Summer School on Network and Information Security 2009

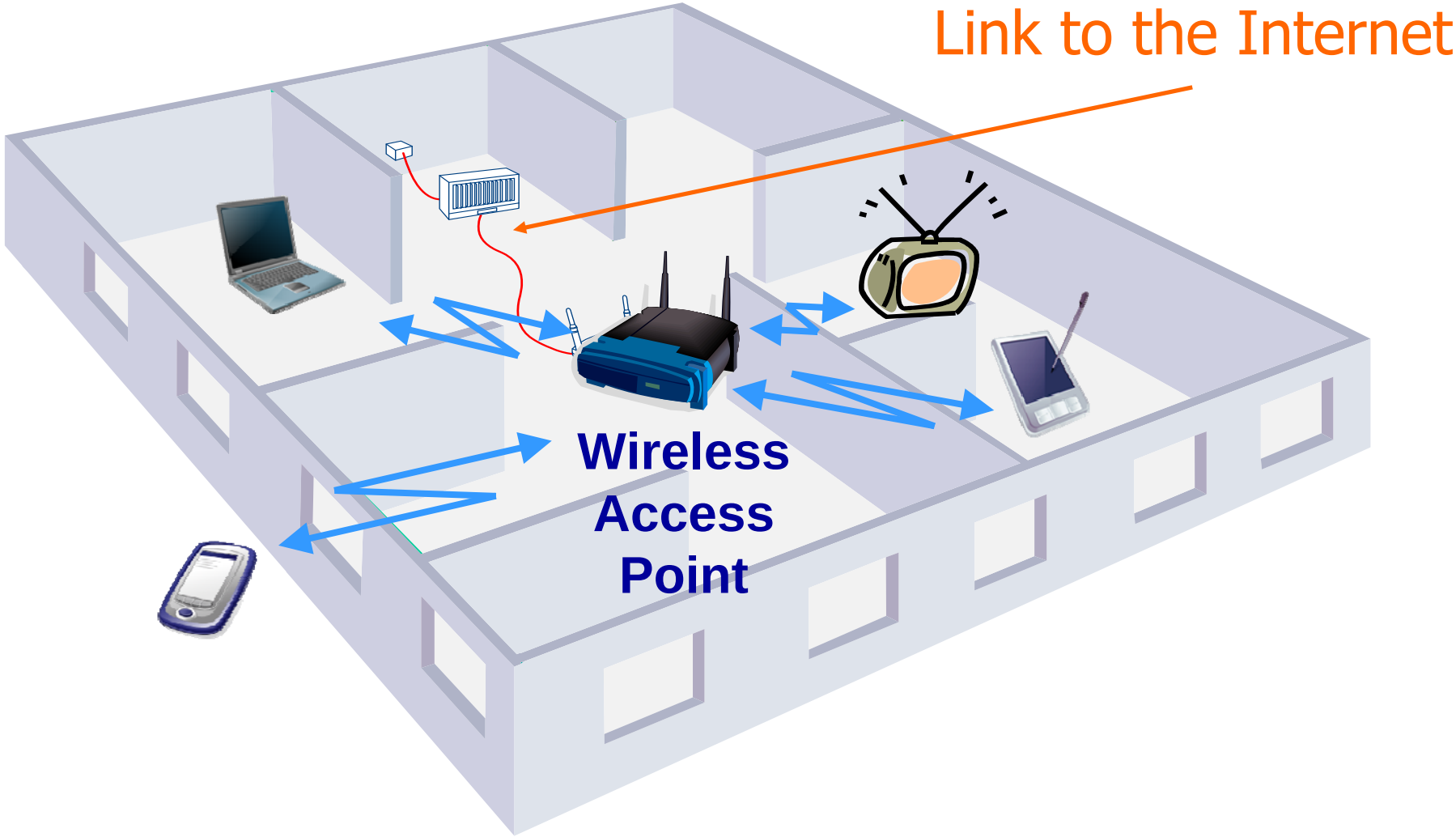
Wireless System Security

Panos Papadimitratos

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Wireless Networked Systems

- Wireless local area networks (WLANs)



Wireless Networked Systems (cont'd)

- WLANs, Personal Area (PANs), Ad hoc Networks

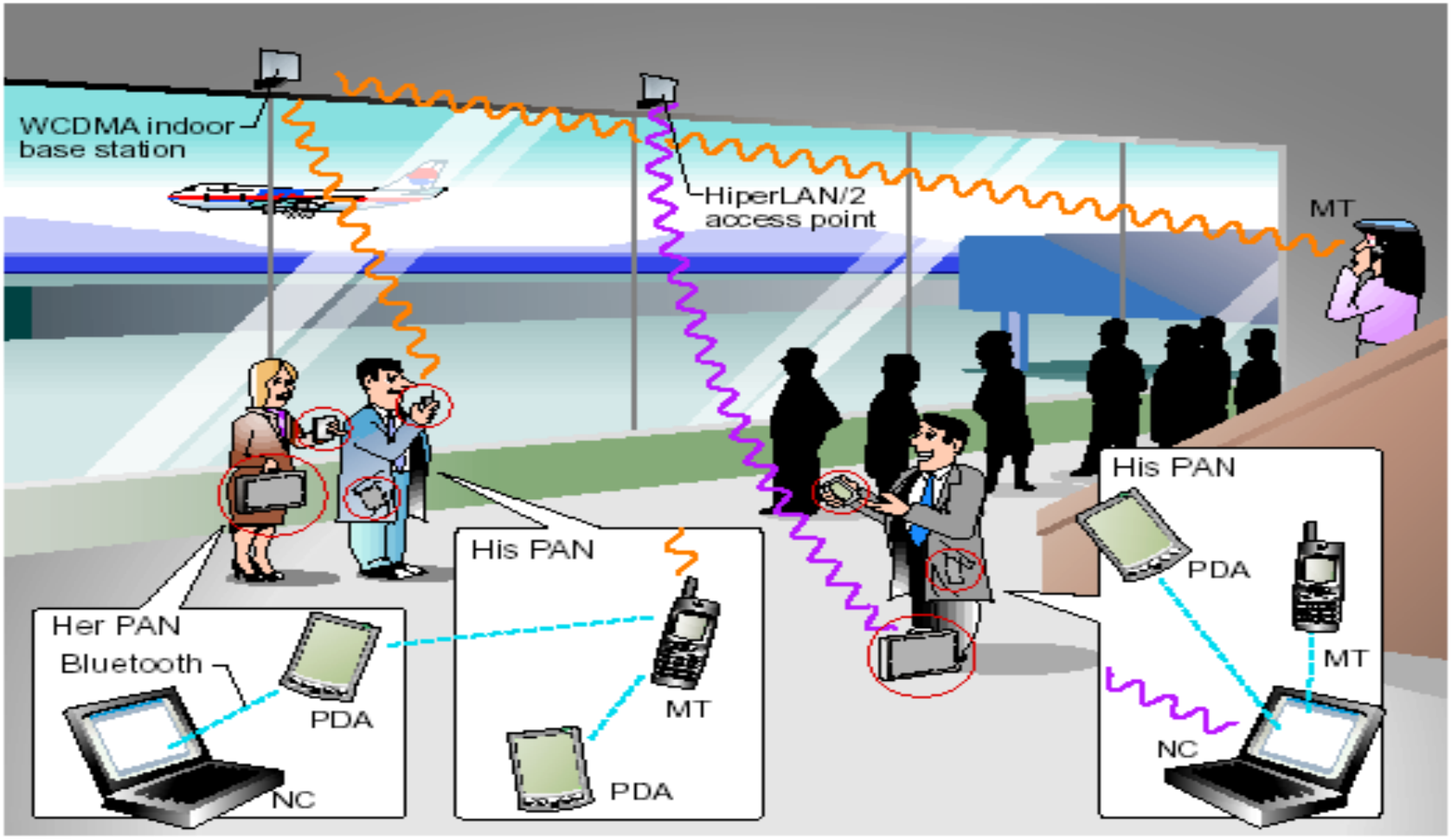


Illustration: Ericsson, ca. 2000

Wireless Networked Systems (cont'd)

- Radio Frequency Identification (RFID)

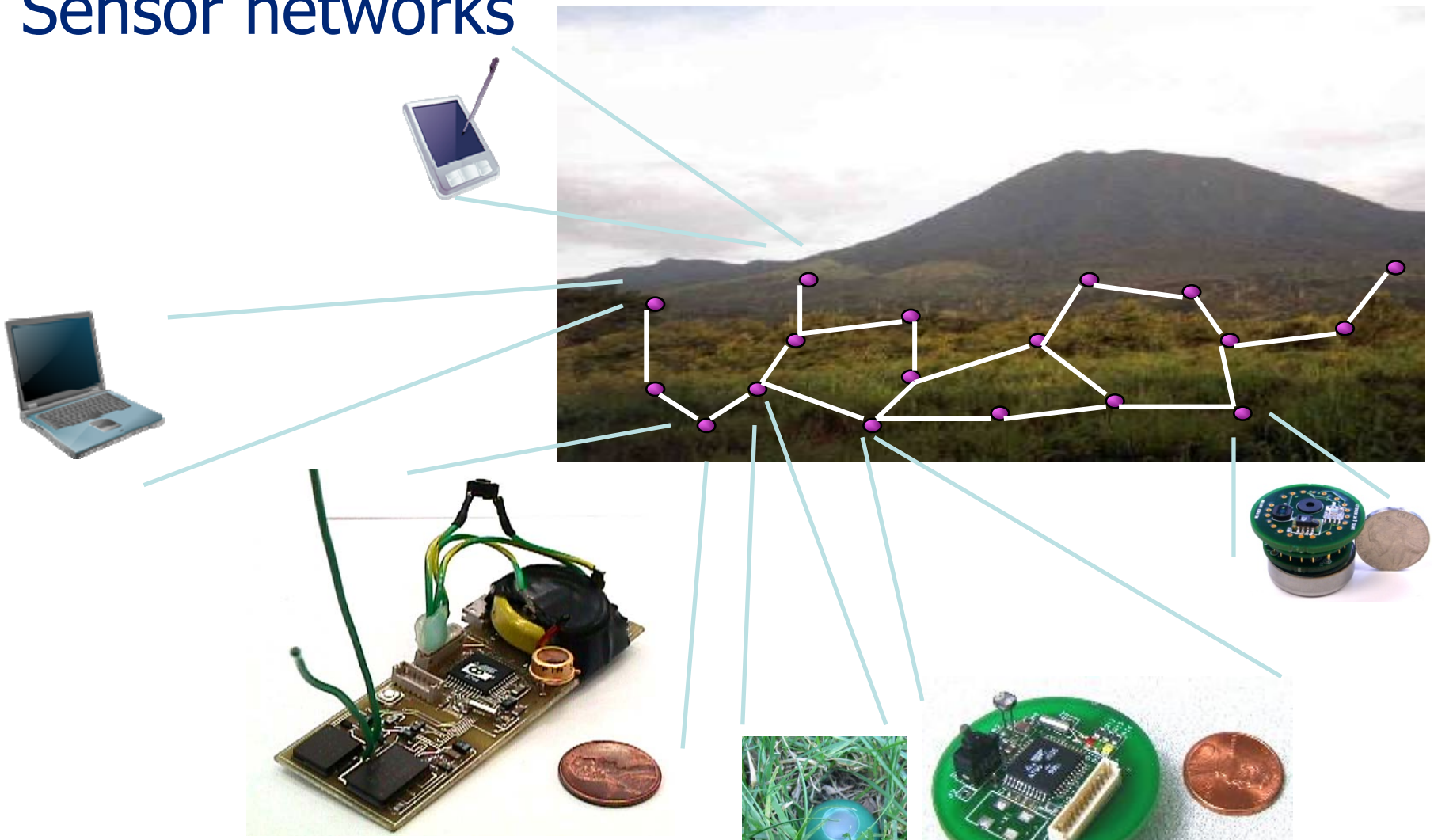


- Wi-Fi and Bluetooth enabled devices



Wireless Networked Systems (cont'd)

- Sensor networks



Node photos: XBow

Wireless Networked Systems (cont'd)

- Tactical ad hoc networks
  - Military
  - Search-and-rescue















Wireless Networked Systems (cont'd)

- Vehicular ad hoc networks (VANETs)

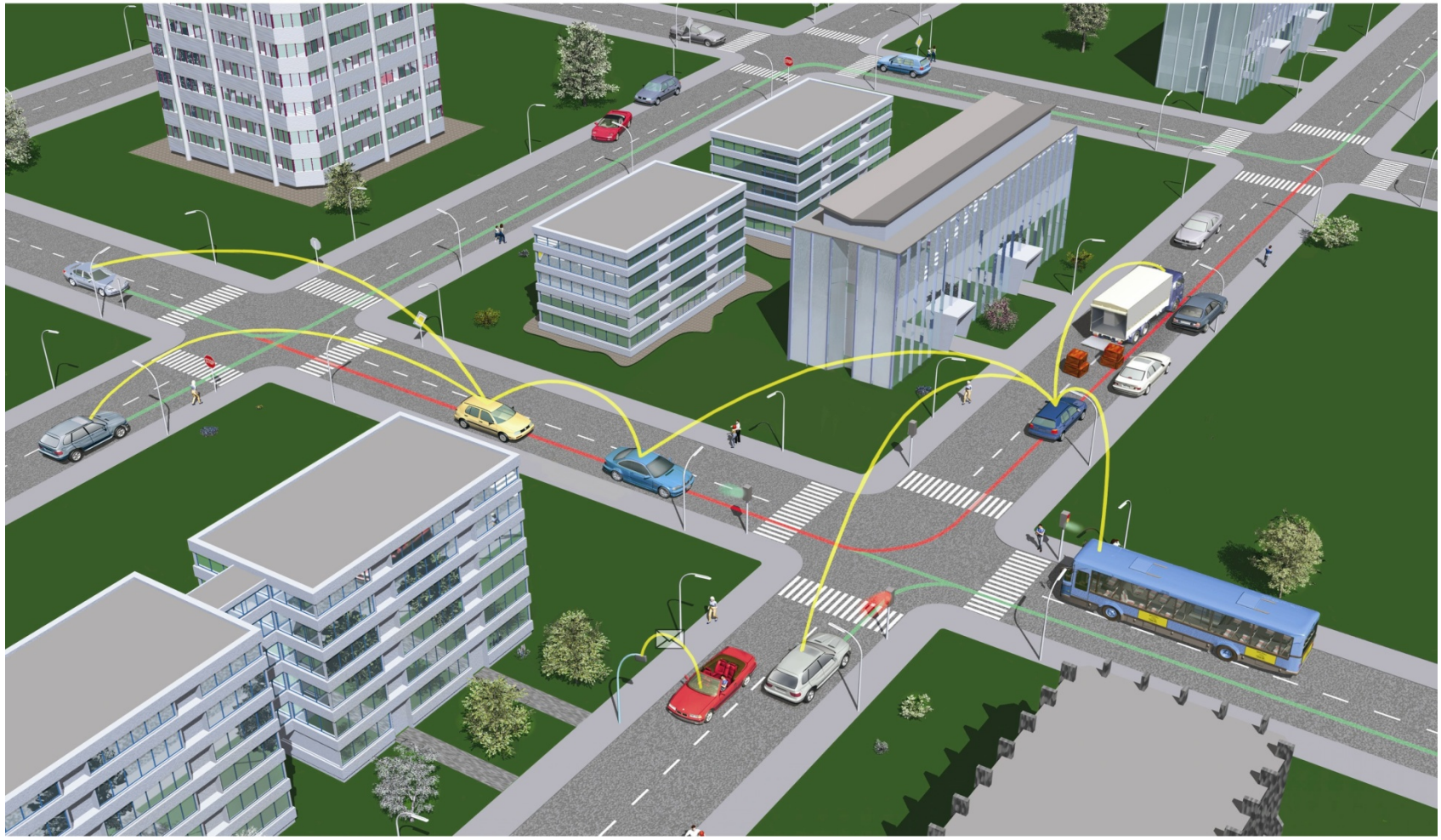
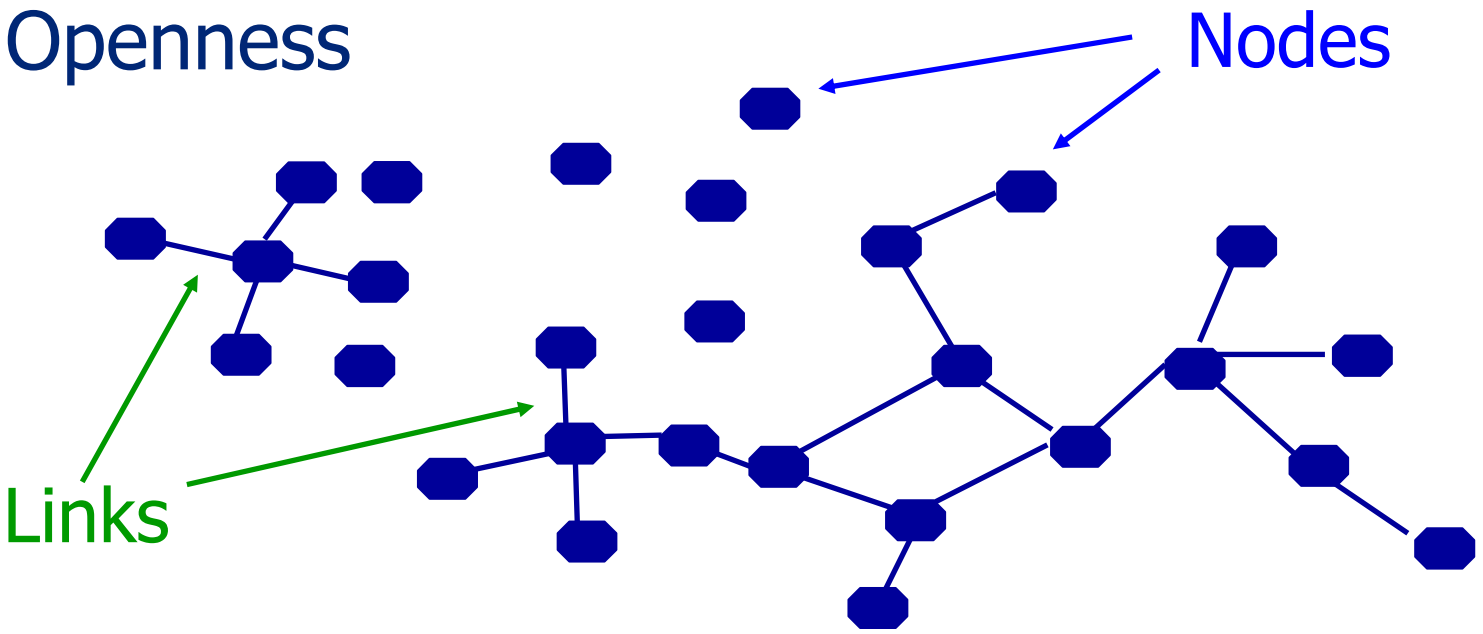


Illustration: C2C-CC

Wireless Networked Systems (cont'd)

- Ad hoc networks
  - Limited wireless communication range
  - Collaborative support of the network operation
  - Peer-to-peer interactions
  - Transient associations
  - Openness



Wireless Networked Systems (cont'd)

- Security challenges
  - Easy eavesdropping and message injection
  - Each and every node can disrupt the network operation
  - No monitoring facility
  - Resource constraints
  - Error-prone communication
  - Hostile environments
  - Nodes and applications tightly coupled to the user and her physical environment

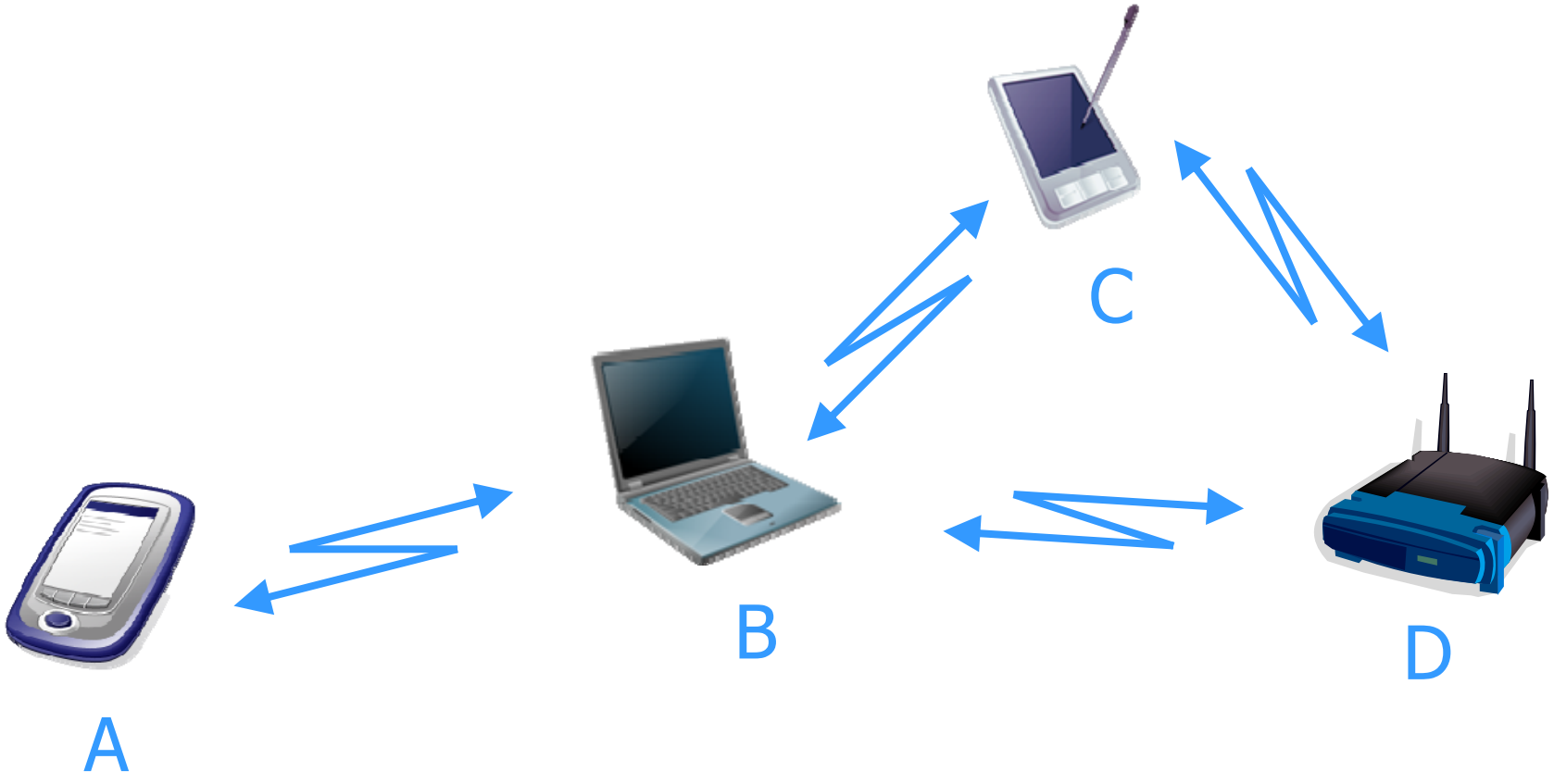
Outline

- Secure Neighbor Discovery
- Secure Route Discovery
- Secure Data Communication
- Secure Localization

Secure Neighbor Discovery

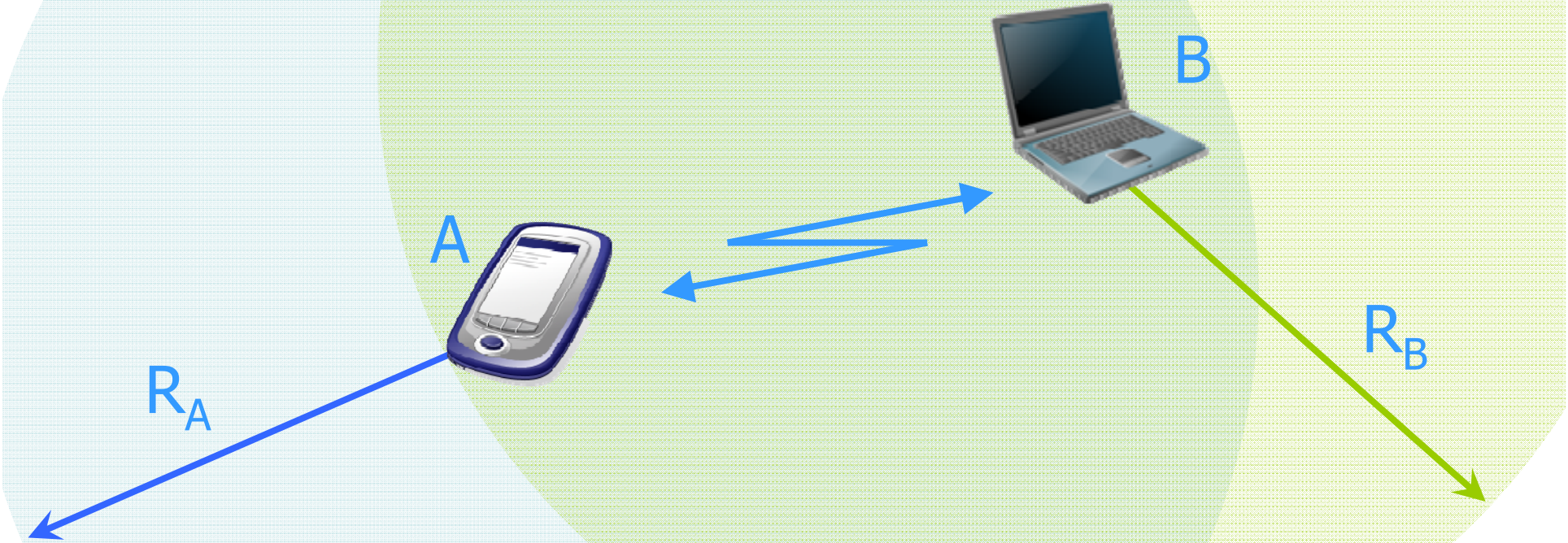
© 2009 P. Papadimitratos

Neighbor Discovery (ND)



