-1,3}, k_{p-1,5}\}$

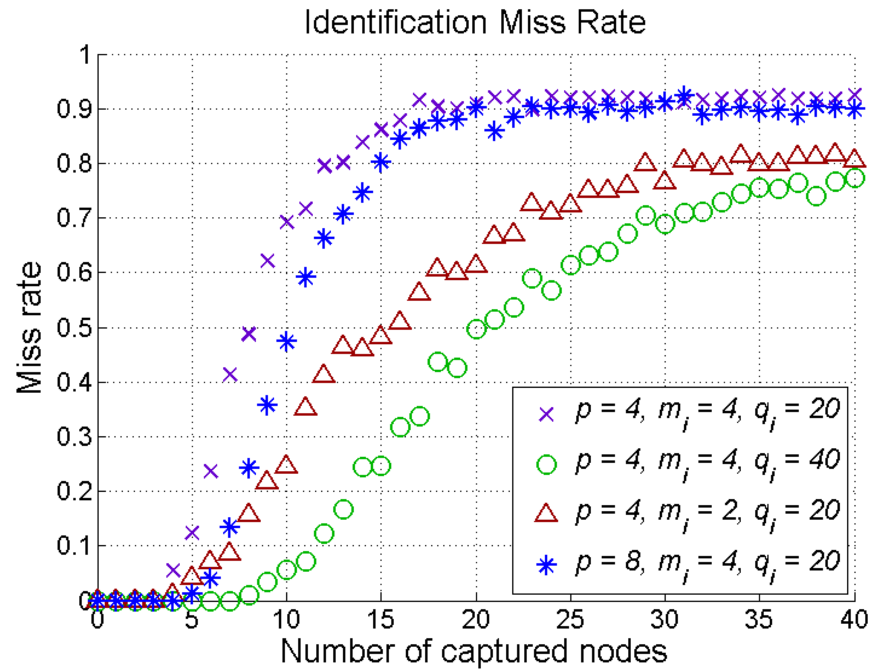
ML/MAP Estimate:
$C' = \arg\max_C \Pr[C \mid \{\boldsymbol{J}^i\}]$
$\quad = \arg\max_C \Pr[\{\boldsymbol{J}^i\} \mid C]$

Heuristic Iterative Estimate:
At each iteration:
add $n' = \arg\max_n \Pr[n \in C \backslash C' \mid \{\boldsymbol{J}^i\}]$

- **Accuracy of ID process *depends on design***
  - **Improves as nodes look more *"different"***
  - **Depends on adversary's choice of what to jam**

Examples





Resilience to jamming for various design parameters

Identification miss rate for various design parameters

250 nodes, jamming on 90% of possible channels

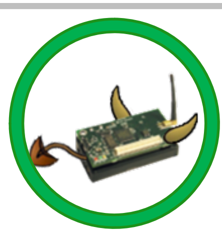
Challenges in Captured Node Detection

Assumption of adversarial behavior required for detection


Trade-offs between resilience to attack and detection capabilities


vs


Non-trivial false alarm and miss rates due to redundant key assignment




How can we address these challenges?

Acknowledgements

- Agnes Chan, Guevara Noubir : North Eastern University
- Yih-Chun Hu, Jerry Chang: UIUC
- Loukas Lazos: UoA, Tucson
- Patrick Tague: NSL
- http://www.ee.washington.edu/research/nsl

Reading list for the 1st lecture

- **Prof. Dawn Song**
  - **A**
  - **B**
  - **C**
- **Prof. Poovendran**
  - P. Tague, M. Li, and R. Poovendran, Mitigation of Control Channel Jamming under Node Capture Attacks, IEEE Transactions on Mobile Computing.
  - **http://www.ccs.neu.edu/home/noubir/publications/CLNT07.pdf**
  - **http://users.crhc.illinois.edu/yihchun/pubs/infocom08.pdf**