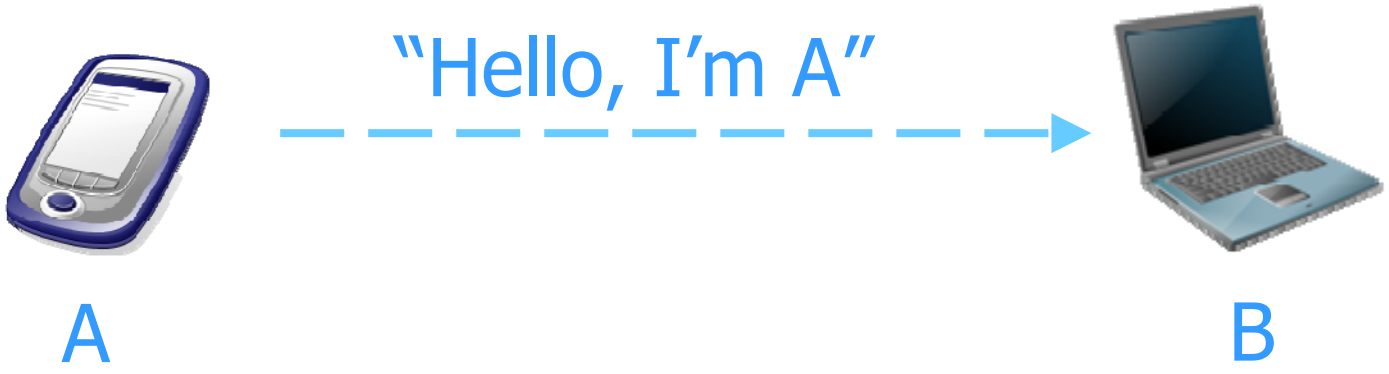
- Neighbor Discovery (ND)
  - A node discovers other nodes it can *directly* communicate with

Neighbor Discovery (ND) (cont'd)



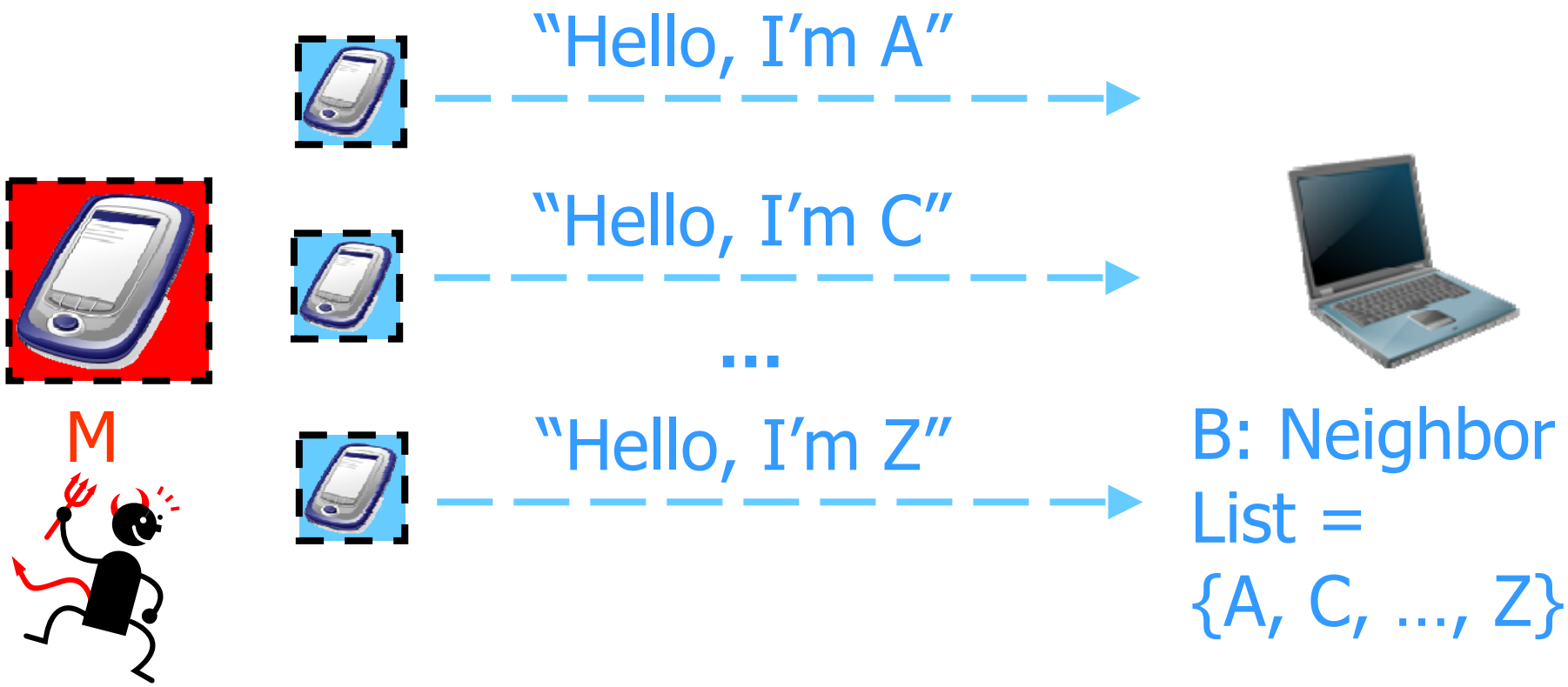
- B is neighbor of A if and only if it can receive directly from A
- Link (A,B) is *up* ⇔ A is neighbor of B
- $R_A \neq R_B$, i.e., (A,B) may be *up* while (B,A) is *down*

Neighbor Discovery (ND) (cont'd)



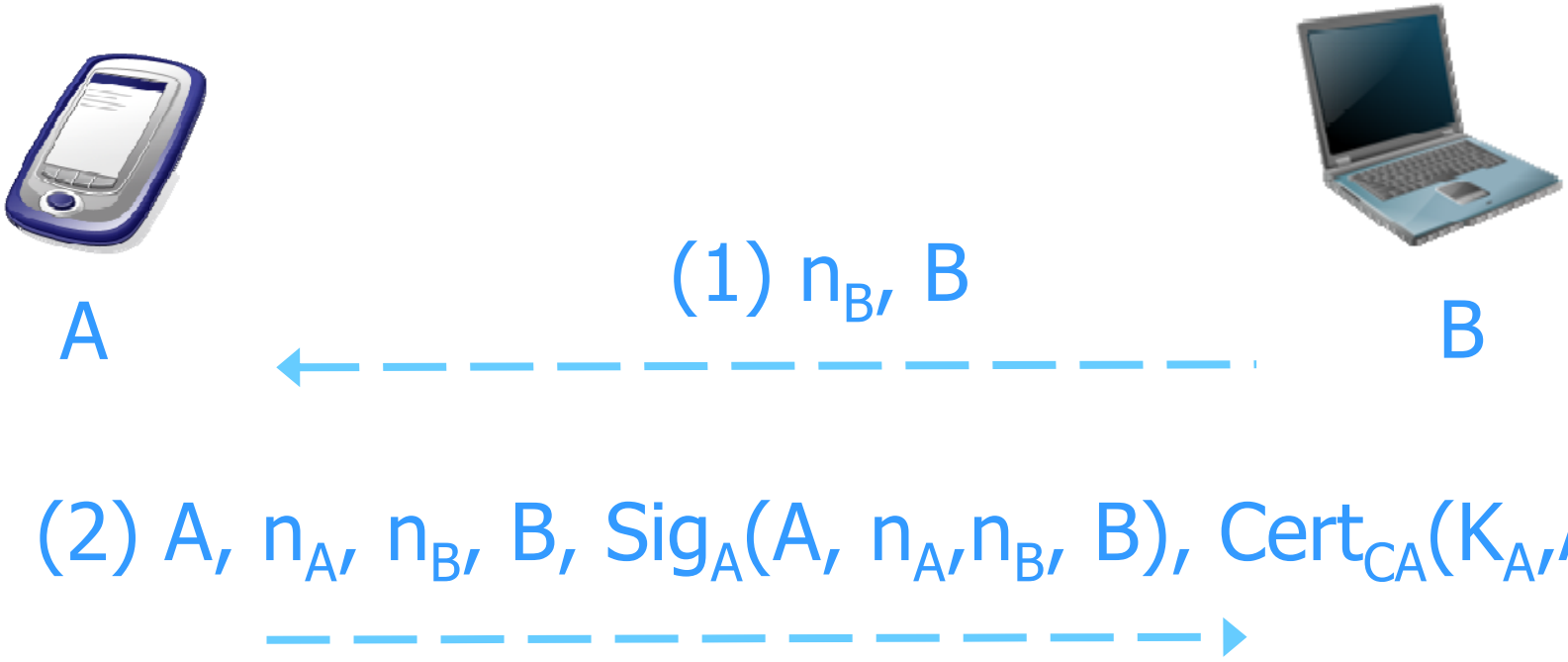
- Simple, widely used solution, but **not** secure
- Easy to attack
  - Mislead B that A is its neighbor, when this is not the case

Attacking ND



- Single adversary appears as multiple neighbors

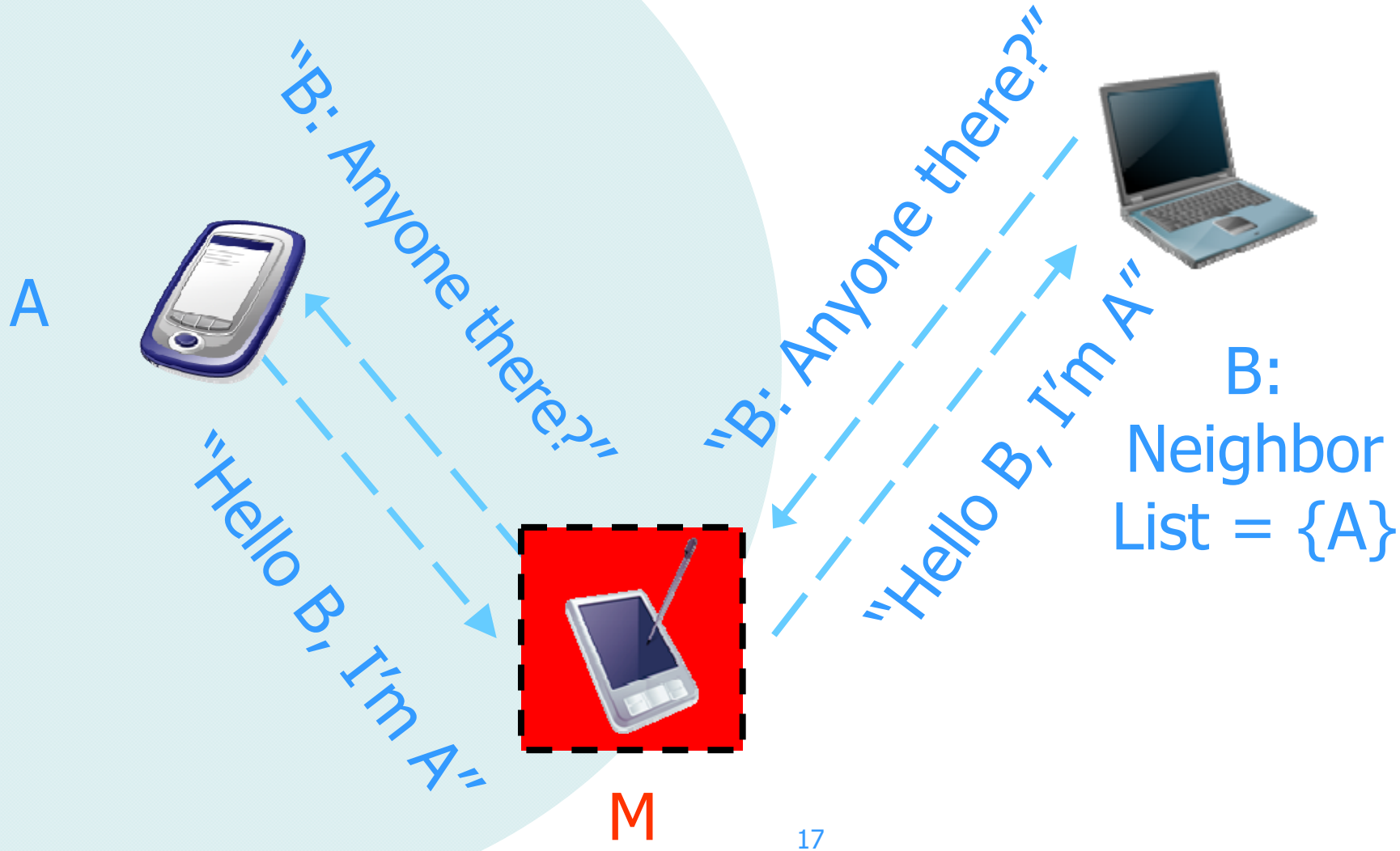
Securing ND



- An attempt
  - Message authenticity and replay protection
    - n_A, n_B are nonces
  - Bob essentially 'challenges' Alice to provide a 'hello' message

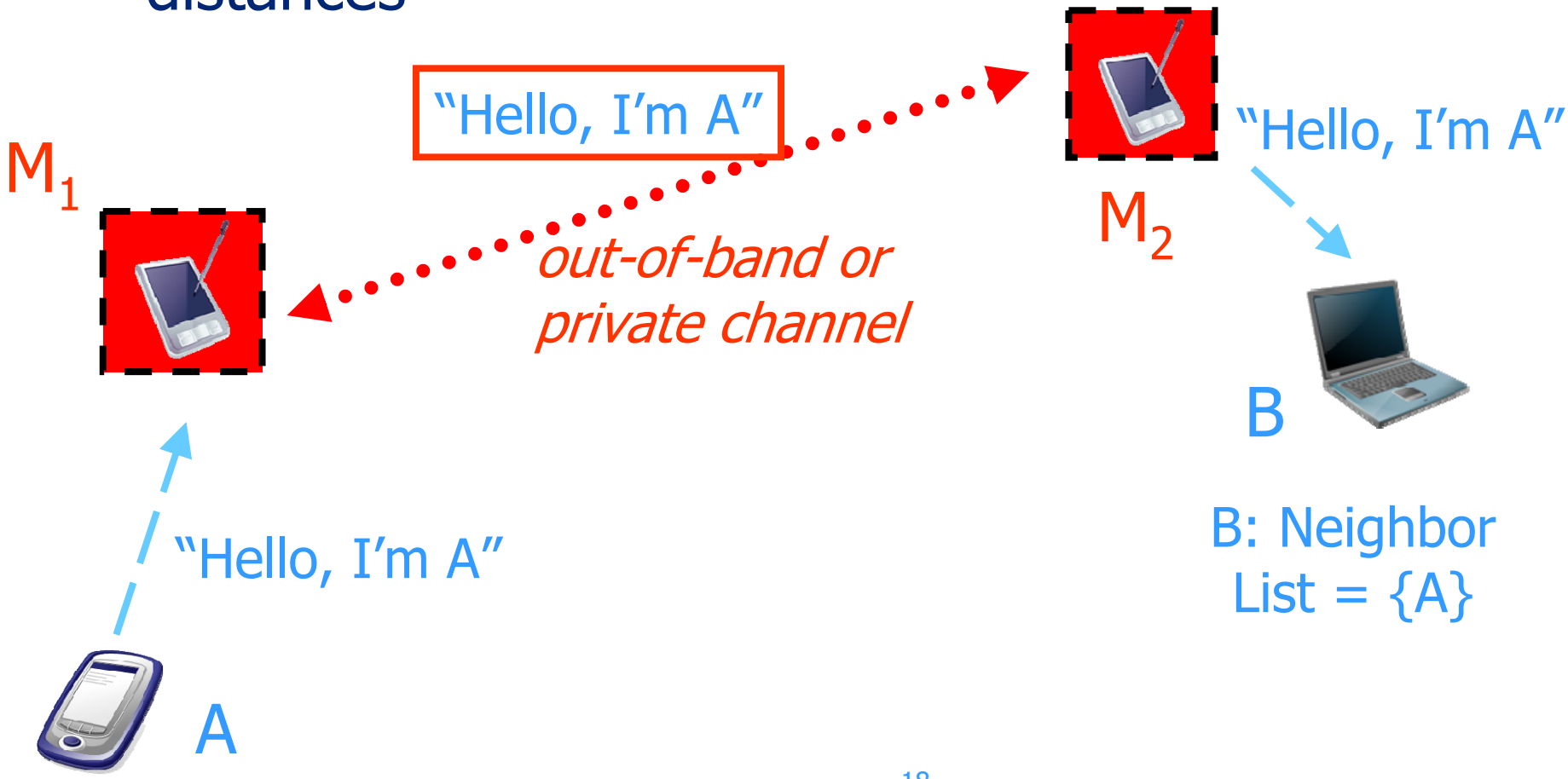
Attacking ND (cont'd)

- "Relay" or "Wormhole" Attack
  - Simply relay any message, without any modification



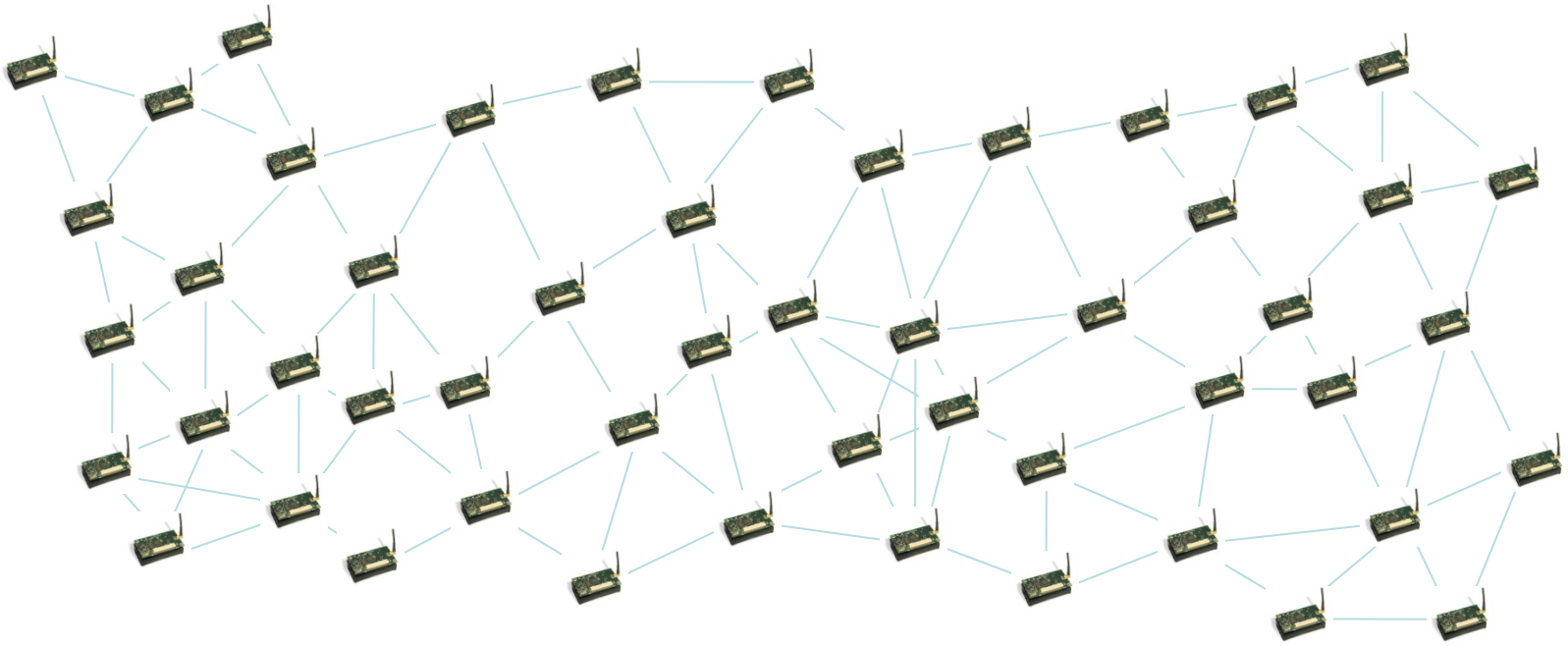
Attacking ND (cont'd)

- Long-range relay / wormhole
  - The attacker relays messages across large distances



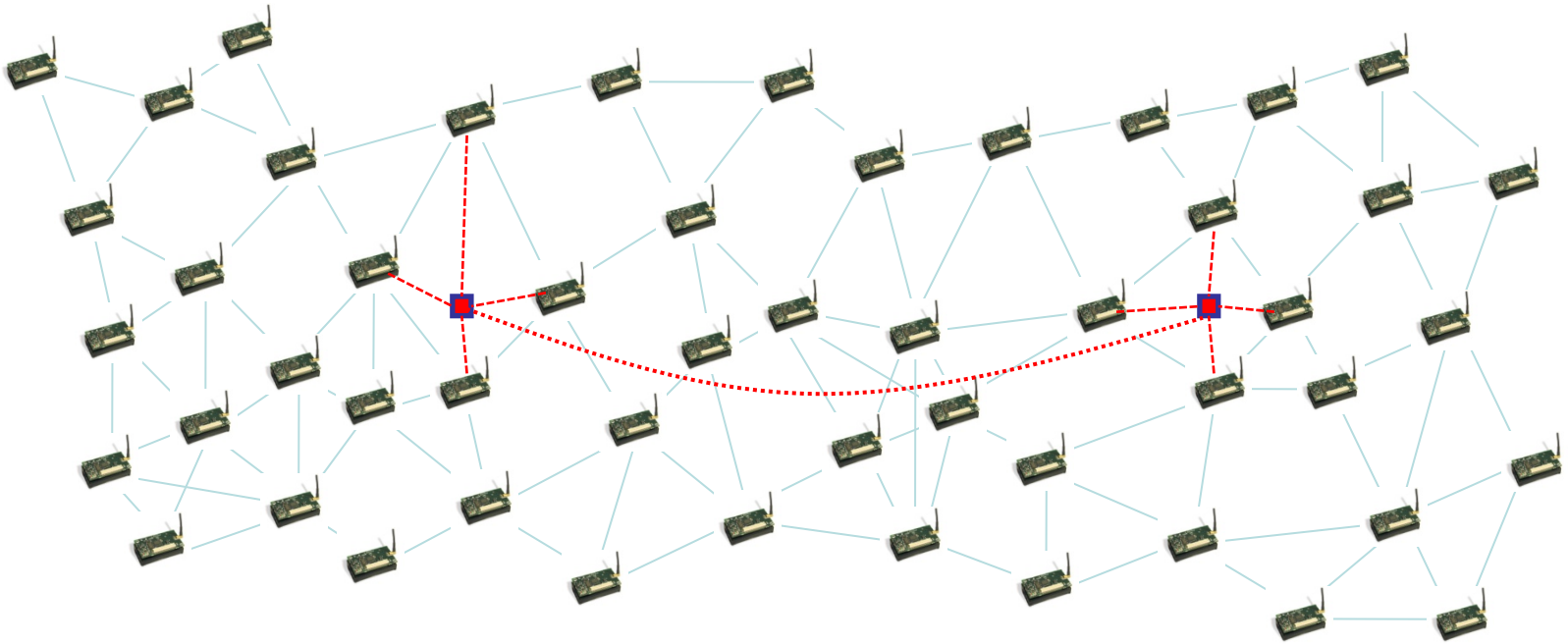
Attacking ND: Implications

- Routing in multihop ad hoc networks



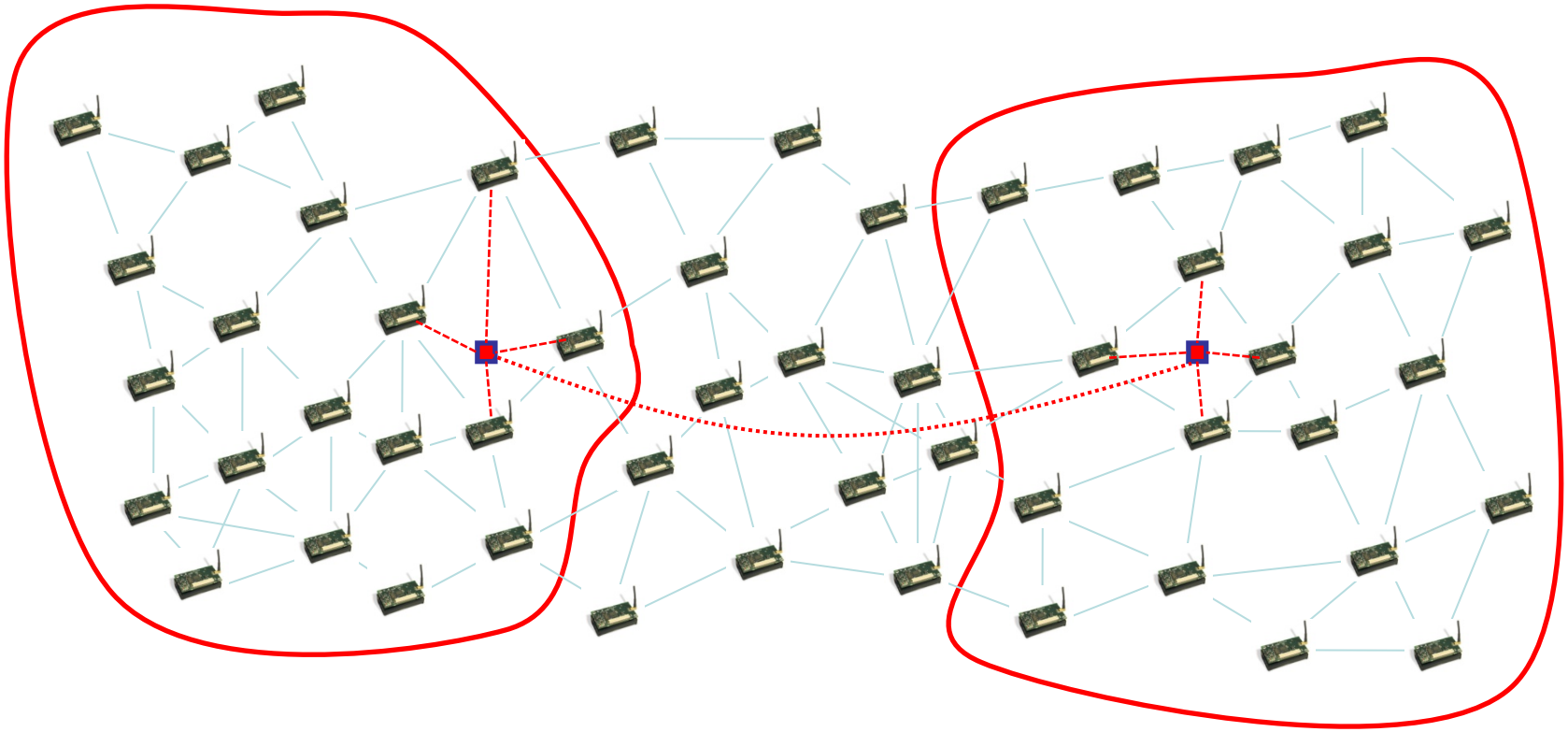
Attacking ND: Implications (cont'd)

- Routing in multihop ad hoc networks



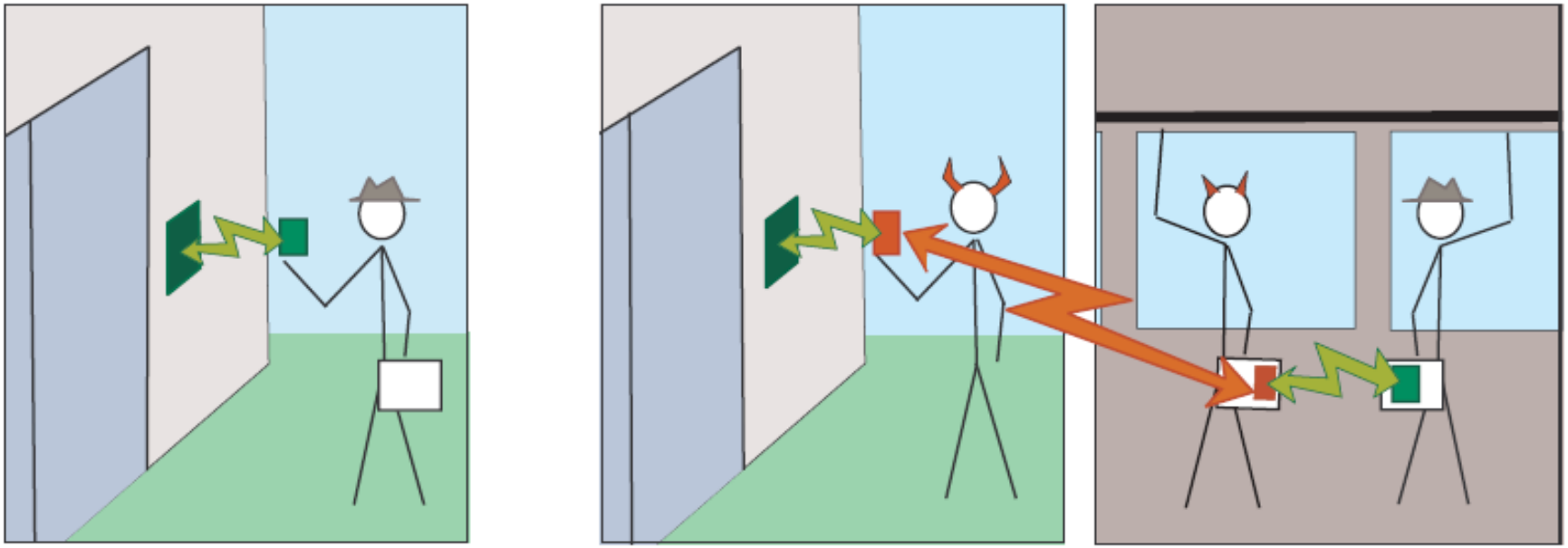
Attacking ND: Implications (cont'd)

- Routing in multihop ad hoc networks



Attacking ND: Implications (cont'd)

- RFID-based access control

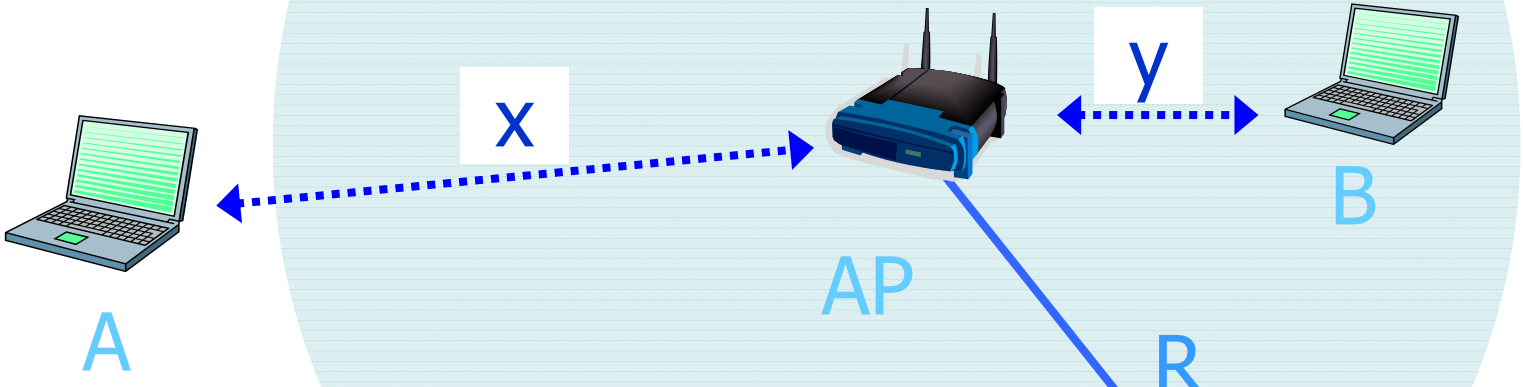


- Attacker close to the access-granting RFID tag
  - Relays signals from and to her accomplice, who obtains access

Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contact-less smartcard," SECURECOMM '05

Securing Two-Party ND

- Basic ideas
  - Authentication
  - Node-to-node distance estimation



  - x>R ➔ A: AP not neighbor
  - Y<R ➔ B: AP neighbor

Securing Two-Party ND (cont'd)

- Use message time-of-flight to measure distance
  - Distance Bounding [1]
  - Temporal Packet Leashes [2]
  - SECTOR [3]
- Use node location to measure distance
  - Geographical Packet Leashes [2]

[1] S. Brands and D. Chaum, "Distance-bounding protocols," EUROCRYPT '93
[2] Y.-C. Hu, A. Perrig, and D. B. Johnson. "Packet leashes: A defense against wormhole attacks in wireless networks," INFOCOM '03
[3] S. Capkun, L. Buttyan, and J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks," SASN '03

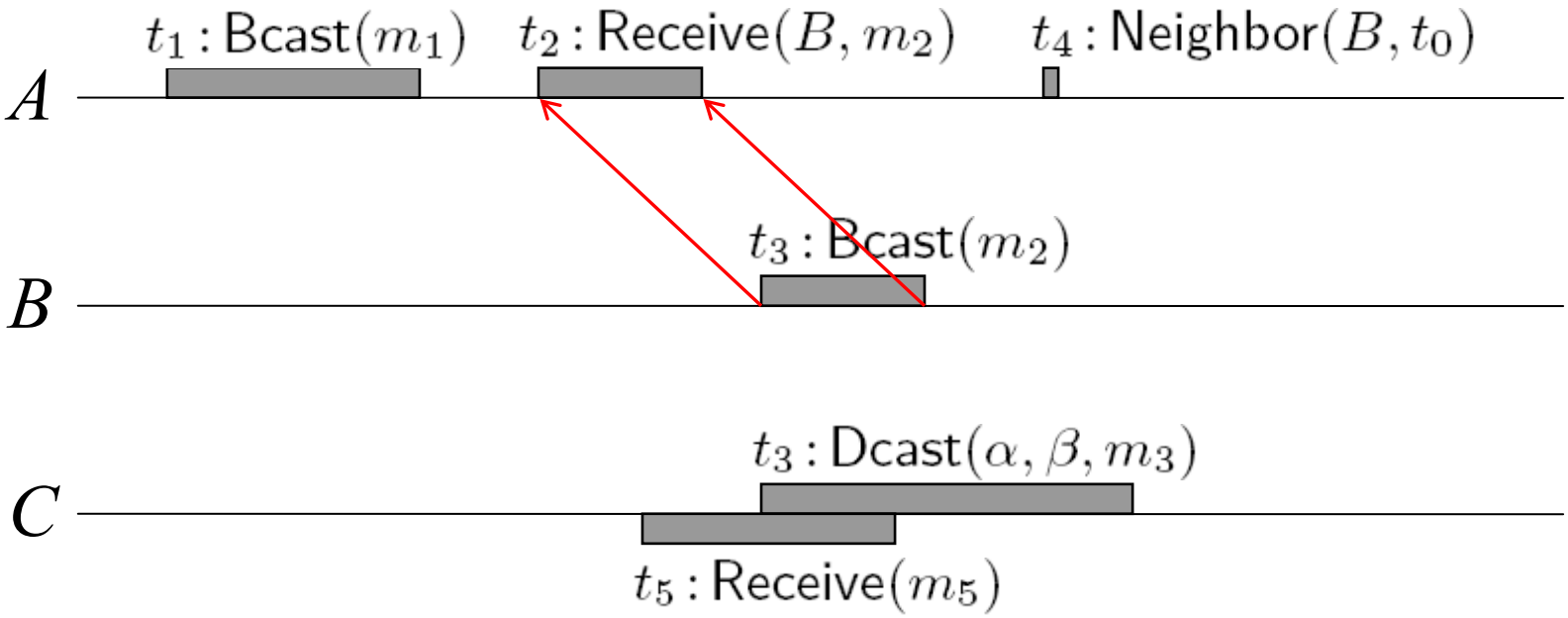
Securing Two-Party ND (cont'd)

- Are these protocols [1,2,3] achieving secure ND?
- Can any protocol, including and similar to [1,2,3], which can measure time, solve the secure ND problem?
- Is there any provably secure ND protocol?
- *Note:* Measurements can be *very* accurate

None of the above protocols secures ND
No (secure) ND protocol that relies on time measurements does

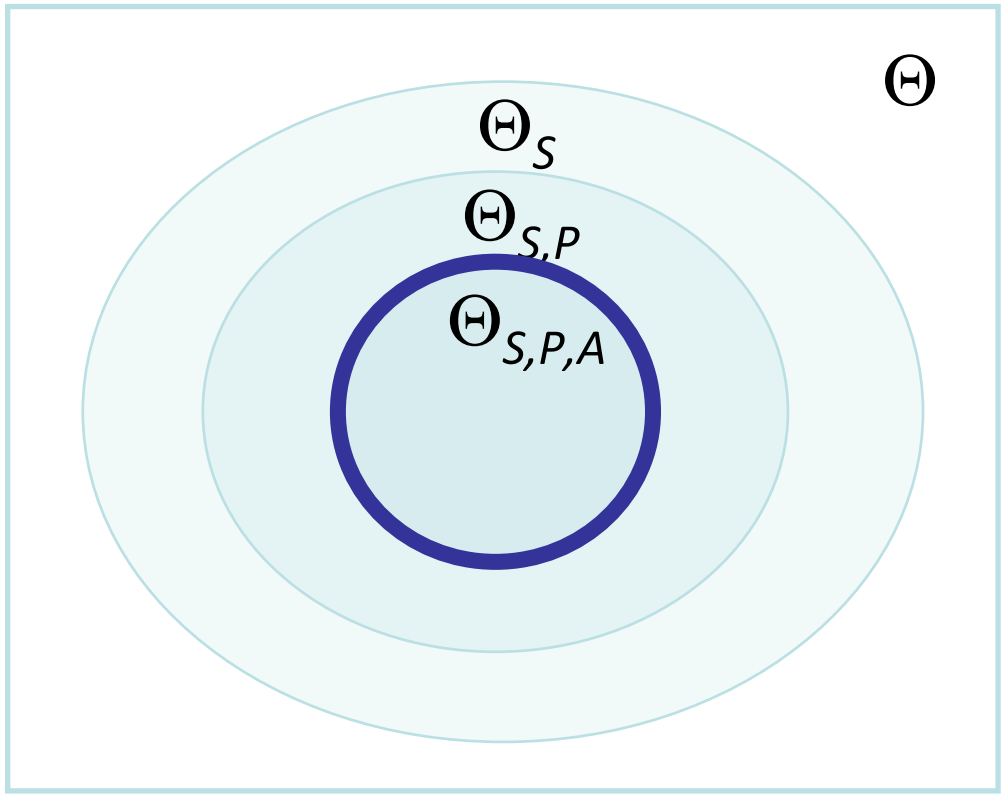
Traces and Events

- **Trace** $\theta \in \Theta$ is a set of **events**



Feasible Traces

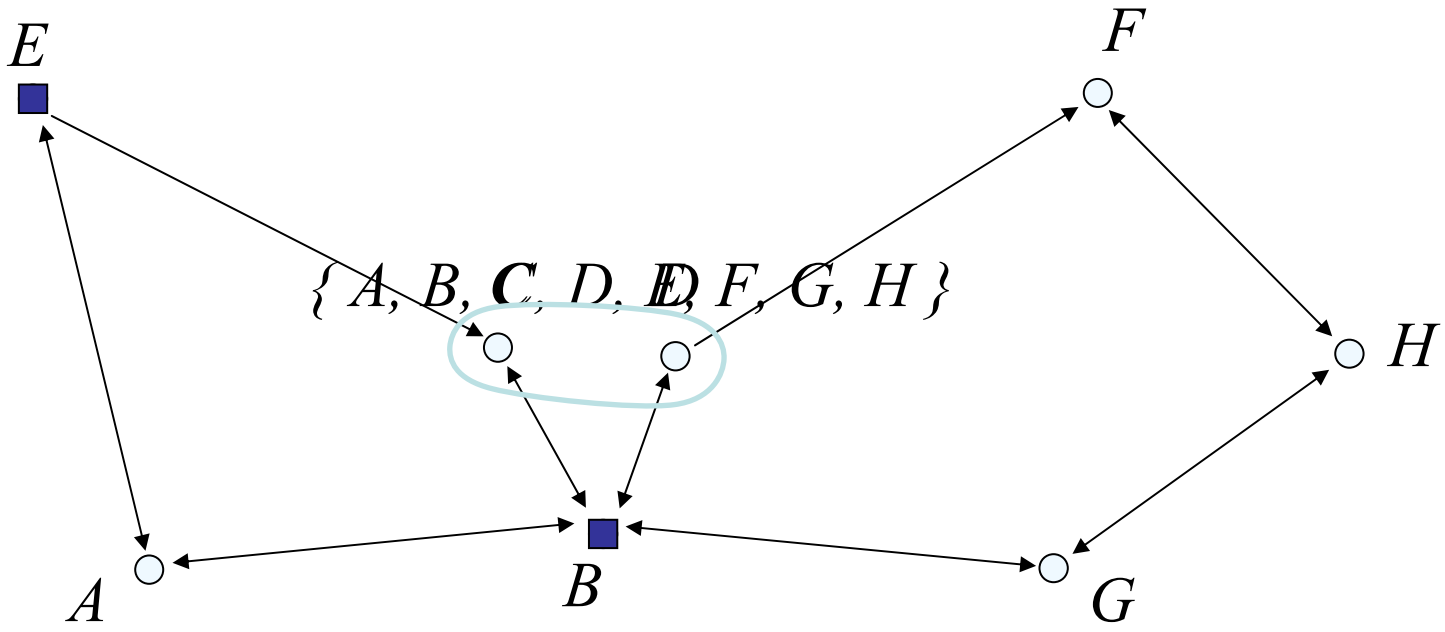
- System execution: **feasible** trace
- Traces feasible with respect to:



- Setting *S*
- Protocol *P*
- Adversary *A*

Setting $\mathcal{S}$

$$\mathcal{S} = \langle nodes, \ldots \rangle$$



$$link : nodes^2 \times \mathbb{R}_{\geqslant 0} \rightarrow \{up, down\}$$

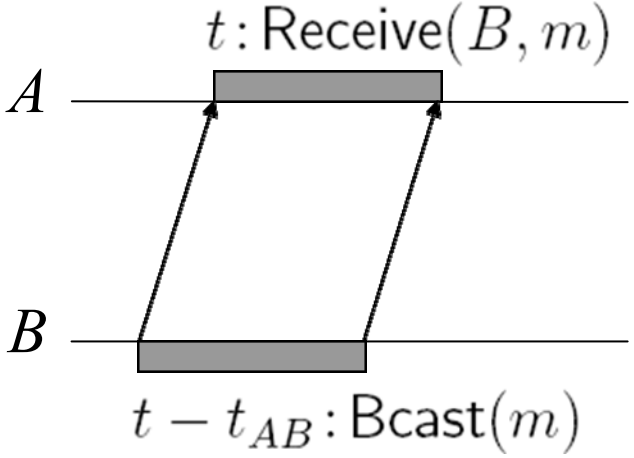
Trace θ Feasible *wrt* Setting S

- Causal and timely message exchange

$$\forall\ \mathsf{Receive}(A;t;B,m) \in \theta,\quad [t,t+|m|]:B \rightarrow A\ \wedge\ \mathsf{Bcast}(B;t-t_{AB};m) \in \theta$$

$$t_{AB} = \frac{dist(A,B)}{\mathbf{v}}$$

v – signal propagation speed



Trace θ Feasible *wrt* Setting S (cont'd)

- Causal and timely message exchange

$$\forall\ \mathsf{Receive}(A;t;B,m) \in \theta,$$
$$(A,B \in V)\ \wedge\ ([t,t+|m|]:B{\rightarrow}A)\ \wedge$$
$$(\mathsf{Bcast}(B;t-t_{AB};m) \in \theta\ \veebar\ (inrange(B,\alpha,\beta,A)\ \wedge$$
$$\mathsf{Dcast}(B;t-t_{AB};\alpha,\beta,m) \in \theta))$$

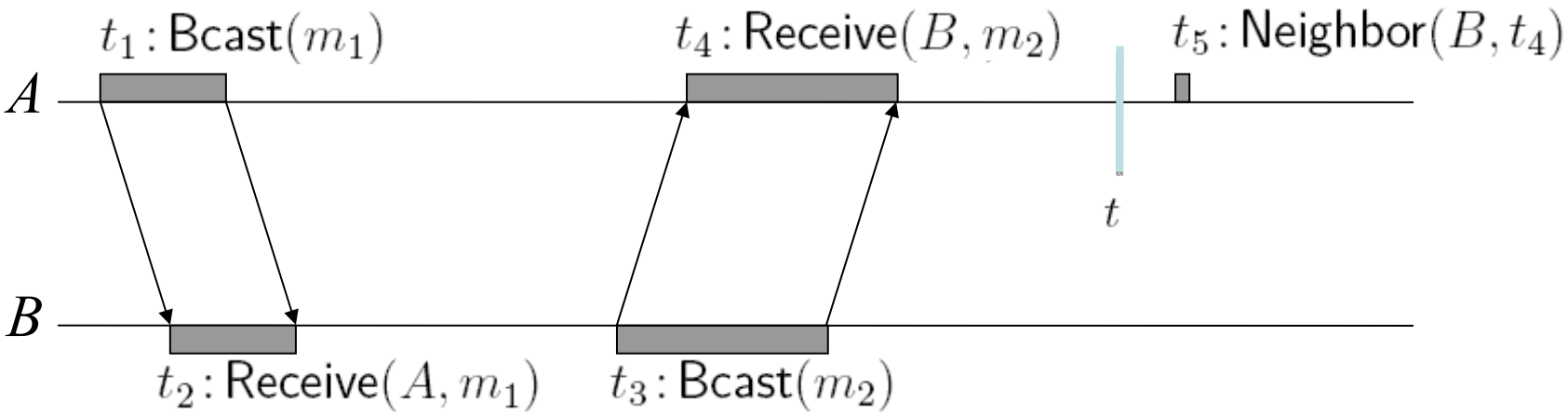
$$\forall\ \mathsf{Bcast}(A;t;m) \in \theta,\quad (A \in V)\ \wedge$$
$$(\forall B \in V,\quad [t+t_{AB},t+t_{AB}+|m|]:A{\rightarrow}B\ \Longrightarrow$$
$$\mathsf{Receive}(B;t+t_{AB};A,m) \in \theta)$$

$$\forall\ \mathsf{Dcast}(A;t;\alpha,\beta,m) \in \theta,\quad (A \in V_{\mathrm{adv}})\ \wedge$$
$$(\forall B \in V,\quad (inrange(A,\alpha,\beta,B)\ \wedge$$
$$[t+t_{AB},t+t_{AB}+|m|]:A{\rightarrow}B)\ \Longrightarrow$$
$$\mathsf{Receive}(B;t+t_{AB};A,m) \in \theta)$$

$$t_{AB} = \frac{dist(A,B)}{\mathbf{v}}$$

Local Trace

$$\theta \rightsquigarrow \theta|_{A,t}$$



Protocol $\mathcal{P}$

- Local view

$$\begin{array}{ll} \mathrm{T} & \theta||_{A,t} = \langle A, t, \theta|_{A,t} \rangle \\ \mathrm{TL} & \theta||_{A,t} = \langle A, t, loc(A), \theta|_{A,t} \rangle \end{array}$$

- Protocol

$$\mathcal{P} : \text{local view} \mapsto \text{set of actions}$$

- Actions
  - Bcast(m)
  - Neighbor(B, t)
  - ϵ

Trace θ Feasible *wrt* Protocol

- Correct nodes follow the protocol

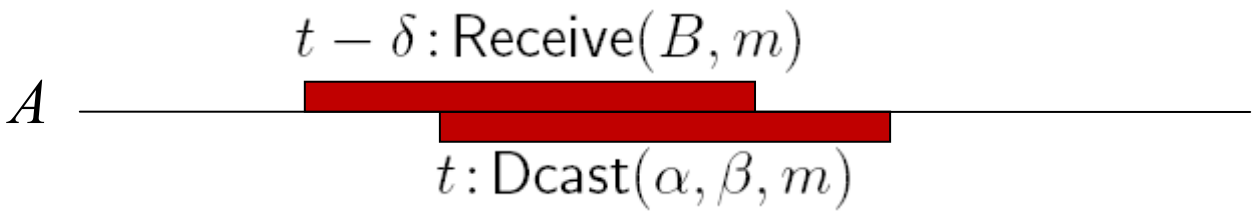
$$\forall A \in V_{\text{cor}}, \quad \forall\ \mathsf{Bcast}(A; t; m) \in \theta, \quad \mathsf{Bcast}(m) \in \mathcal{P}(\theta||_{A,t})$$

$$\forall A \in V_{\text{cor}}, \quad \forall\ \mathsf{Neighbor}(A; t; B, t') \in \theta,$$
$$\mathsf{Neighbor}(B, t') \in \mathcal{P}(\theta||_{A,t})$$

$$\forall A \in V_{\text{cor}}, \quad \forall t \in X_A, \quad \epsilon \in \mathcal{P}(\theta||_{A,t}), \text{ where}$$
$$X_A = \mathbb{R}_{\geqslant 0} \setminus start(\theta|_A \cap E),$$
$$E = \{t : \mathsf{Bcast}(m) \mid m \in \mathbb{M}, t \in \mathbb{R}_{\geqslant 0}\} \cup$$
$$\{t : \mathsf{Neighbor}(B, t') \mid B \in \mathbb{V}, t, t' \in \mathbb{R}_{\geqslant 0}\}$$

Trace θ Feasible *wrt* Adversary

- Adversarial nodes can only relay messages with minimum delay $\Delta_{\text{relay}} > 0$



$$\delta > \Delta_{\text{relay}}$$

- Denote the adversary as: $\mathcal{A}_{\Delta_{\text{relay}}}$

Neighbor Discovery Specification

Protocol *P* solves Neighbor Discovery for adversary *A* if

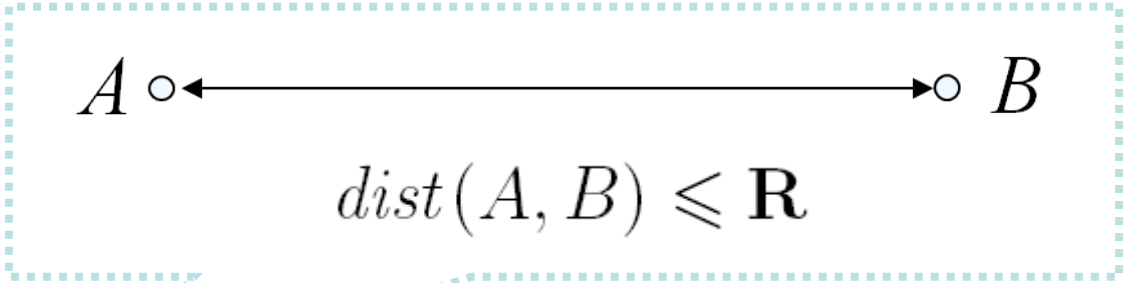
1) Discovered neighbors are actual neighbors
2) It is possible to discover neighbors

$$\text{ND1}\quad \forall \mathcal{S} \in \Sigma,\quad \forall \theta \in \Theta_{\mathcal{S},\mathcal{P},\mathcal{A}},\quad \forall A, B \in V_{\text{cor}},$$
$$\forall\ \text{Neighbor}(A; t; B, t') \in \theta,\quad t' : B \rightarrow A$$

Neighbor Discovery Specification (cont'd)

Protocol *P* solves Two-Party Neighbor Discovery for adversary *A* if

1) Discovered neighbors are actual neighbors
2) It is possible to discover neighbors **in the ND range R**



ND2 ... $\exists\theta \in \Theta_{\mathcal{S},\mathcal{P},\mathcal{A}}$, $\mathsf{Neighbor}(A; t; B, t') \in \theta$

T-protocol Impossibility

Theorem: No T-protocol can solve Neighbor Discovery for adversary $\mathcal{A}_{\Delta_{\text{relay}}}$ *if* $\Delta_{\text{relay}} < \frac{\mathbf{R}}{\mathbf{v}}$.

Proof (sketch):

Any T-protocol *P* that satisfies ND2 cannot satisfy ND1

Observation: Physical proximity does not necessarily imply correct nodes are able to communicate directly

Results

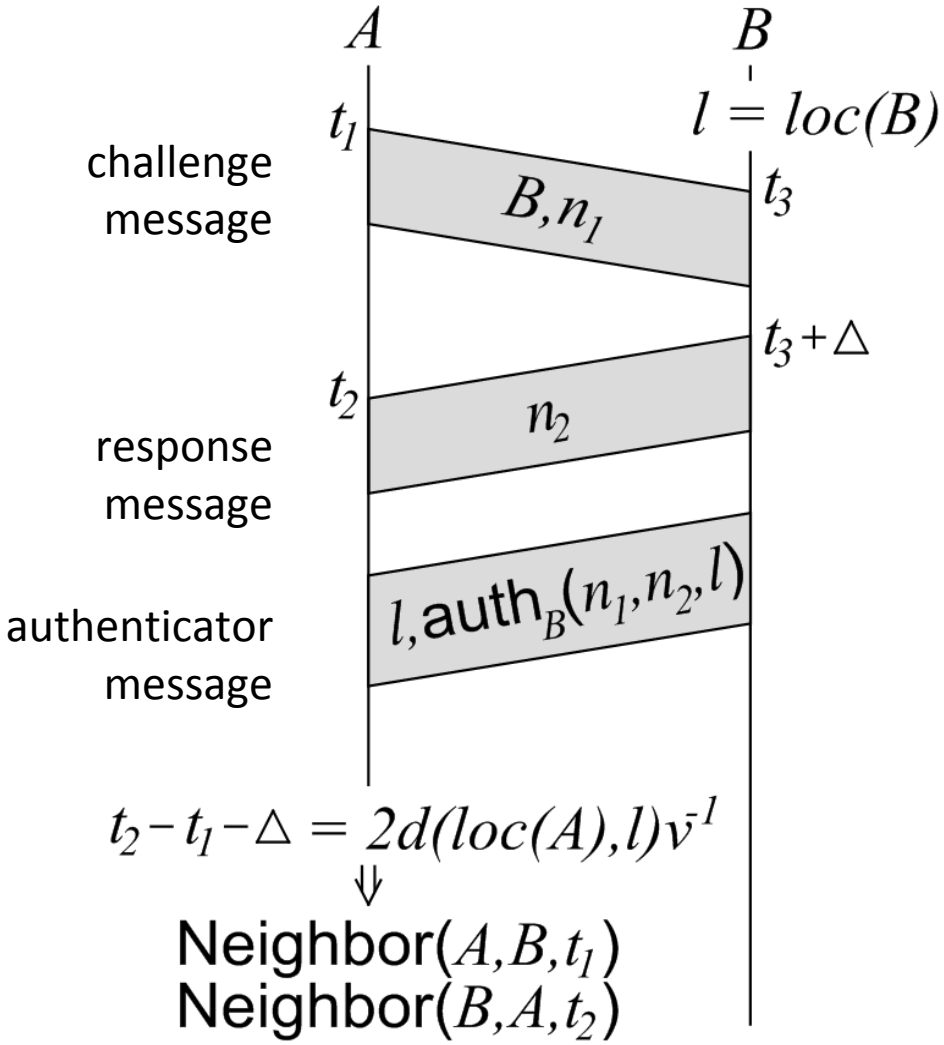
- T-protocol ND impossibility (general case)
- T-protocol solving ND (restricted case)
- TL-protocol solving ND (general case)

M. Poturalski, **P. P.**, and J-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: A Formal Investigation of Possibility," ASIACCS 2008

M. Poturalski, **P. P.**, and J-P. Hubaux, "Secure Neighbor Discovery: Is it Possible?" LCA-REPORT-2007-004, 2007

Protocol $P^{CR/TL}$

- Challenge-Response/Time-and-Location



ND Properties – Revisited (cont'd)

- Correctness:

ND1 $\quad \forall \mathcal{S} \in \mathit{Settings}, \theta \in \Theta_{\mathcal{S},\mathcal{P},\mathcal{A}}.\ \forall A, B, C \in V_{\mathrm{cor}}, t, t' \in \mathbb{R}_{\geqslant 0}.$
$\mathsf{Neighbor}(A; t; B, C, t') \in \theta \implies t' :: B \rightarrow C$

- Availability:

ND2$^{\mathsf{CR/TL}}$ $\quad \forall \mathcal{S} \in \mathit{Settings}, \theta \in \Theta_{\mathcal{S},\mathcal{P},\mathcal{A}}.\ \forall A, B \in \mathbb{V}_{\mathrm{cor}}, t \in \mathbb{R}_{\geqslant 0}.$
$\mathsf{NDstart}(A; t; B) \in \theta \ \wedge\ [t, t + T_{\mathcal{P}}] :: A \leftrightarrow B \ \wedge\ \mathit{nlos}(A, B) = 0$
$\implies \exists t_1, t_2 \in [t, \infty), t', t'' \in [t, t + T_{\mathcal{P}}].$
$\mathsf{Neighbor}(A; t_1; A, B, t') \in \theta$
$\wedge\ \mathsf{Neighbor}(A; t_2; B, A, t'') \in \theta$

T_P – protocol specific duration

Protocol $P^{CR/TL}$ (cont'd)

Theorem: Protocol $P^{CR/TL}$ satisfies the Neighbor Discovery Specification:

- Correctness (ND1)
- Availability ($ND2^{CR/TL}$)

Under the assumptions:

i. Any processing delay $\Delta_{relay} > 0$

ii. Equality of maximum information propagation speed and wireless channel propagation speed $v_{adv} = v$

M. Poturalski, **P. P.**, and J.-P. Hubaux, "Towards provable secure neighbor discovery in wireless networks," CCS FMSE 2008

Summary

- Secure Neighbor Discovery
  - Prerequisite for secure networking protocols and various applications, and system security
  - Hard problem
  - Proven secure solutions
  - Implementation is not easy in practice

Additional Readings

- Overview

  P. P., M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J-P. Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking," IEEE Communications Magazine, February 2008

- Implementation

  R. Shokri, M. Poturalski, G. Ravot, **P. P.**, and J.-P. Hubaux, "A Low-Cost Secure Neighbor Verification Protocol for Wireless Sensor Networks," *ACM WiSec, Zurich, Switzerland,* March 2009

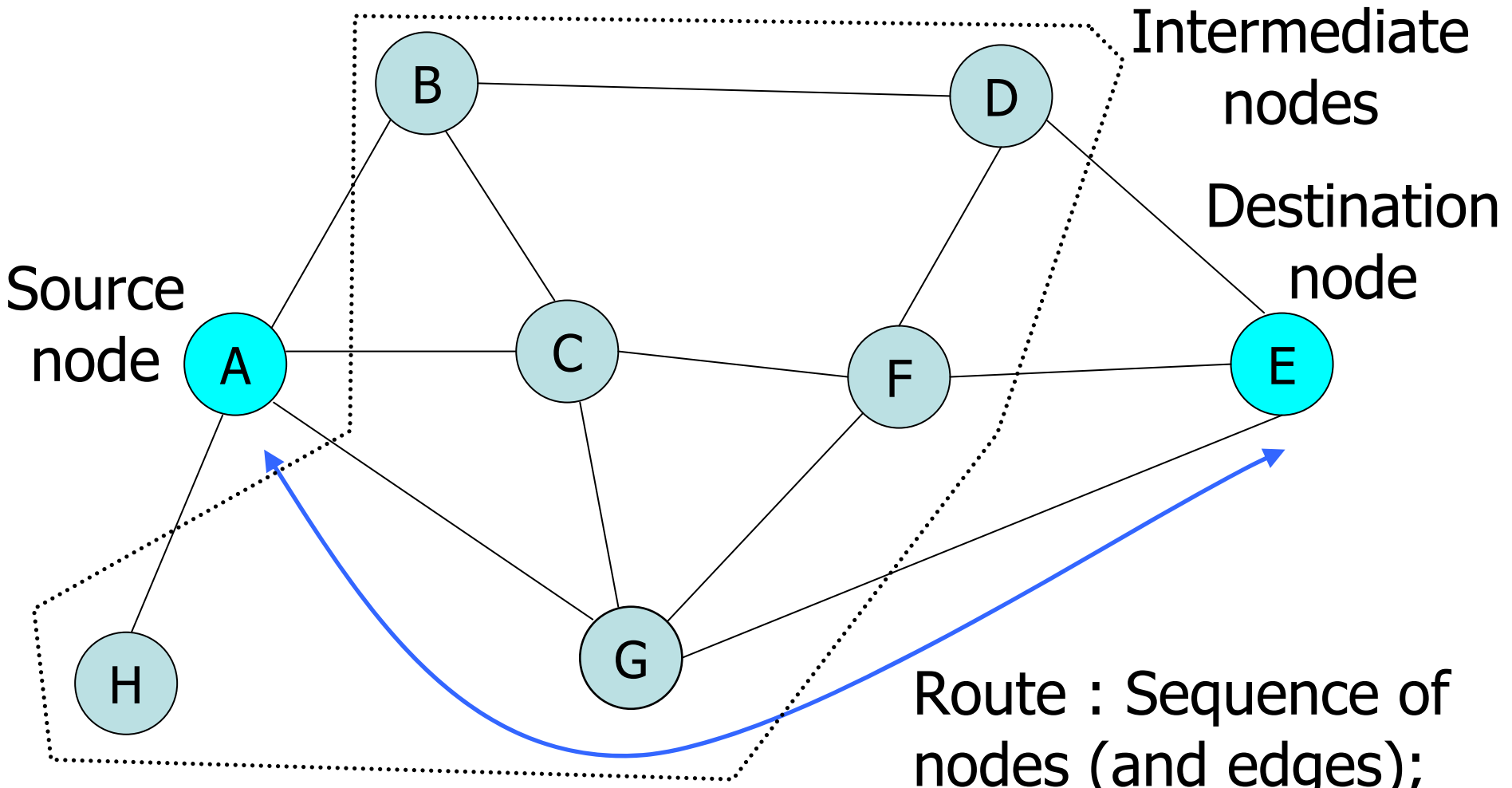
- Beyond relay attacks: Early Detect / Late Commit

  J. Clulow, G.P. Hancke, M.G. Kuhn, and T. Moore, "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," ESAS, Hambourg, Germany, September 2006

Secure Route Discovery

© 2009 P. Papadimitratos

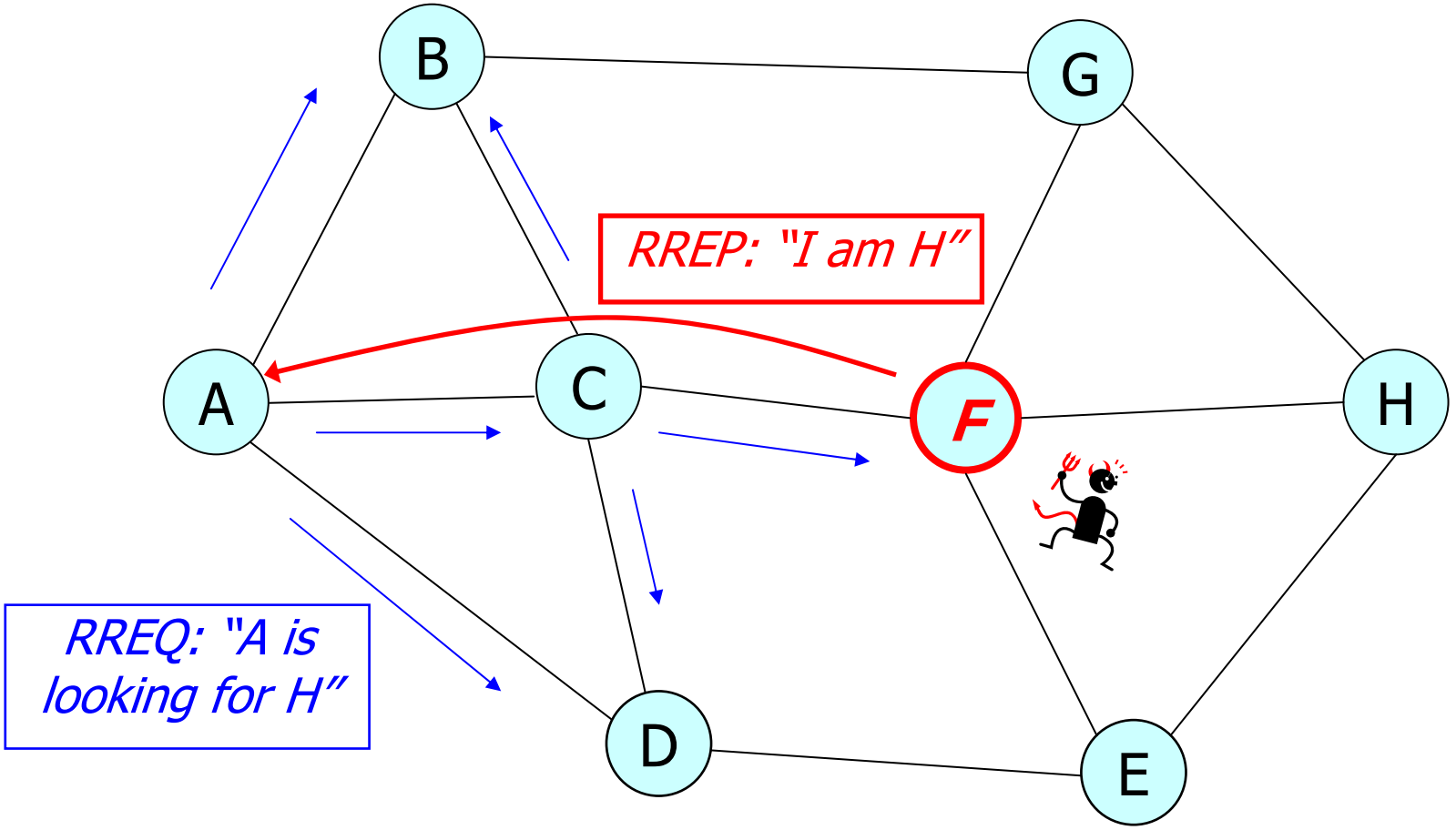
Route Discovery



- Stage 0: Neighbor discovery
- Stage 1: Route discovery

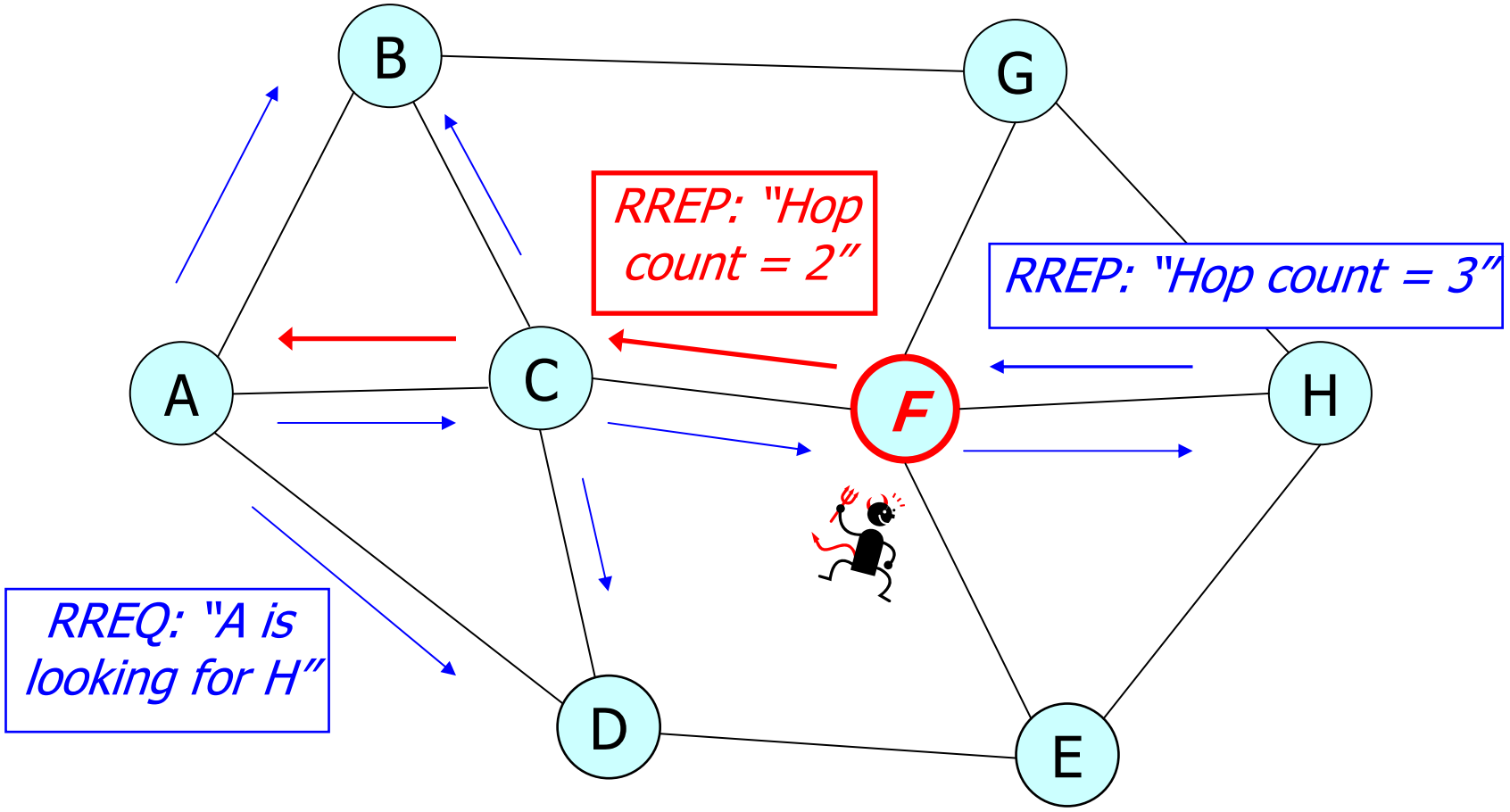
Route : Sequence of nodes (and edges); for simplicity: (A, G, E)

Attacking Route Discovery



- Impersonation of the destination, for example, in any reactive routing protocol

Attacking Route Discovery (cont'd)



- Disrupting distance vector routing (for example, in AODV)

Attacking Route Discovery (cont'd)

- Caution: None of these protocols (DSR, AODV) was designed with security in mind
- Many possible ways to attack the route discovery
- Outcome of attacks
  - Control communication
    - Become part of utilized routes
    - Monopolize resources
  - Disrupt communication
    - Degrade or deny

Requirements

- We are interested in protocols that discover routes with the following two properties:

  (1) ***Loop-freedom***: an (S,T)-route is loop-free when it has no repetitions of nodes

  (2) ***Freshness***: an (S,T)-route is fresh with respect to a (t_1,t_2) interval if each of the route's constituent links is up at some point during the (t_1,t_2)

- Loop-freedom and freshness are relevant for both explicit and implicit route discovery

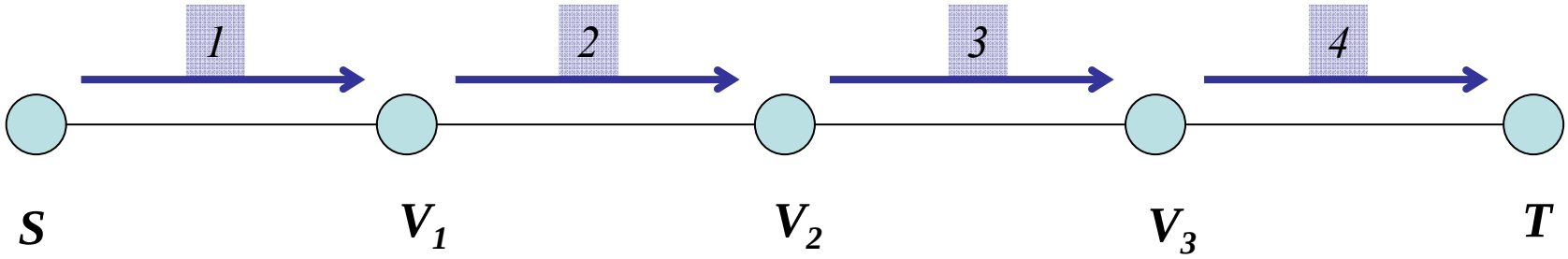
P. P., Z.J. Haas, and J.-P. Hubaux, "How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET," BroadNets'06

Secure Routing Protocol (SRP)

- Explicit basic route discovery
- Observation
  - It is hard to 'know' all nodes in the network, i.e., establish associations with all of them
  - Often infeasible and very costly
  - Especially in 'open' networks
- SRP assumptions
  - Secure neighbor discovery
  - Hop-by-hop authentication of all control traffic
  - End nodes (source, destination) 'know' each other
    - Can set up security associations

P. P. and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," CNDS 2002

SRP (cont'd)

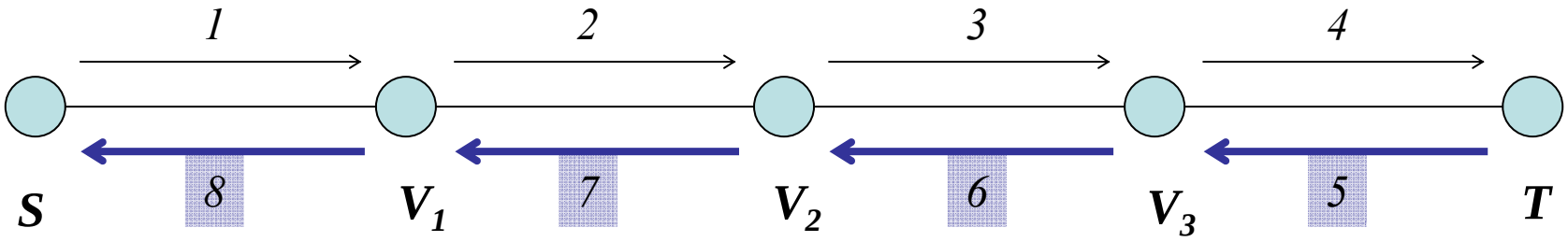


Route Request (*RREQ*):

$S, T, Q_{SEQ}, Q_{ID}, MAC(K_{S,T}, S, T, Q_{SEQ}, Q_{ID})$

1. *S* broadcasts *RREQ*;
2. V_1 broadcasts *RREQ*, $\{V_1\}$;
3. V_2 broadcasts *RREQ*, $\{V_1, V_2\}$;
4. V_3 broadcasts *RREQ*, $\{V_1, V_2, V_3\}$;

SRP (cont'd)



Route Reply (*RREP*):

Q_{ID}, {T, V_3, V_2, V_1, S},

$MAC(K_{S,T}, Q_{ID}, Q_{SEQ}, T, V_3, V_2, V_1, S)$

5. $T \rightarrow V_3$: *RREP*;
6. $V_3 \rightarrow V_2$: *RREP*;
7. $V_2 \rightarrow V_1$: *RREP*;
8. $V_1 \rightarrow S$: *RREP*;

Additional Readings

- Secure Explicit Routing
  - Link State Routing

    P. P. and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," IEEE WSAAN, Orlando, Florida, January 2003

  - Reactive Route Discovery
    - Ariadne

    Y.-C. Hu, A. Perrig, and D. Johnson, ”Ariadne: A secure on-demand routing protocol for ad hoc networks,” Wireless Networks, 2005

    - EndAir

    G. Acs, L. Buttyan, and I. Vajda, “Provably secure on-demand source routing in mobile ad hoc networks,” TMC, 2006

Additional Readings (cont'd)

- Secure Implicit Routing

  K. Sanzgiri, D. LaFlamme, B. Dahill, B.N. Levine, C. Shields, E. M. Belding-Royer, "Authenticated routing for ad hoc networks," JSAC 2005

  Y.-C. Hu, D.B. Johnson, A. Perrig, Secure efficient distance vector routing in mobile wireless ad hoc networks, IEEE WMCSA 2002

  P. P. and Z.J. Haas, "Secure On-Demand Distance Vector Route Discovery in Ad Hoc Networks," IEEE Sarnoff Symposium, 2005

- Secure Augmented Routing
  - QoS-aware routing

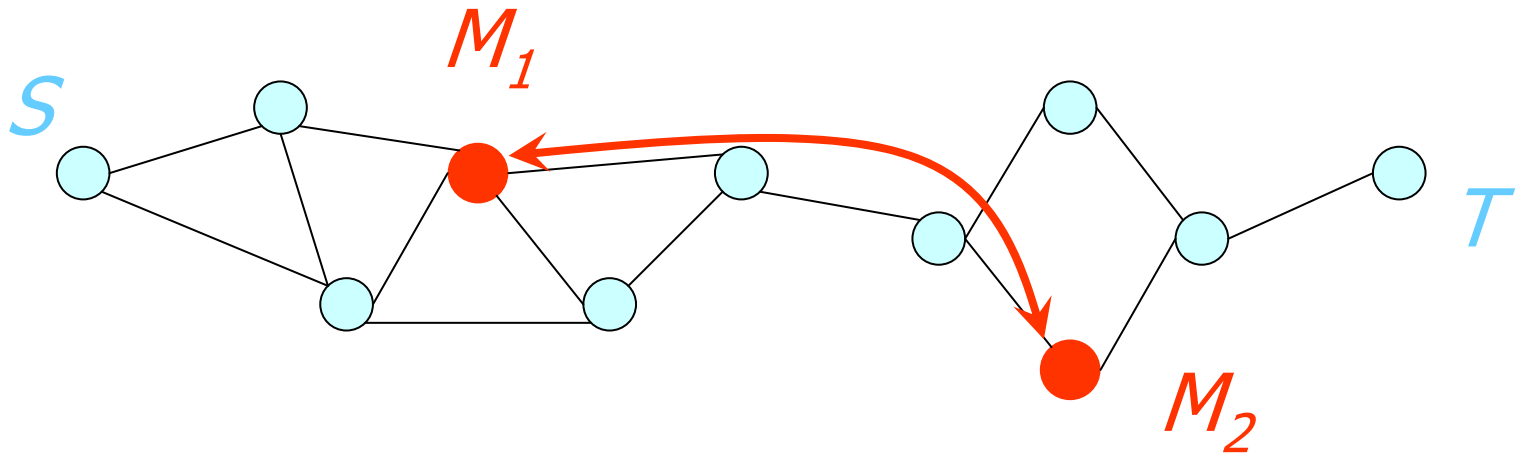
  P. P. and Z.J. Haas, "Secure Route Discovery for QoS-Aware Routing in Ad Hoc Networks," IEEE Sarnoff Symposium, 2005

- Overview

  Chapter 7, L. Buttyan and J.-P. Hubaux, "Security and Cooperation in Wireless Networks", Cambridge Press, 2008

Attacking Routing - Revisited

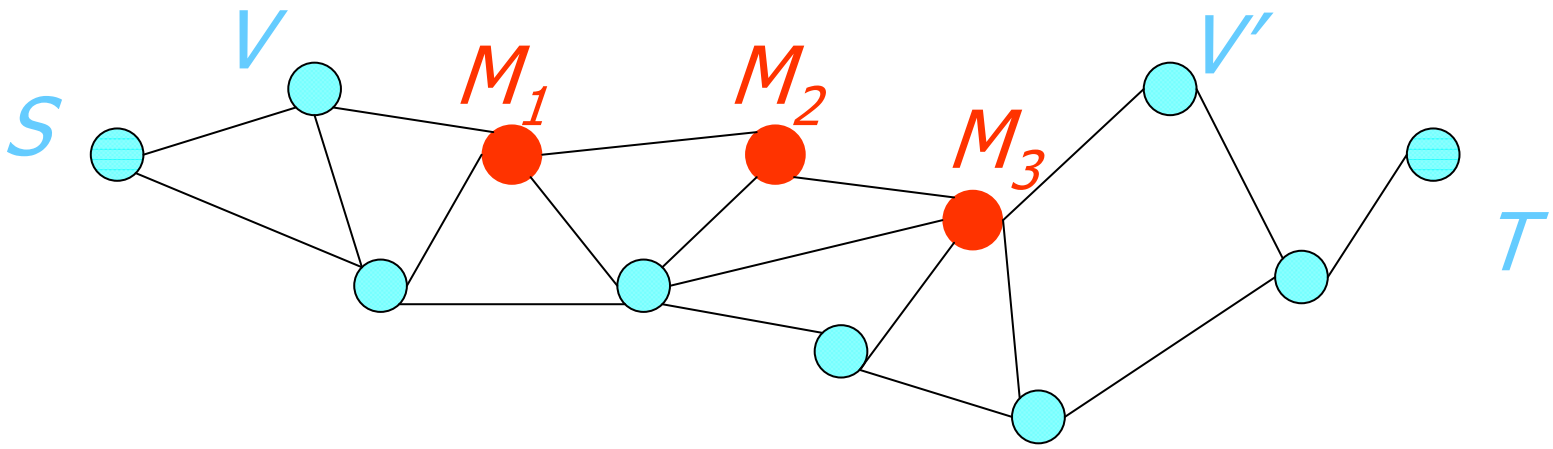
- Tunneling Attack
  - Two colluding attackers: M_1, M_2
  - M_1 encapsulates control traffic and forwards to M_2 and vice versa
  - Attackers seemingly follow the protocol with respect to their neighbors



P. P. and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," CNDS 2002

Attacking Routing – Revisited (cont'd)

- Multiple Colluding Attackers
  - M_1 and M_3 are seemingly correct to their neighbors, but they 'omit' protocol functionality when handling packets from M_2
  - Example: M_2 relays RREQ and RREP packets without appearing in the route discovery



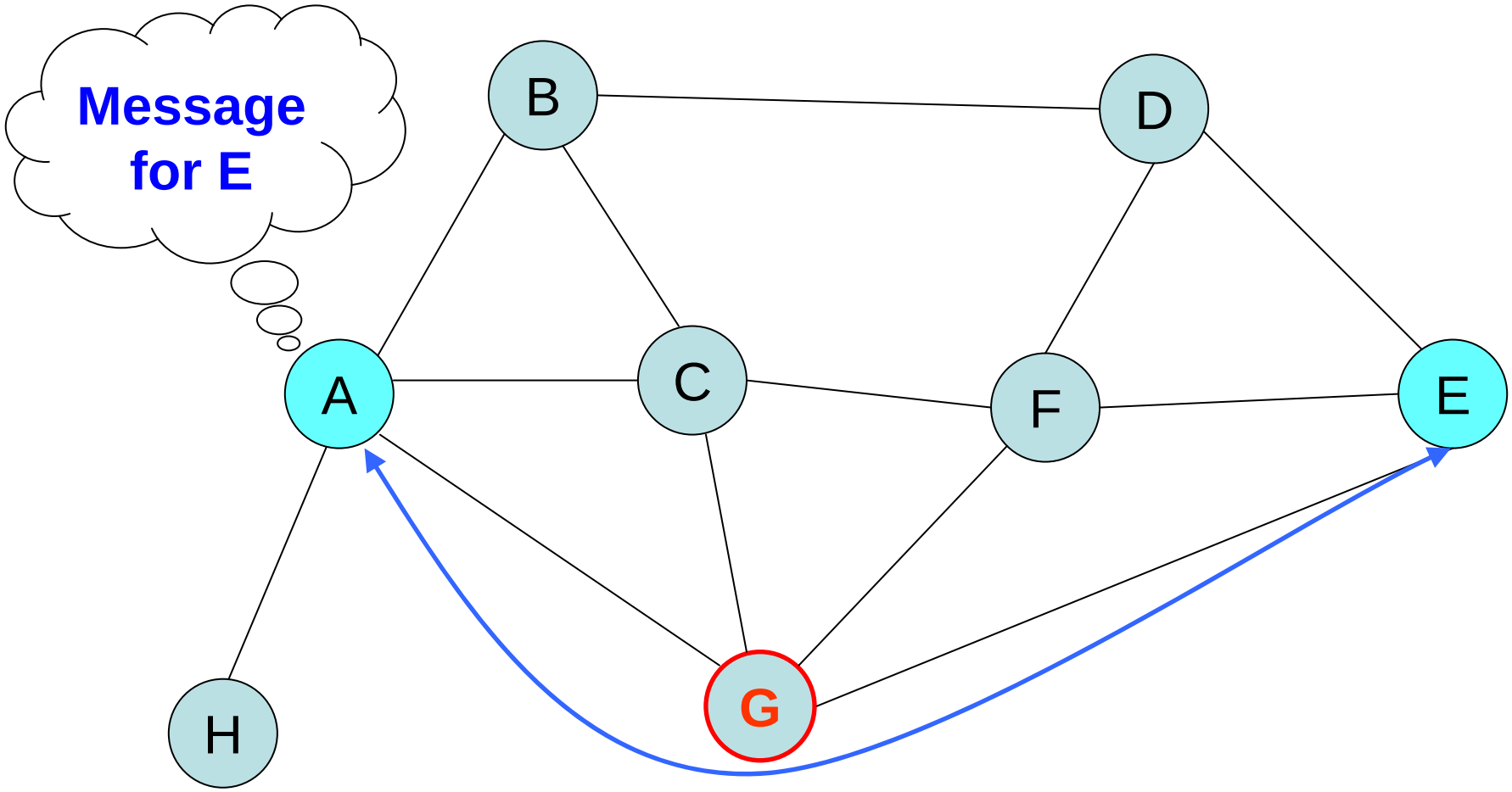
Summary

- Route discovery is vulnerable
- Secure route discovery specification
  - Loop freedom, Freshness
  - Accuracy
- Secure basic and augmented route discovery in open, dynamic networks
- Protocols rely on different trust assumptions
- Colluding adversarial nodes can subvert any route discovery protocol; 'tunneling attack'

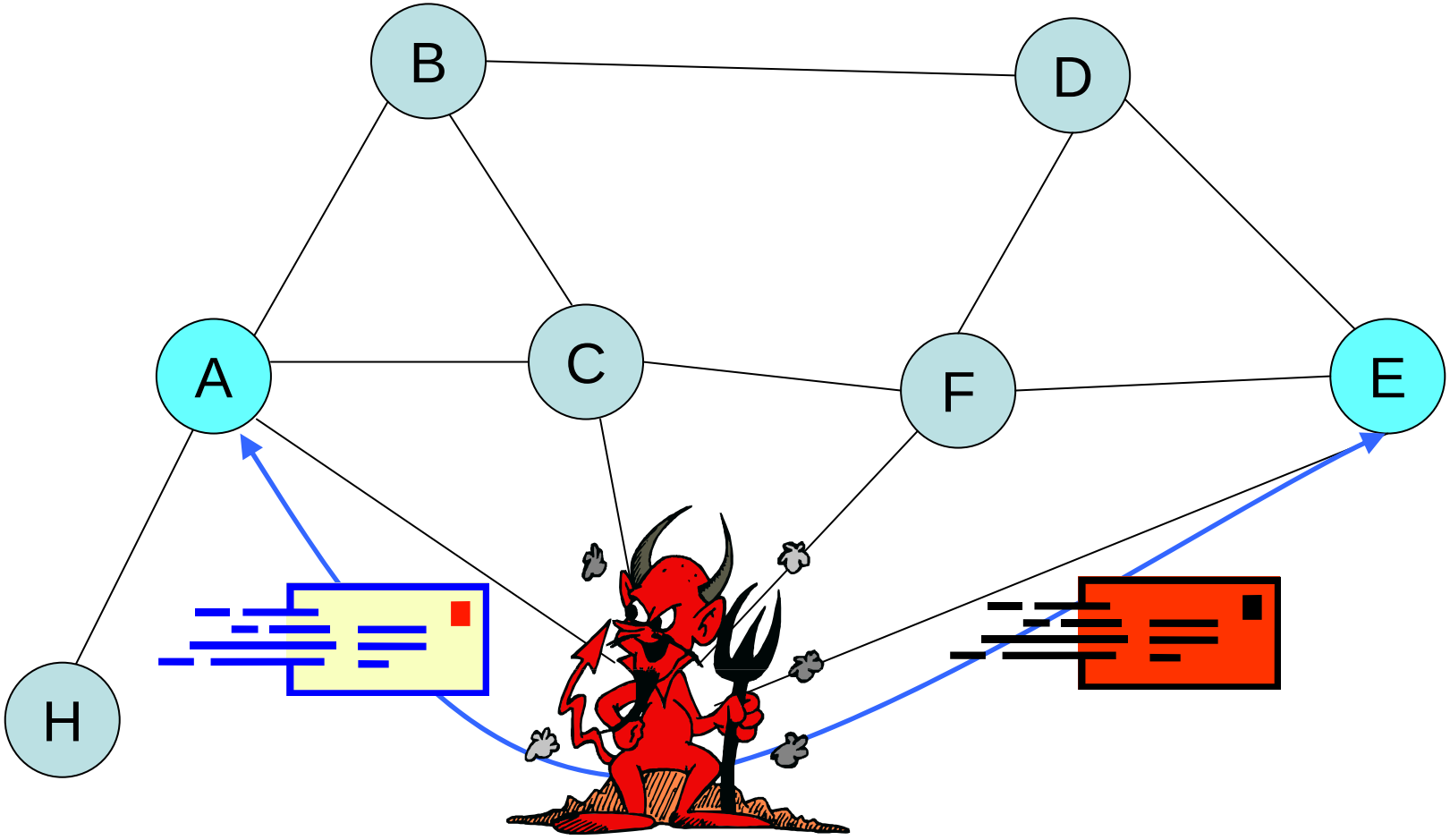
Secure Data Communication

© 2009 P. Papadimitratos

Data Communication



Data Communication (cont'd)



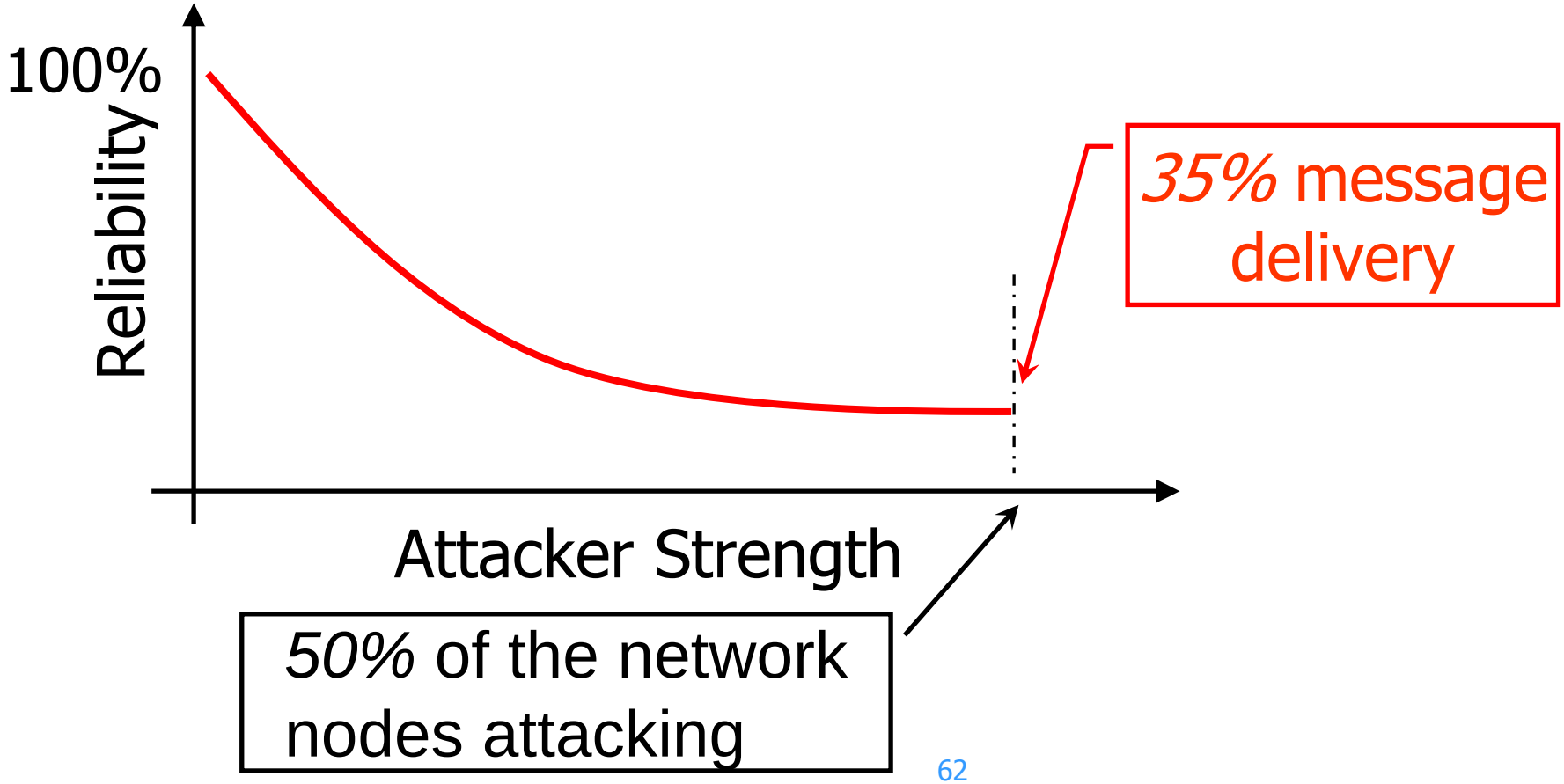
Secure Data Communication

- **Goal:**
  - Reliable and low-delay data delivery in the presence of attackers that disrupt the data communication

- **Solution:**
  - Detect and avoid compromised and failing routes
  - Tolerate malicious and benign faults
    - In general, hard to distinguish in highly dynamic networking environments

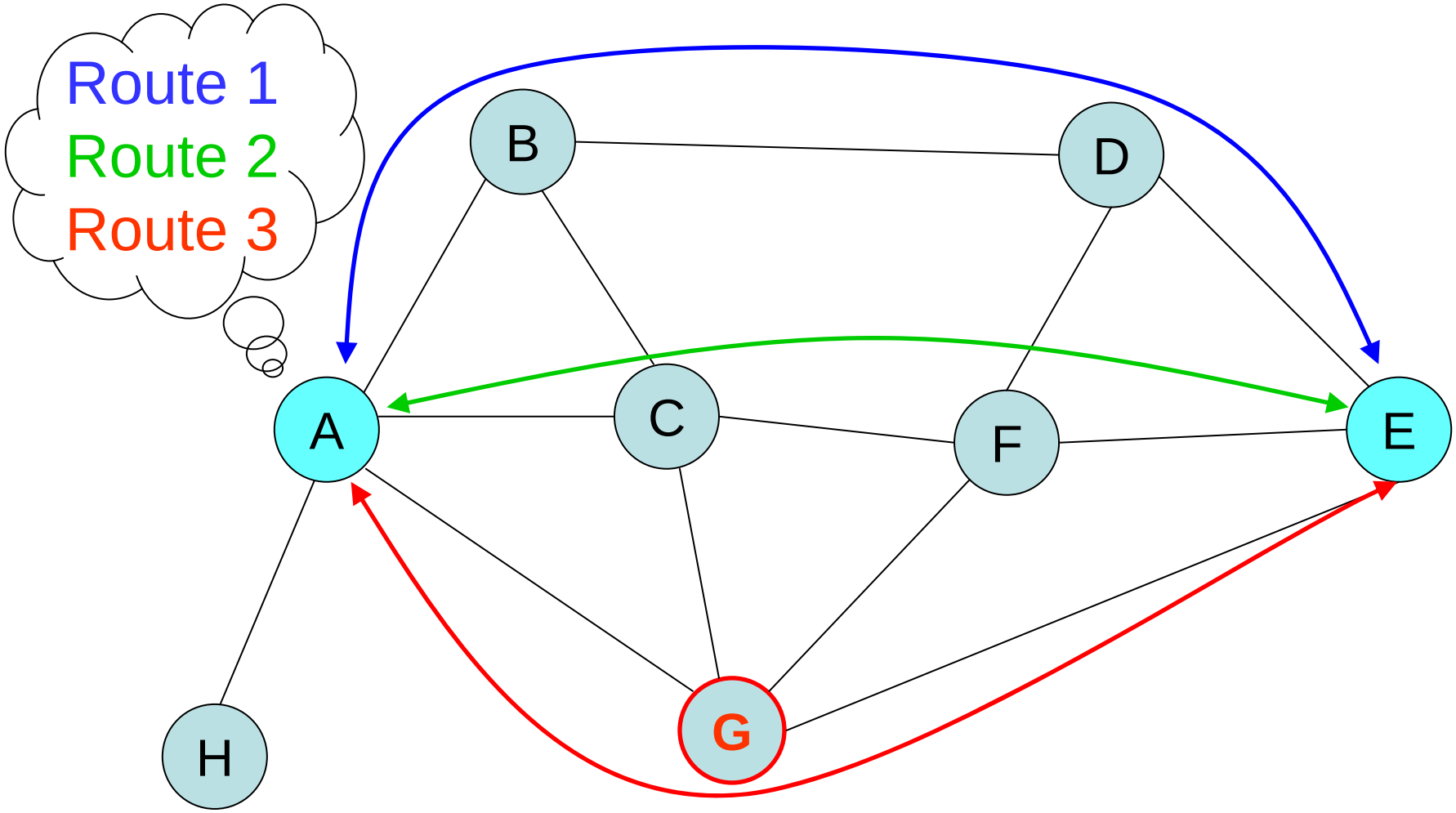
Data Communication (cont'd)

- What is the impact of the adversary that 'lies low' and disrupts only the data communication?



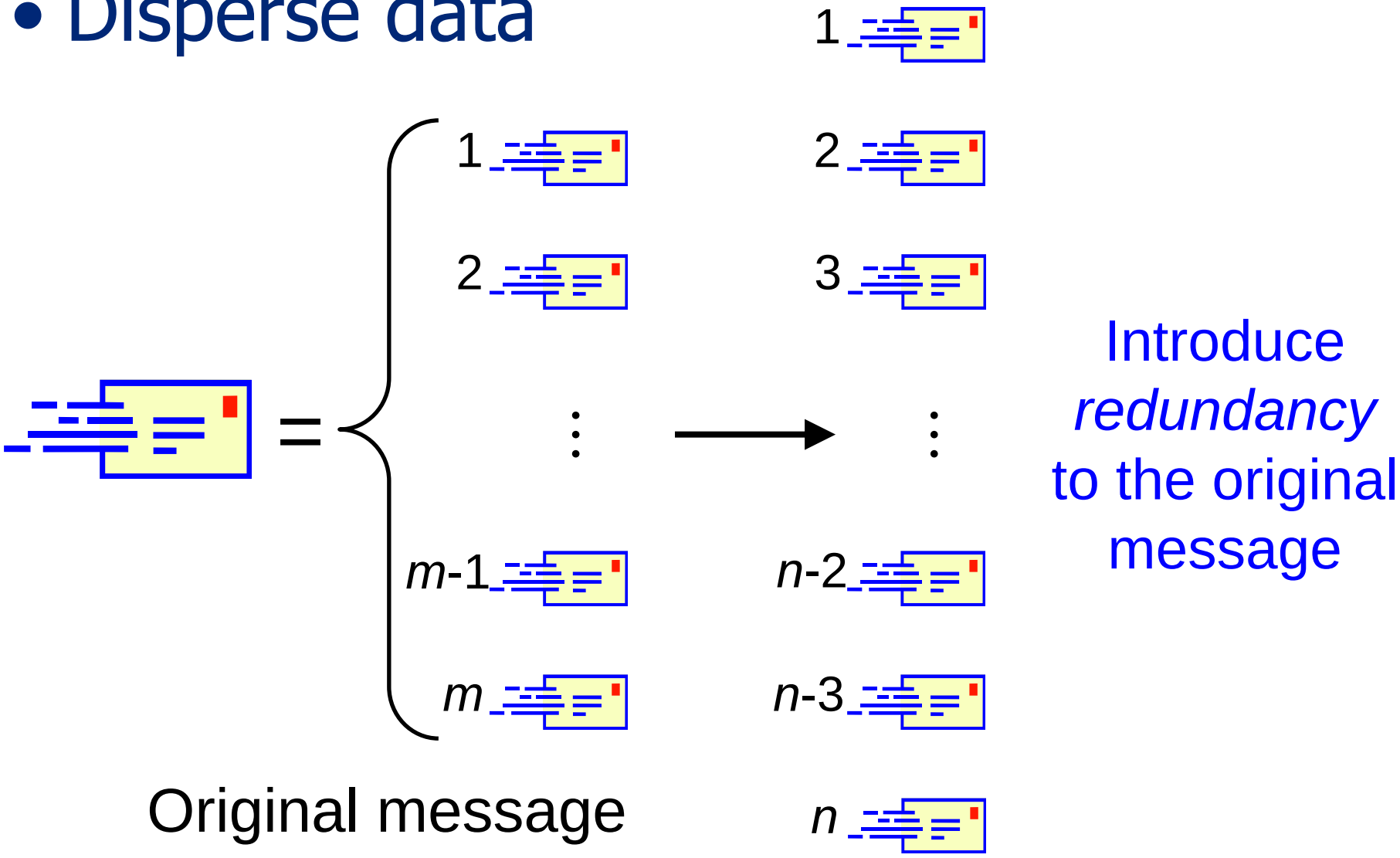
Securing Data Communication

- Use multiple routes



Securing Data Communication (cont'd)

- Disperse data

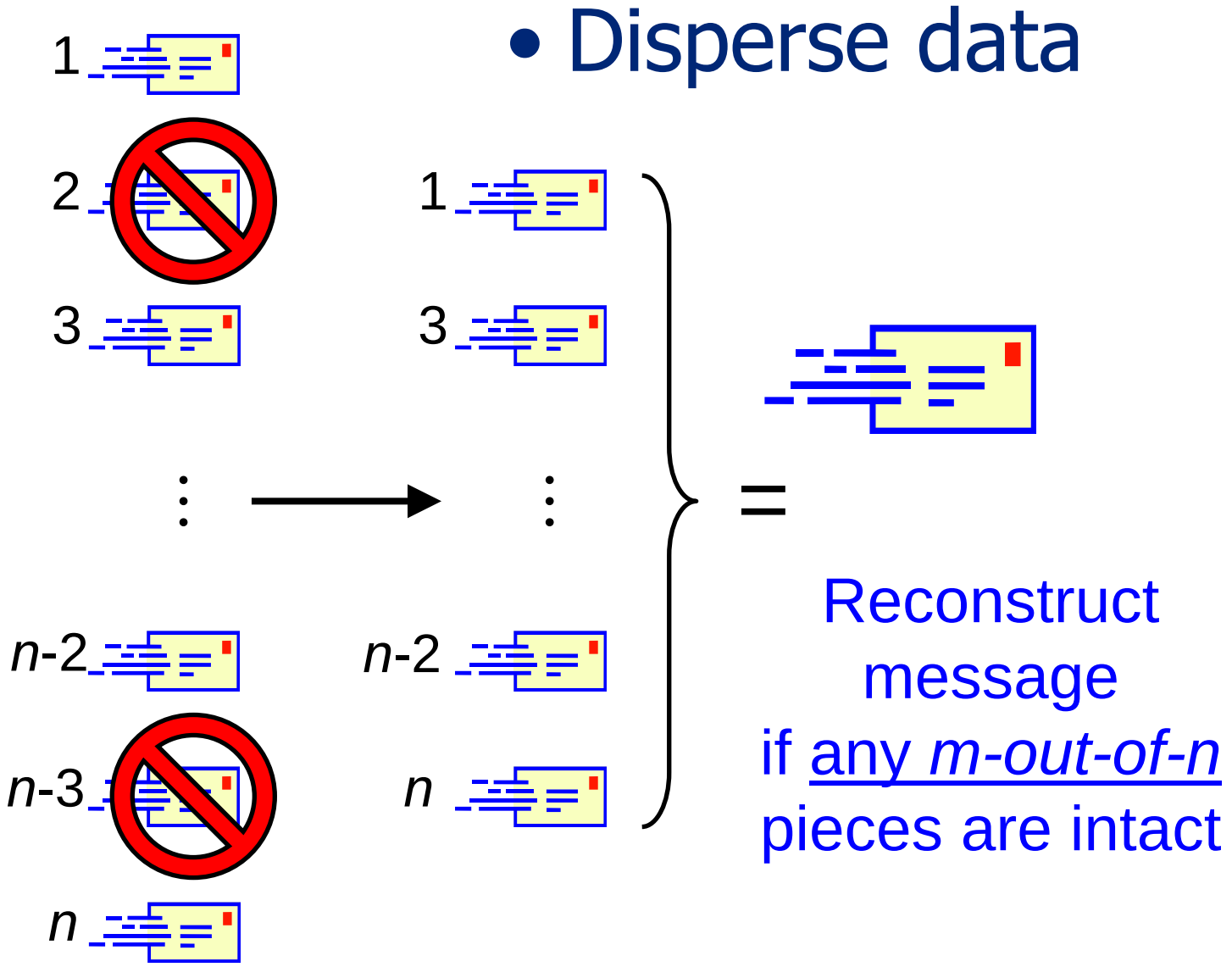


Original message

Introduce *redundancy* to the original message

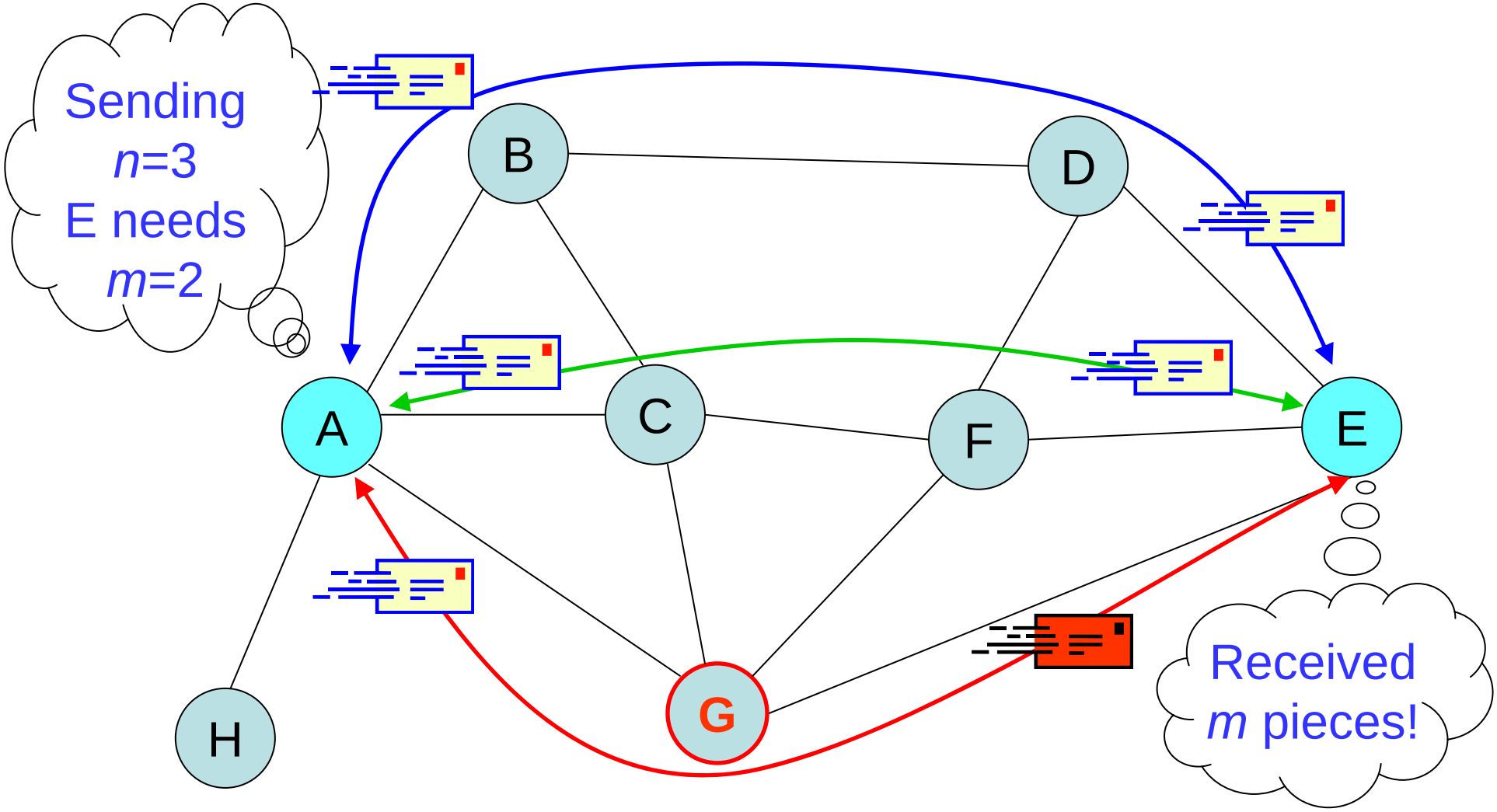
Securing Data Communication (cont'd)

- Disperse data



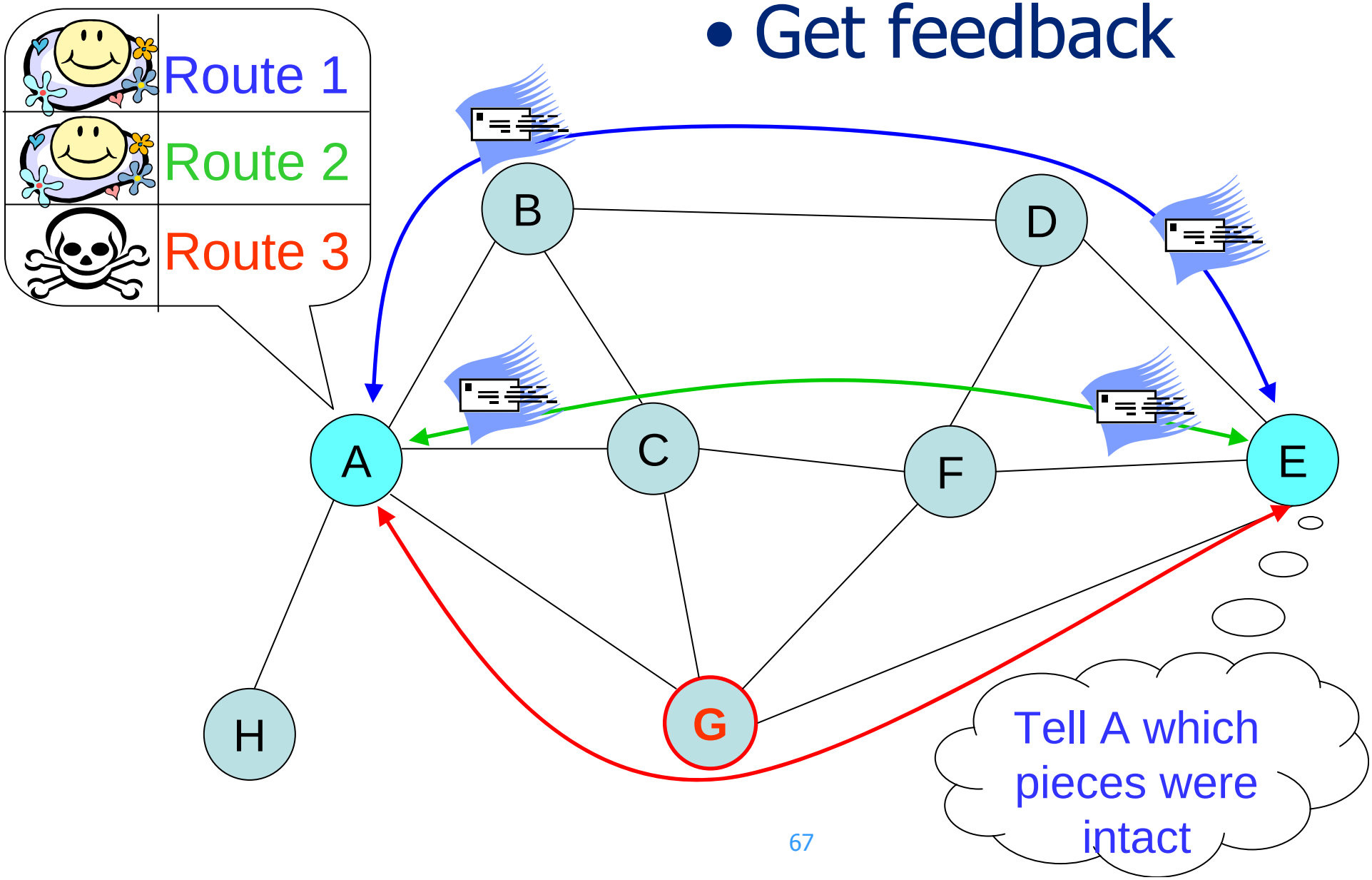
Securing Data Communication (cont'd)

- Transmit simultaneously across the routes



Securing Data Communication (cont'd)

- Get feedback



Securing Data Communication (cont'd)

- Secure Message Transmission (SMT) protocol
  - Dispersion of the transmitted data
  - Simultaneous usage of multiple node-disjoint routes
  - Data integrity and origin authentication
  - End-to-end secure and robust feedback
  - Adaptation to the network conditions
- Secure Single Path (SSP) protocol
  - Discovery and utilization of a single route
  - End–to–end security and feedback

P. P. and Z.J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks," IEEE JSAC, 2006

P. P. and Z.J. Haas, "Secure Message Transmission in Mobile Ad Hoc Networks," ACM WiSe, 2003

P. P. and Z.J. Haas, "Secure Message Transmission in Mobile Ad Hoc Networks," Ad Hoc Networks, 2003

Securing Data Communication (cont'd)

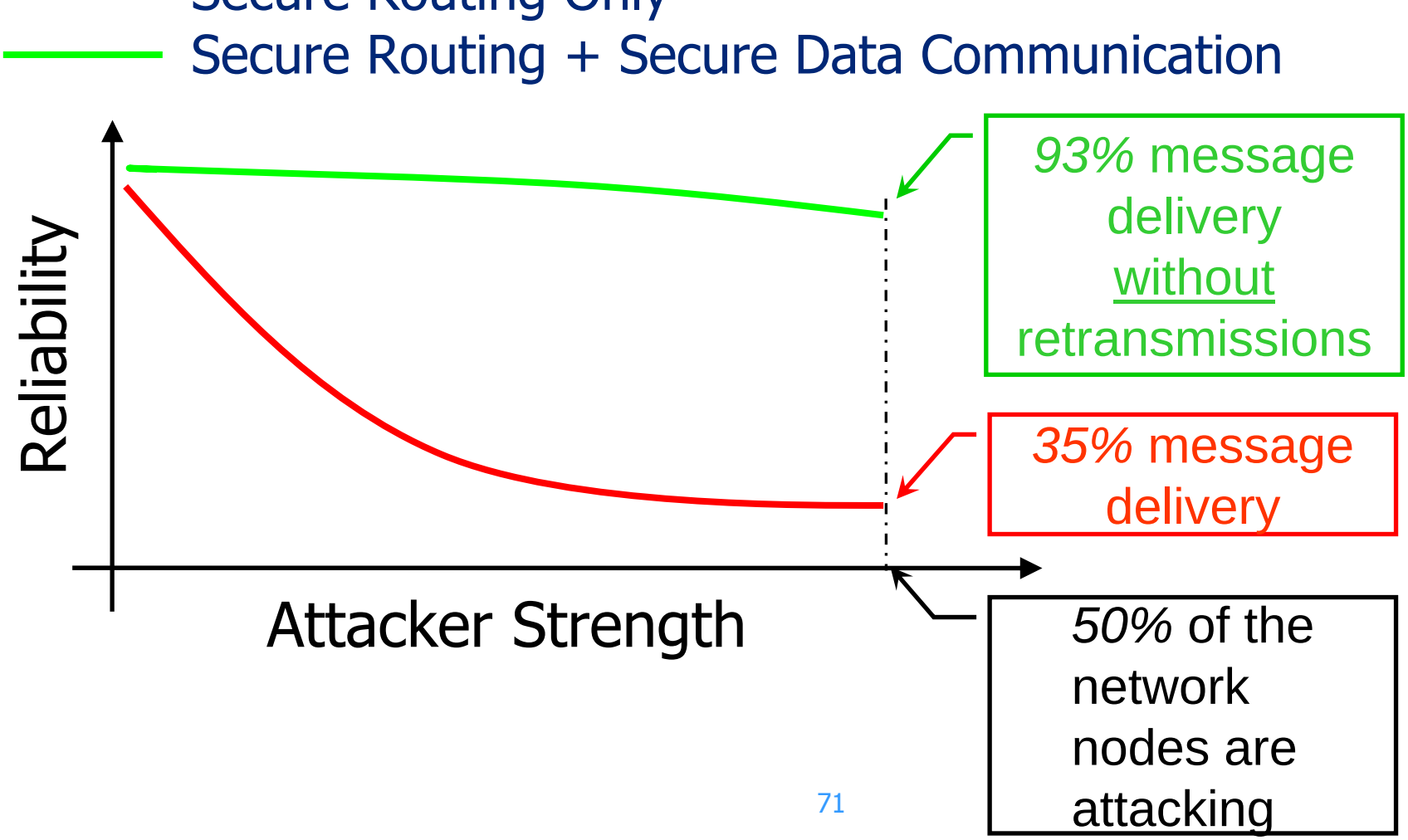
Nodes	50
Fraction of Adversaries	10%, 20%, 30%, 40%, or 50% of the network nodes
Measurements	50 randomly seeded runs for each point
Security Bindings	Single destination per source
Simulated time	300 sec
Mobility	Random waypoint; Pause times: 0, 20, 40, 60, 100, 150, 200, 250 seconds
Load	3, 7, 15, 20 CBR flows, Data payload: 512 Bytes Rates: 4, 10, 15, 20, 25, and 30 packets/sec
Coverage Area	1000m-by-1000m
PHY/MAC	IEEE 802.11, DCF, 2 and 5.5 Mbps, 300m
Transport	UDP / TCP
Tool	OPNET

Securing Data Communication (cont'd)

- Secure Message Transmission (SMT) protocol
- Secure Single Path (SSP) protocol
- Secure route discovery for both protocols
  - Explicit, basic
    - Reactive, Proactive
    - SRP, SLSP
- Attack pattern
  - Full compliance with the route discovery
  - Discard in–transit data packets

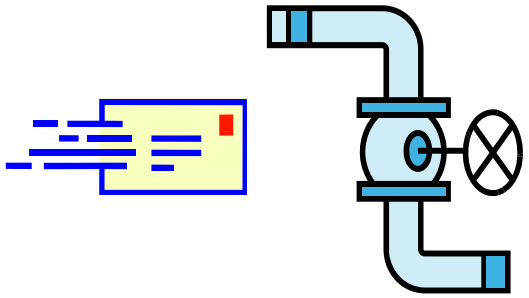
Securing Data Communication (cont'd)

- Reliable and Real-Time Communication in Hostile Environments

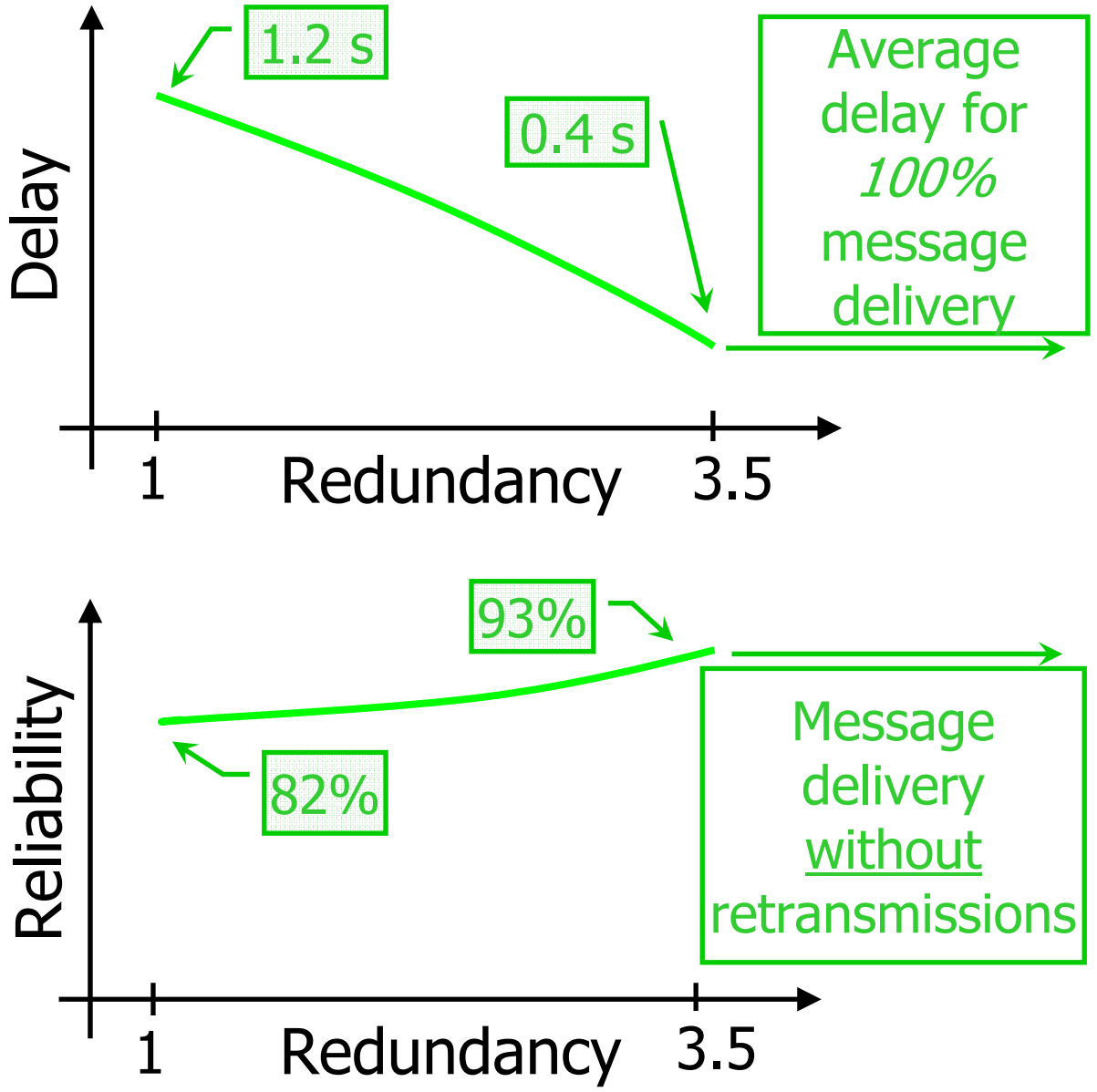


Securing Data Communication (cont'd)

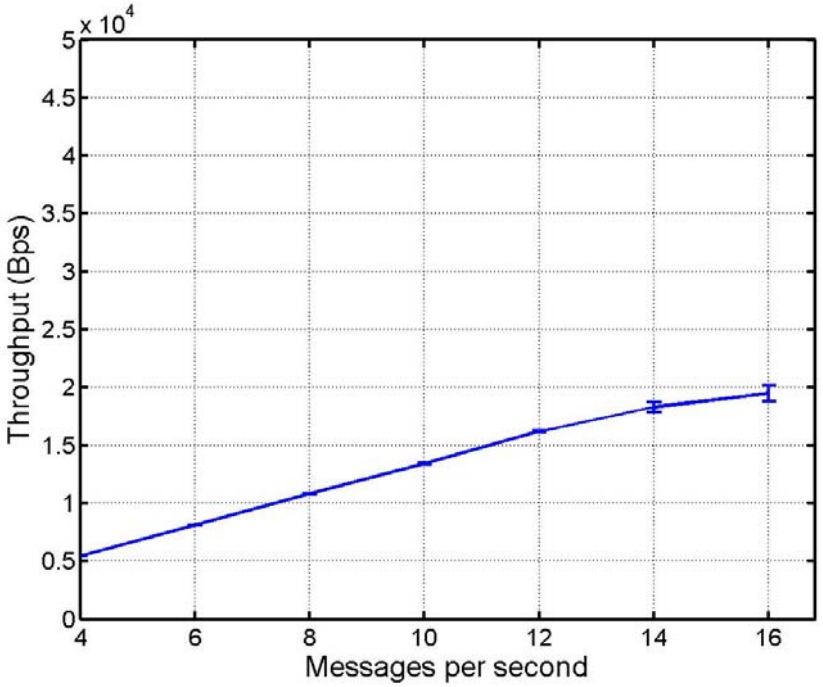
Bandwidth For Security



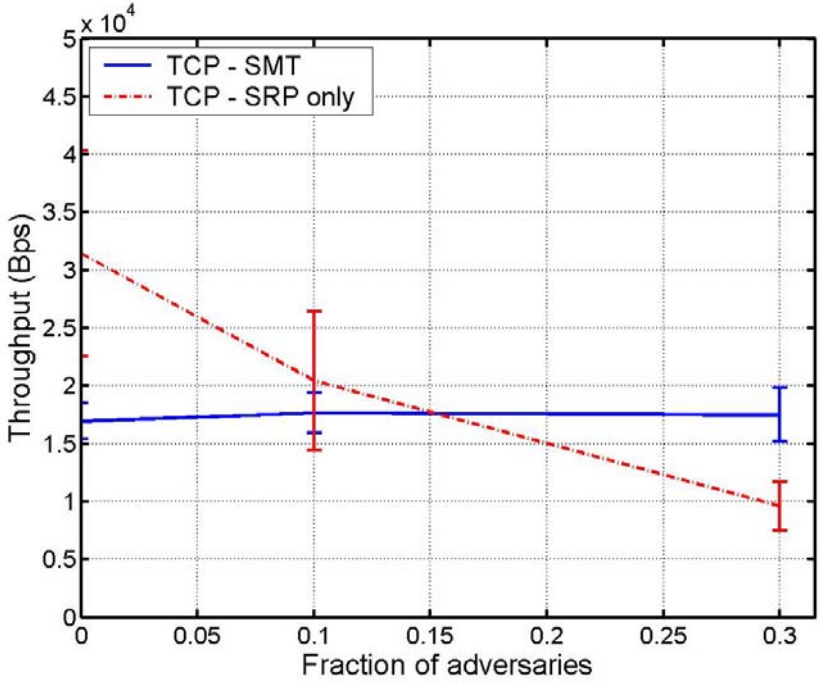
Redundancy



Performance Evaluation (cont'd)



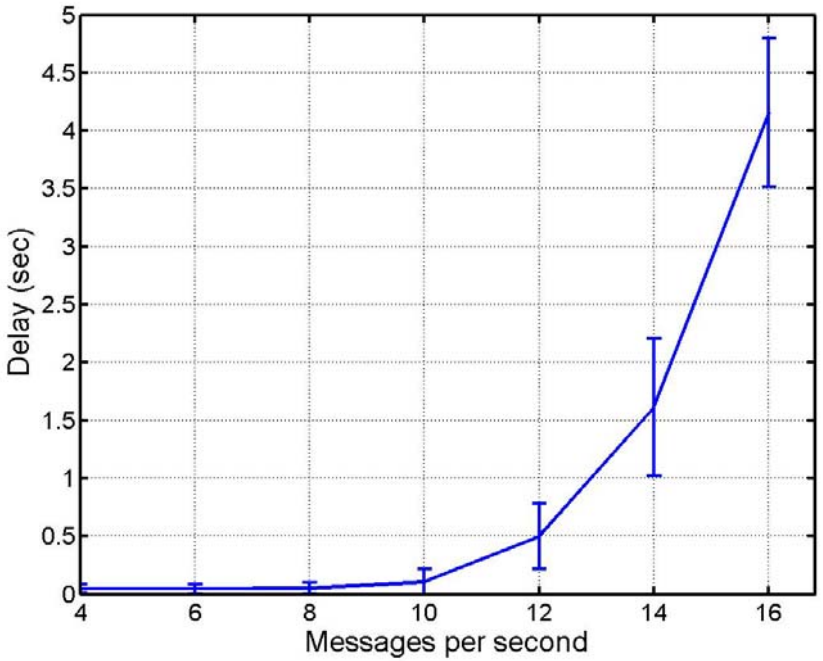
Throughput – no flow control



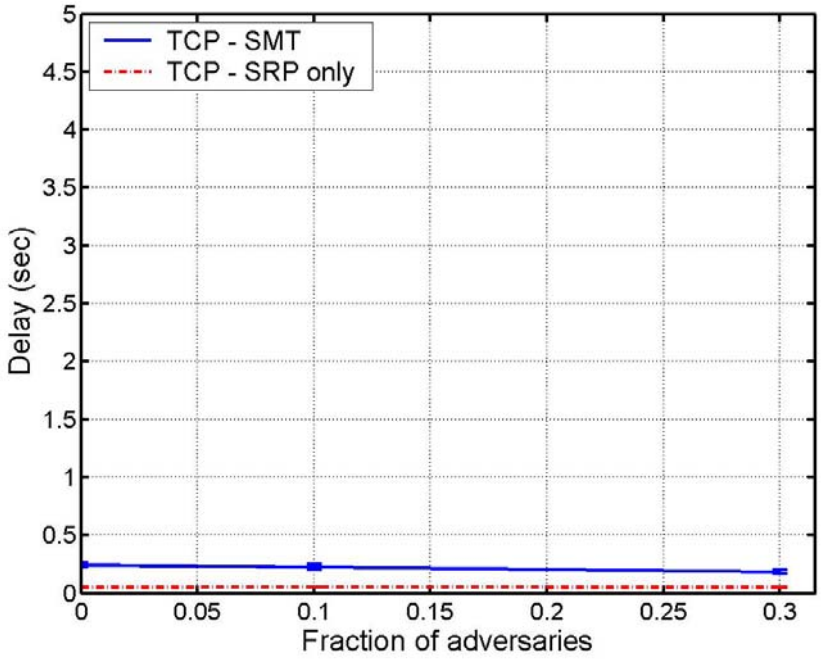
Throughput - SMT-RRD with TCP

Impact of Load and SMT-TCP interaction

Performance Evaluation (cont'd)



Message delay – no flow control



Message delay - SMT-RRD with TCP

Impact of Load and SMT-TCP interaction

Summary

- Secure data communication is critical
  - Secure routing protocols are vulnerable
  - As long as attackers can place themselves on utilized routes, they can degrade or deny communication
  - The only answer is to assess whether data are delivered, and avoid non-operational routes
- Secure data communication is practical
  - Low-delay, low-jitter, and highly reliable; essentially, real-time
  - Flexible
  - Low overhead
  - End-to-end
  - Effective against any data-dropping pattern

Additional Readings

- Secure Data Communication

  J.-P. Hubaux and **P. P.**, ACM MobiCom 2007 tutorial, slides

- CASTOR (Continuously Adapting Secure Topology-Oblivious Routing)
  - Integration route discovery and communication
  - Localized routing decisions
  - Outcome: Scalability and resilience

    W. Galuba, **P. P.**, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable Secure Routing for Ad hoc Networks," EPFL Technical Report, LSIR-REPORT-2009-002, 2009

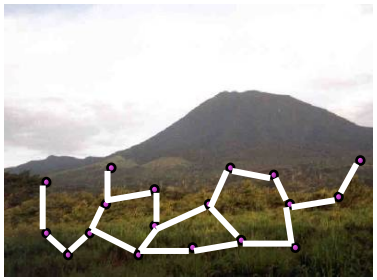
Secure Localization

© 2009 P. Papadimitratos

Localization

- Mobile computing is becoming increasingly location-based
  - Location-aware devices
  - Location-based services
- Two main problems
  - Determine own location
    - With the help of own equipment some infrastructure
  - Determine the location of another device
    - Could be as simple as asking a location-aware device to report its location
    - Often, some infrastructure performs the task

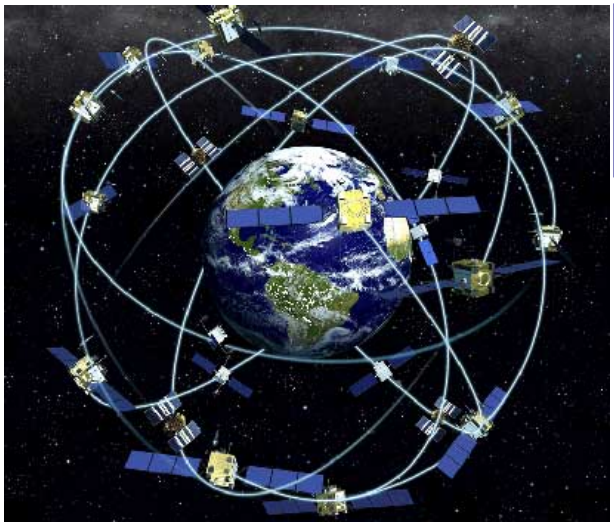
Localization (cont'd)







Sensing



Global Navigation Satellite Systems

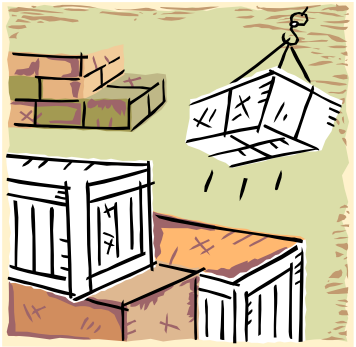




Navigation



Context awareness

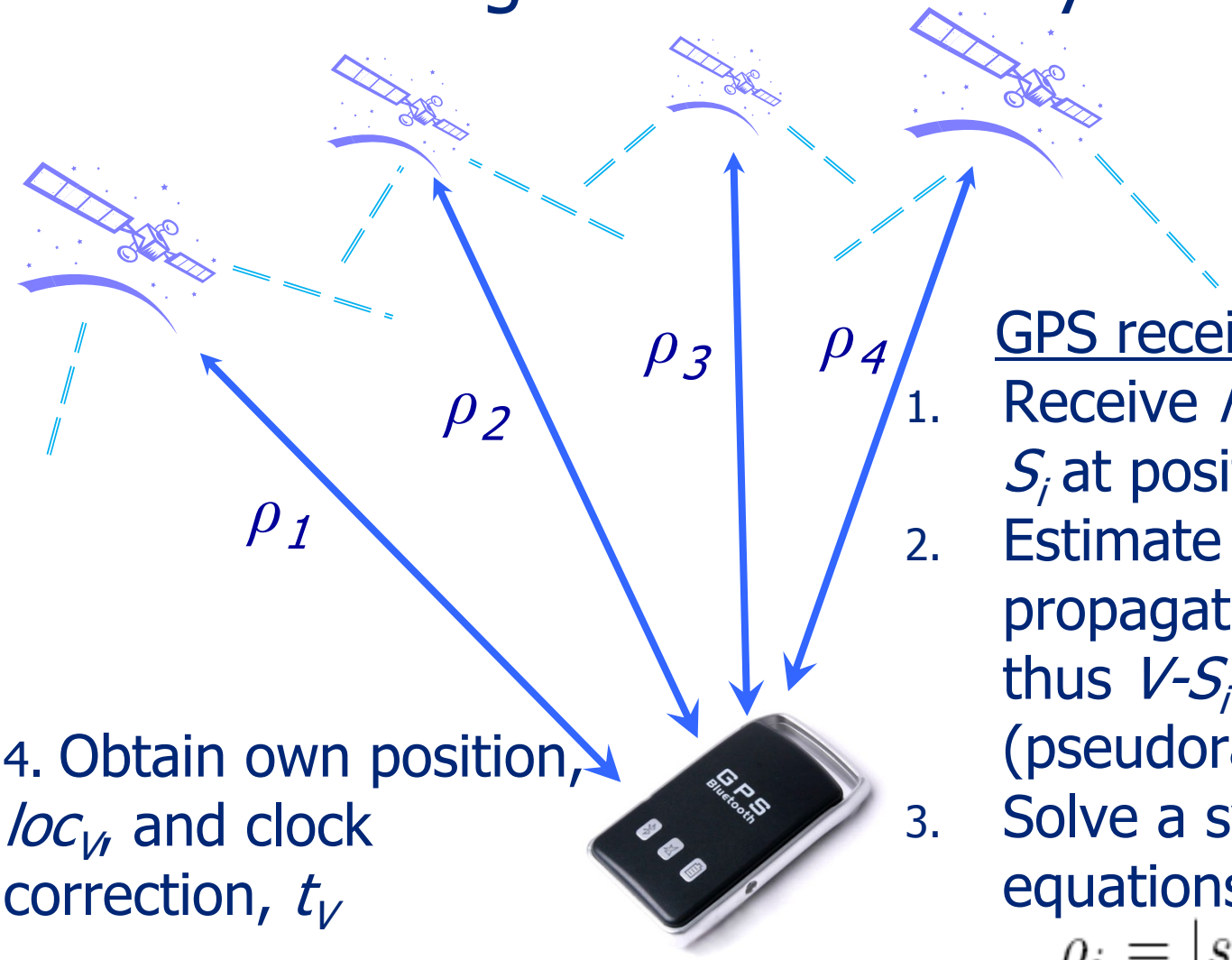


Fleet and cargo management

Graphics by Nokia

Localization (cont'd)

- Global Navigation Satellite Systems



GPS receiver, *V*

1. Receive NAV_i from satellite S_i at position s_i
2. Estimate the NAV_i propagation delays, and thus V-S_i distances (pseudoranges), ρ_i
3. Solve a system of equations:

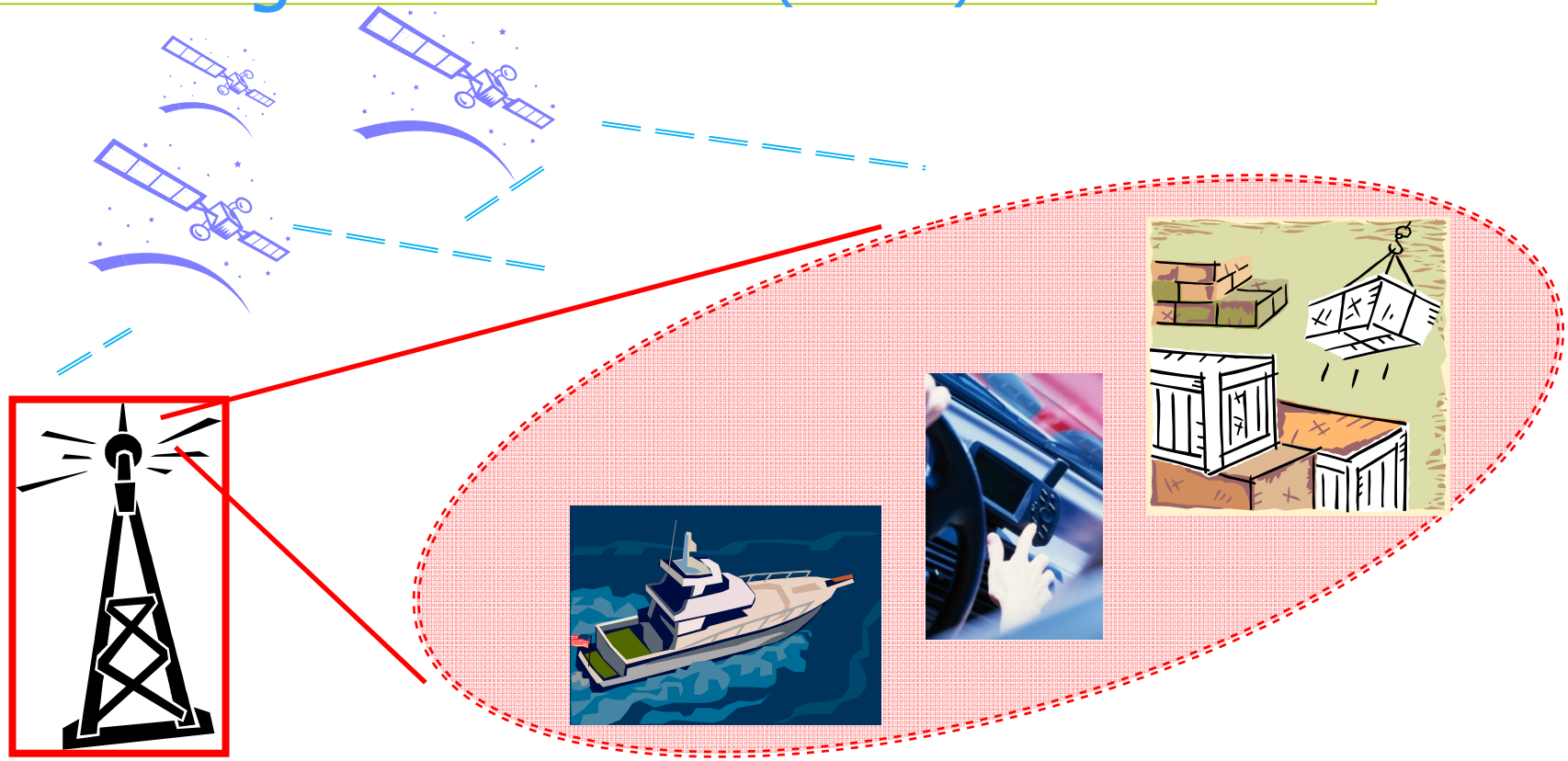
$$\rho_i = |s_i - loc_V| + c \cdot t_V$$

4. Obtain own position, loc_V, and clock correction, t_V

Attacking Localization

- (For this talk) Mislead devices, and their users, about their location
  - Compromise the device
    - Can be hard
  - Interfere with the wireless communication
    - Jam ➔ Outage
    - Overwrite legitimate transmissions with synthesized ones ➔ Control loc_V and t_V

Attacking Localization (cont'd)



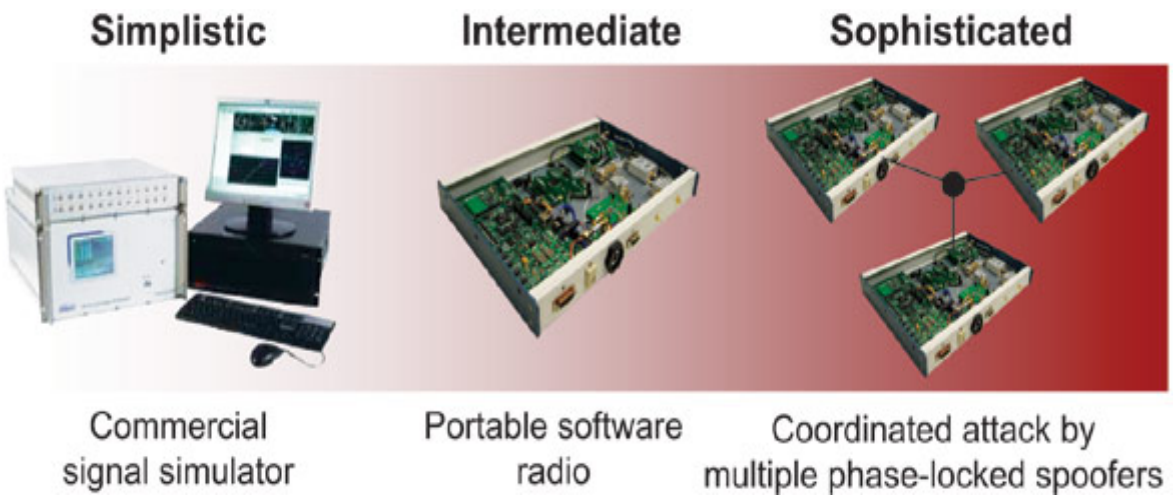
- *Attacker:* Record and replay, or forge, GPS signals, overwriting the legitimate GPS signals
- *System:* GPS receiver locks on spoofed signals
- *Consequence:* User is provided with a false, attacker-controlled location

Attacking Localization (cont'd)

- GPS Jammers and Simulators
- Meaconing (record and re-broadcast, a.k.a. replay)



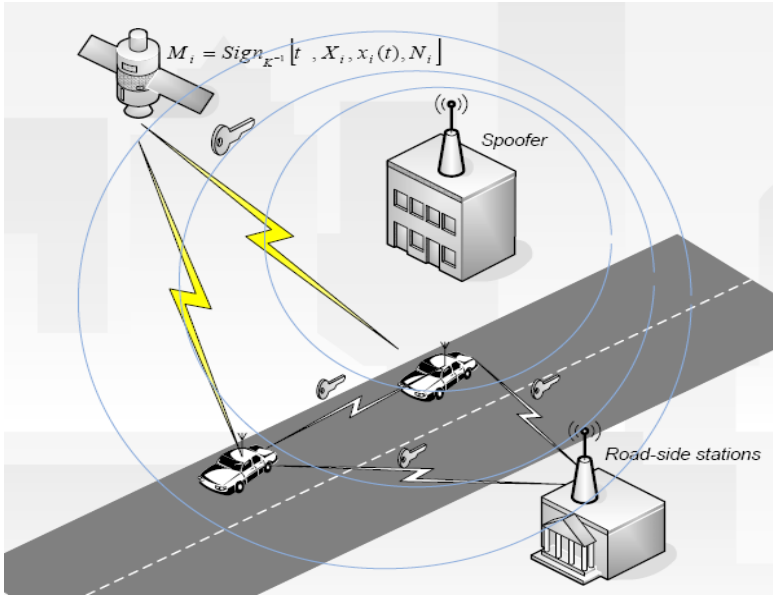
Low-power jammer (1 W); it can affect a 35km radius



T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," ION GNSS Conf., 2008

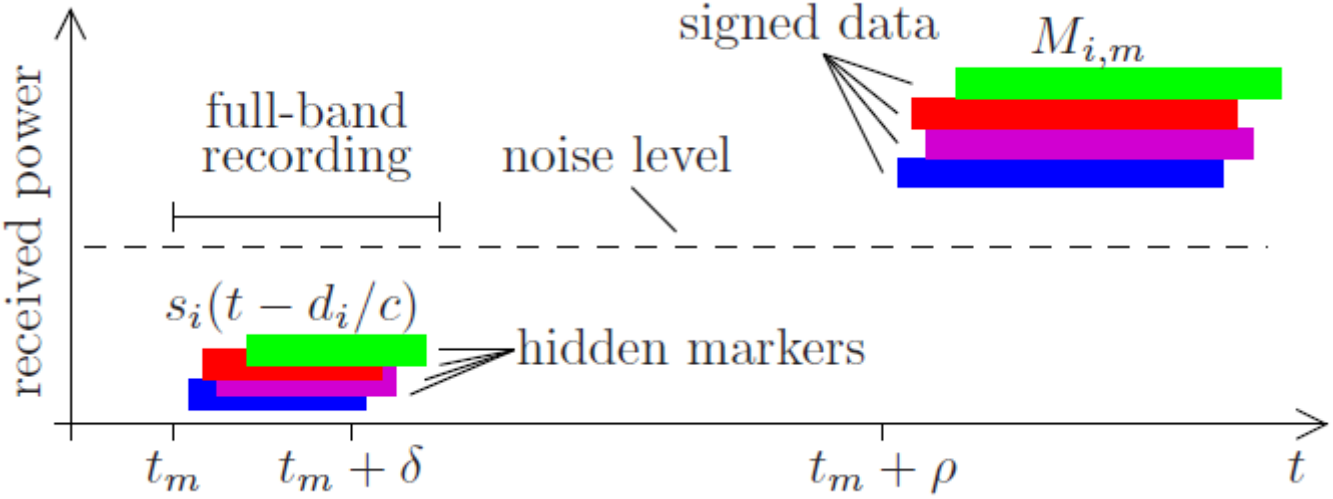
Securing Localization

- Authenticate navigation messages (NAV)
  - Public key crypto: one private-public key pair per satellite
  - Symmetric key authentication; single system key
    - Need tamper-resistant storage at receivers
  - Public key authentication delays can be significant
    - Low NAV transmission rate; ~ 40 sec for a signature
    - Caution: Need to maintain the relative NAV arrival timings



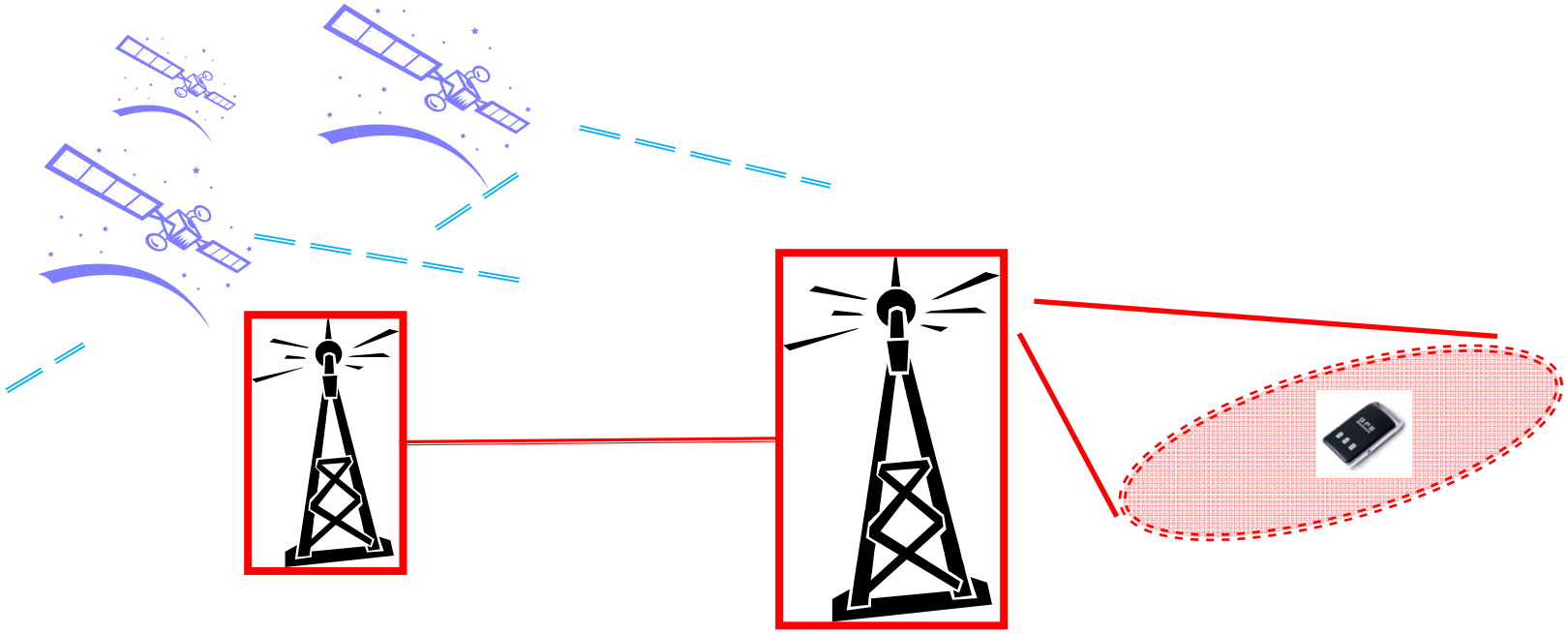
Securing Localization (cont'd)

- Public key authentication / "Hidden markers"
  - S_i transmit unpredictable sequences below noise; they release an authenticated spreading code with a delay ρ
  - V record the entire bandwidth and "detect" the hidden marker *a posteriori*, to calculate the NAV arrival times (thus the pseudo-ranges)



M. Kuhn, An Asymmetric Security Mechanism for Navigation Signals, 6th Information Hiding Workshop, 2004

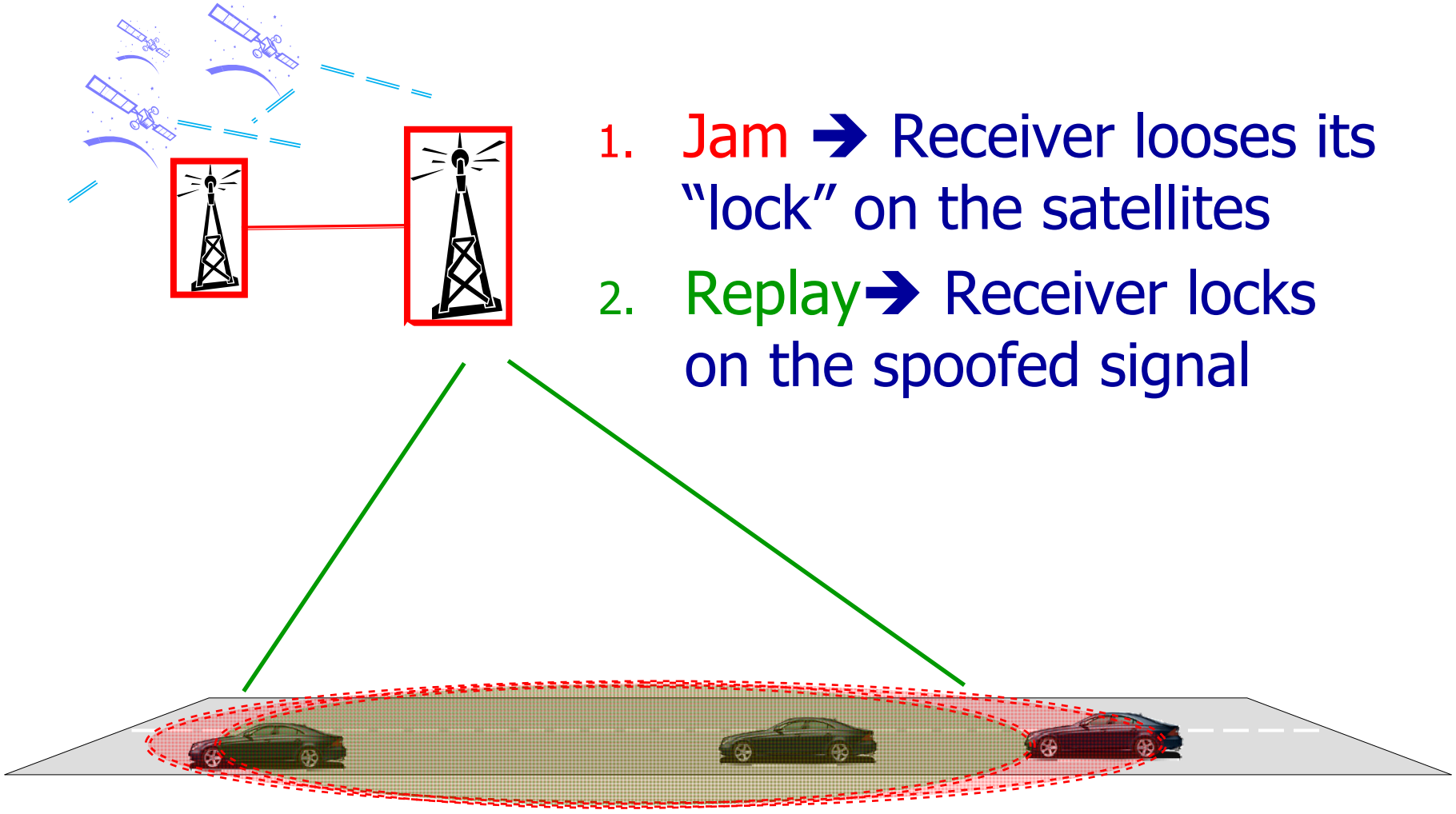
Attacking Localization (cont'd)



- Replay attacks can be effective even against future systems with authentication (e.g., Galileo)

P. P. and A. Jovanovic, "Protection and Fundamental Vulnerability of Global Navigation Satellite Systems (GNSS),"*IEEE IWSSC, Toulouse, France, October 2008*

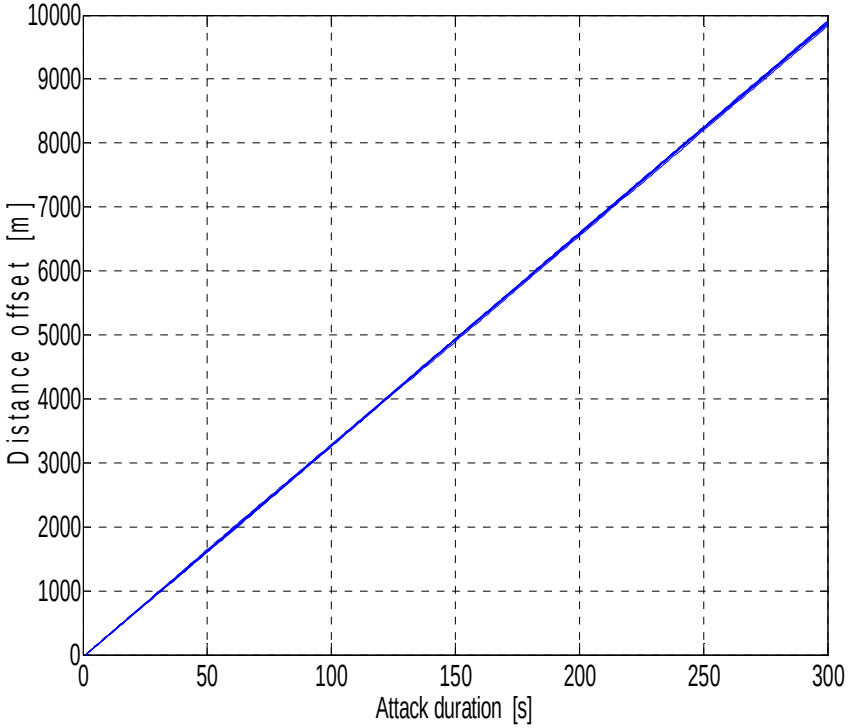
Attacking Localization (cont'd)

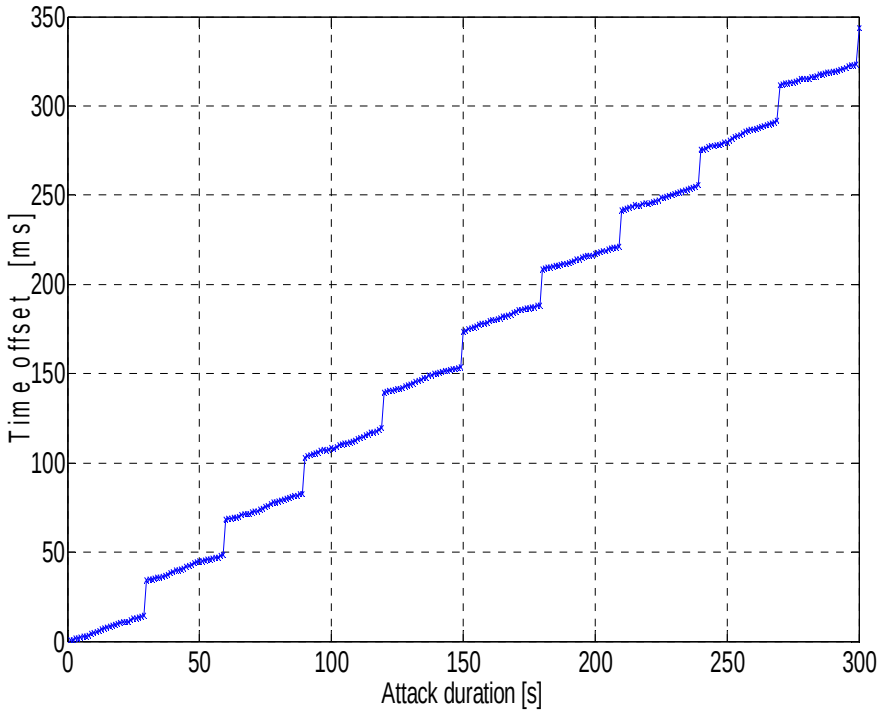


1. Jam → Receiver looses its "lock" on the satellites
2. Replay→ Receiver locks on the spoofed signal

- One ms of replay translates into ~300m of position error

Attacking Localization (cont'd)



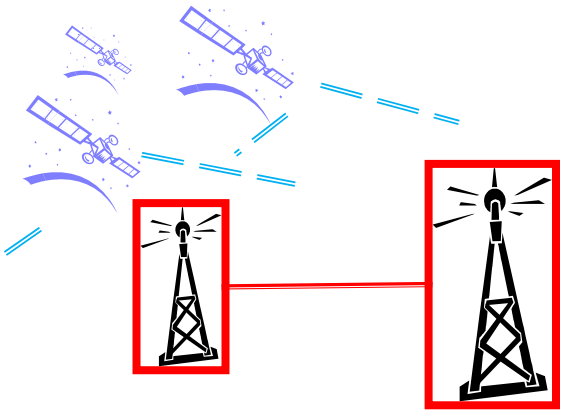


- Record NAV messages after the detection of the preamble at least the first bit
  - Minimum replay delay t_{min} =20ms
  - Replay after any $t_{min} + t_{replay}$

Securing Localization (cont'd)

- *Assumption*: the adversary covers part of the system: Receivers can operate in an unaffected area before entering an area under attack
- *Objective*: Receivers detect the attack onset
  - No additional complex equipment
  - No system reconfiguration
  - Resilience to sophisticated adversaries
- *Approach*: Rely on own (receiver) measurements
  - Predict future values from available ones that are deemed correct
  - Discrepancy between measurements and predicted values → Attack

Securing Localization (cont'd)



1. Normal mode:

   Collect [V_k, V_{k-1}, V_{k-2}, …, V_{k-W}]

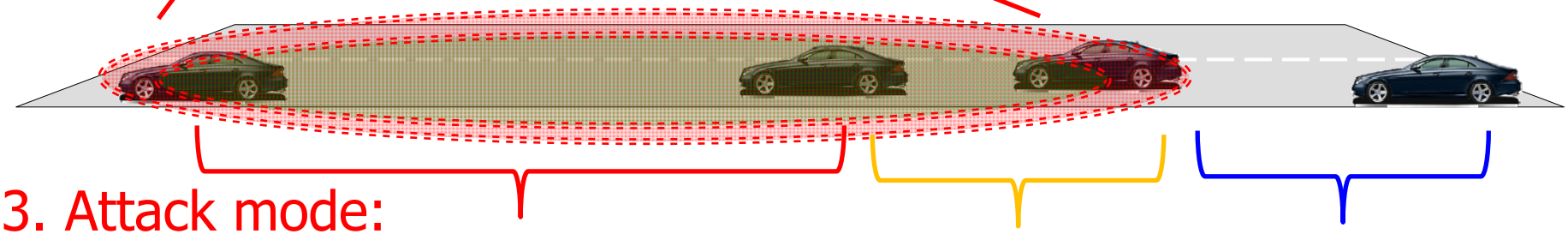
   Predict [PV_{k+p}, …, PV_{k+2}, PV_{k+1}]

   = f (V_k, V_{k-1}, V_{k-2}, …, V_{k-W})

2. Alert mode:

   Collect [V_{k+p}, …, V_{k+2}, V_{k+1}] and

   Compare with [PV_{k+p}, …, PV_{k+2}, PV_{k+1}]



3. Attack mode:

If $|g([V_{k+j}]) - h([PV_{k+i}])| > \varepsilon$, detect attack

Alert mode

Normal mode

Securing Localization (cont'd)

- Inertial sensors
  - *Location Inertial Test*
- Accurate and stable clocks
  - *Clock Offset Test*
- Doppler shift
  - *Doppler Shift Test*

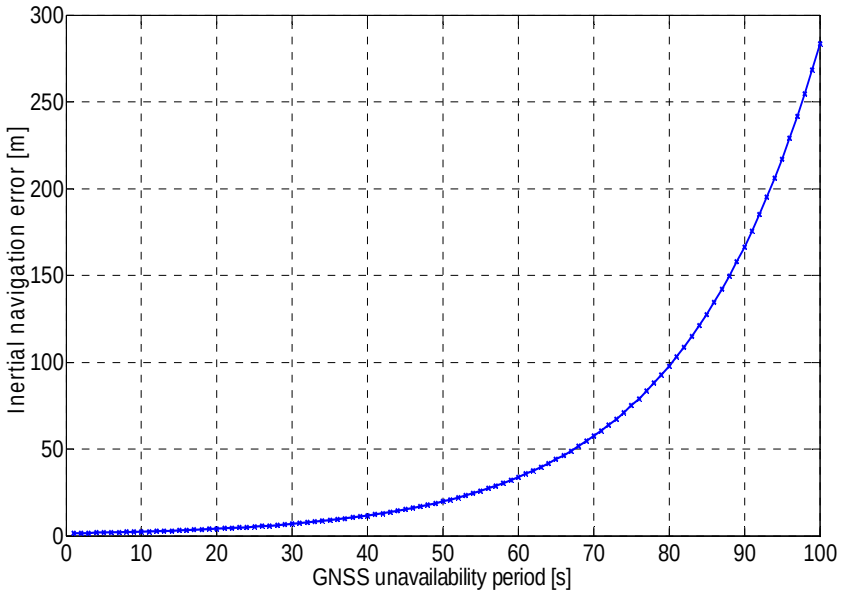
P. P. and A. Jovanovic, "GNSS positioning: Attacks and Countermeasures," IEEE MILCOM, San Diego, CA, USA, November 2008

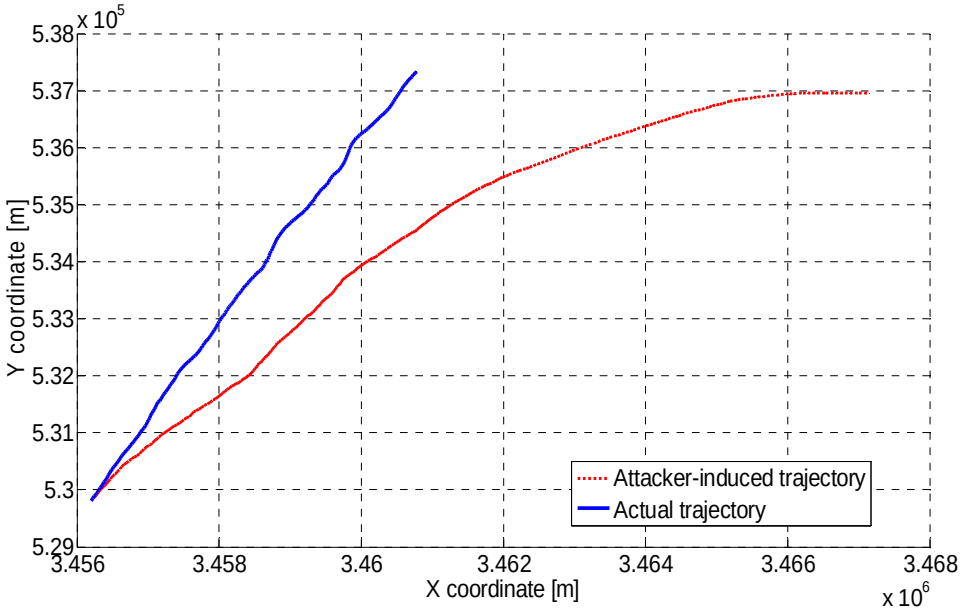
Securing Localization (cont'd)

- Setup
  - Observation and navigation data; RINEX format
  - GPS functionality implemented in Matlab
  - Receiver movement over 300s
  - Adversary
    - Static
    - Mobile with velocities less than 250 km/h
    - Without or with control over the transmission frequency
    - Multiple radios

Securing Localization (cont'd)

- Location Inertial Test

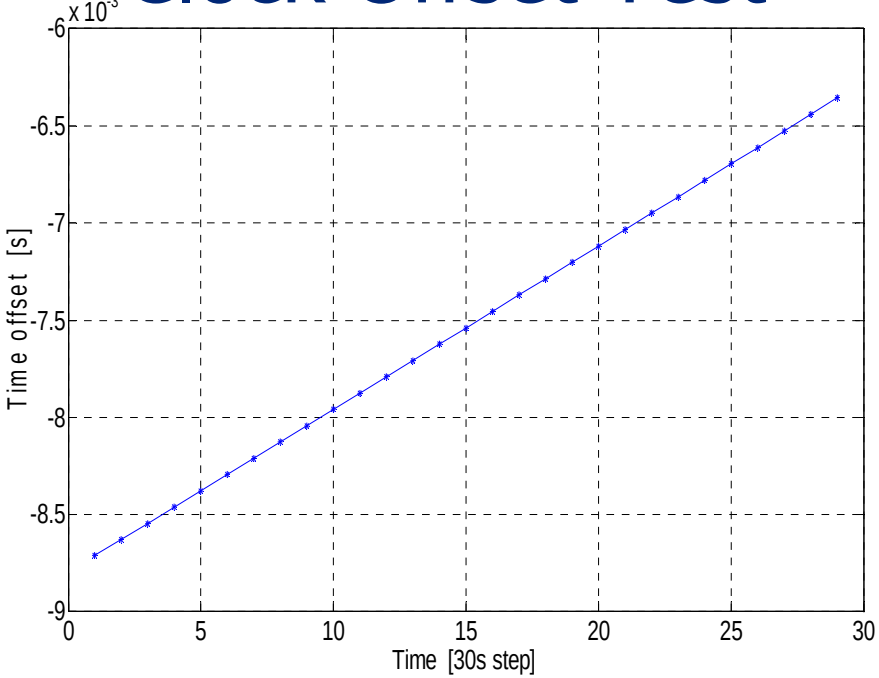


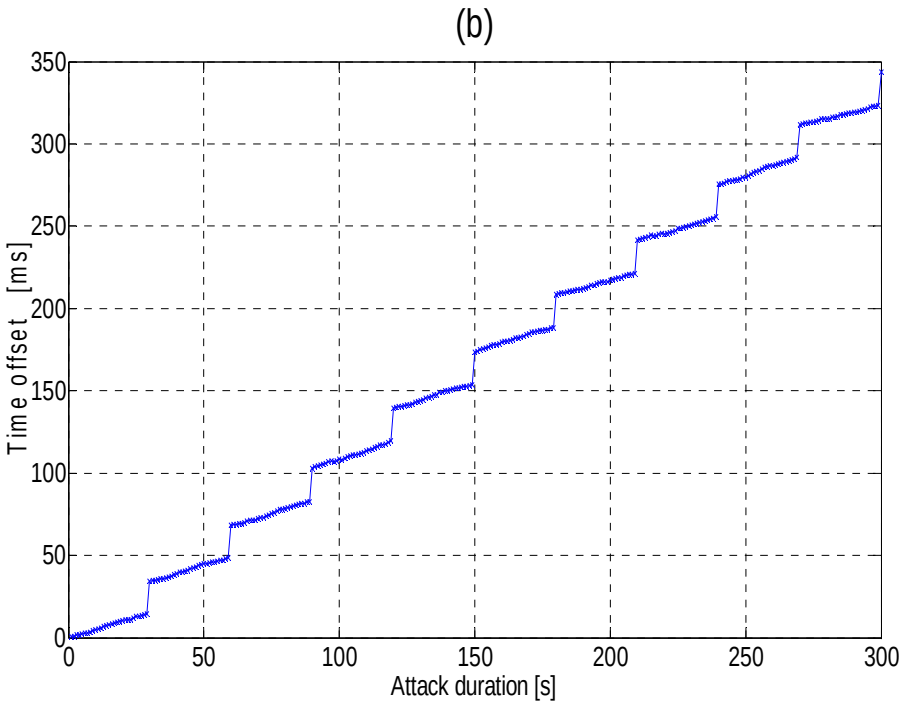


- Fast increasing inaccuracy of the inertial measurement unit
  - To succeed with replay attack: Jam for < 1 min

Securing Localization (cont'd)

- Clock Offset Test

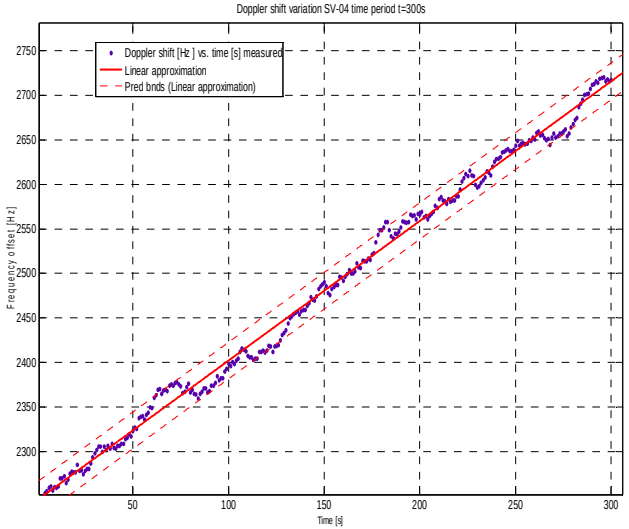


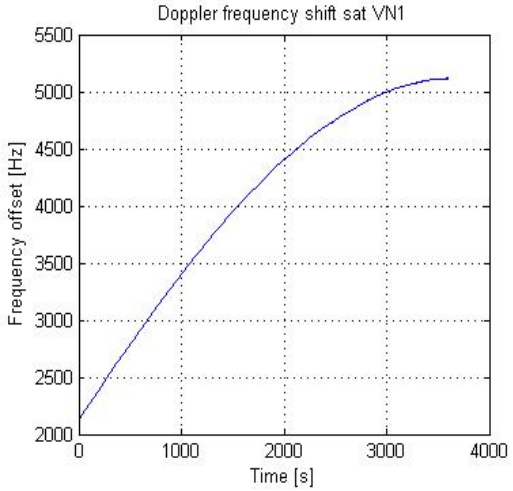


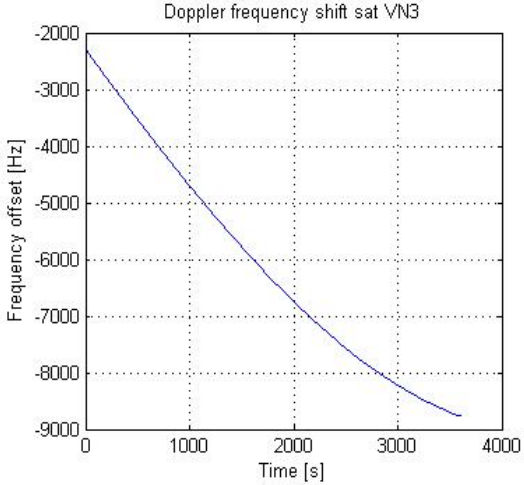
- Commodity receivers: clocks drift fast (see left figure)
  - To succeed with replay attack: Jam for 2 min, to make t_V ~20-30 ms acceptable
- Improve clock; e.g., micro-second accuracy for 6 min
  - To succeed with replay attack: Jam for hours

Securing Localization (cont'd)

- Doppler Shift Test



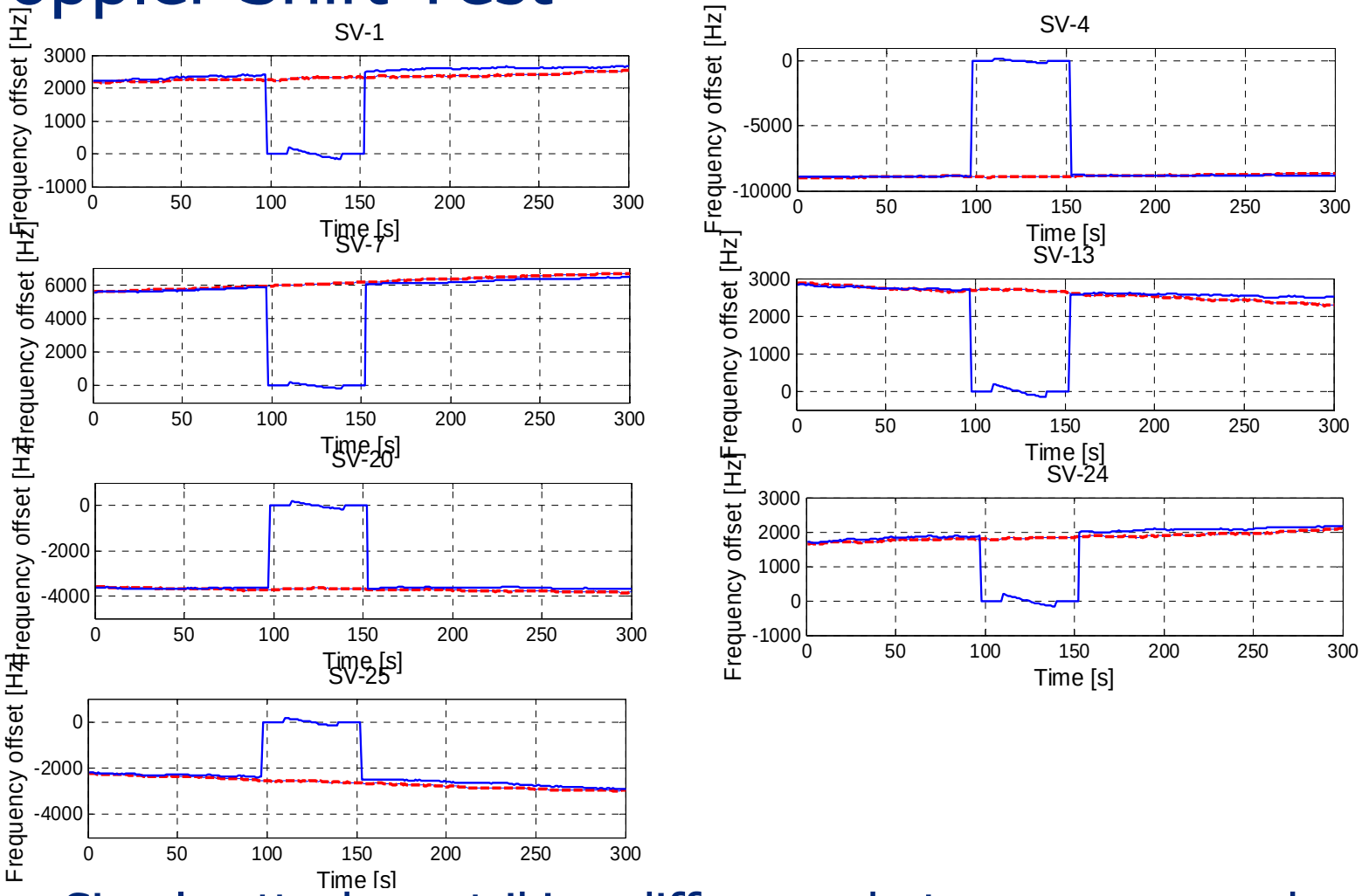




- Doppler Shift (DS) at the receiver depends primarily on the relative velocity of transmitter and receiver
  - Satellite velocity, ~ 3km/s, dominant; Smooth DS changes
  - Easy to detect a simple attacker
  - Sophisticated attackers need to predict the mobility of the receiver, thus predict the DS, and adjust their transmission frequency accordingly

Securing Localization (cont'd)

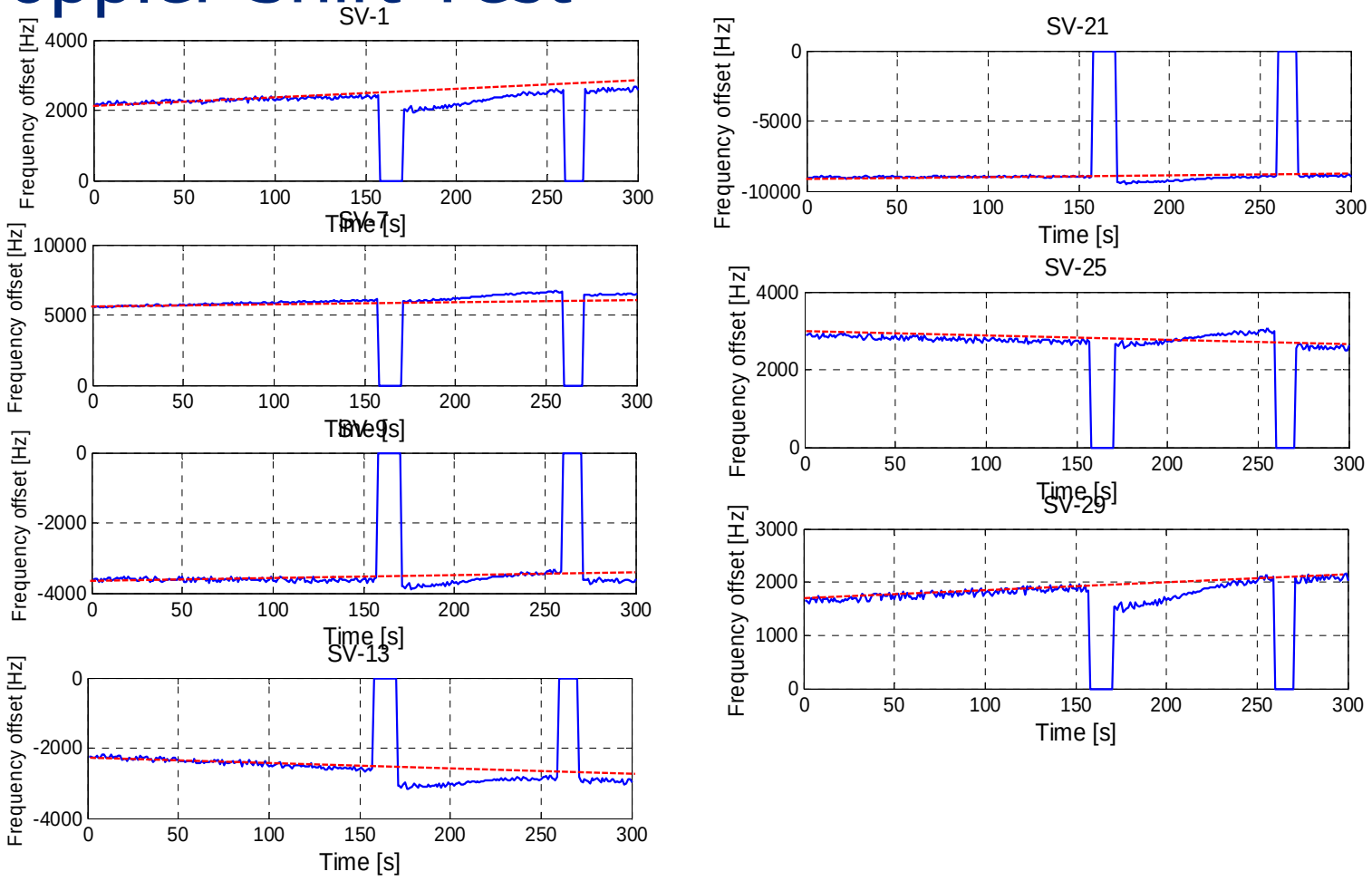
- Doppler Shift Test



  - Simple attacker: striking difference between measured and expected DS

Securing Localization (cont'd)

- Doppler Shift Test



  - Sophisticated attacker: some uncertainty about the receiver's mobility; detectable DS differences ~ 300 Hz

Summary

- Vulnerability of GNSS: Long known issue, could become a major problem
- Upcoming systems are to enhance availability (against unintentional interference) and offer security features
- Attacks at the physical layer (e.g., replay attacks) are possible even when cryptographic protection is available
- Simple non-cryptographic solutions can be very effective and raise the bar even for sophisticated adversaries

Additional Readings

J.A. Volpe, "Vulnerability Assessment of the Transportation Infrastructure Relying on GPS," NTSC, NAVCEN draft report, 2001

L. Scott, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Signals," ION-GNNS, Portland, Oregon, 2003

B. O'Hanlon, B. Ledvina, M.L. Psiaki, P.M. Kintner Jr., T. E. Humphreys, "Assessing the GPS Spoofing Threat," GPS World, January 2009 (*)

T.K. Adams, "GPS Vulnerabilities," Military Review, 2001

(*) Source for graphic on slide 83

Summer School on Network and Information Security 2009

Wireless System Security

Panos Papadimitratos

panos.papadimitratos@epfl.ch

http://people.epfl.ch/panos.papadimitratos

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE