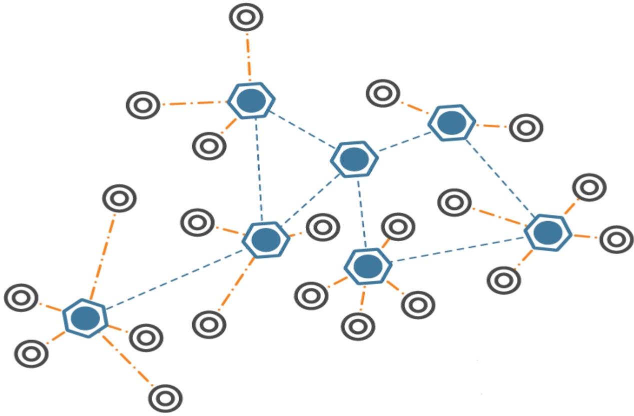
The Third IEEE International Symposium on Trust, Security and Privacy for Emerging Applications (TSP-10)

An Authentication Framework for Wireless Sensor Networks using Identity-based Signatures

Rehana Yasmin
R.Yasmin@cs.bham.ac.uk

Co-authors: Dr Guilin Wang, Dr Eike Ritter
University of Birmingham

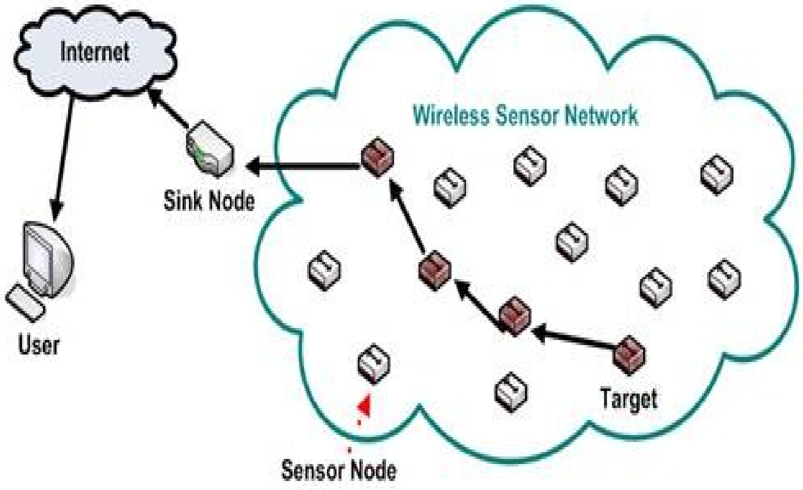


Outline of the Presentation

- Introduction
- Challenges
- Existing Approaches in WSN
- Problem Definition
- Proposed Authentication Framework
- Comparison with Existing Schemes
- Conclusion & Future Work

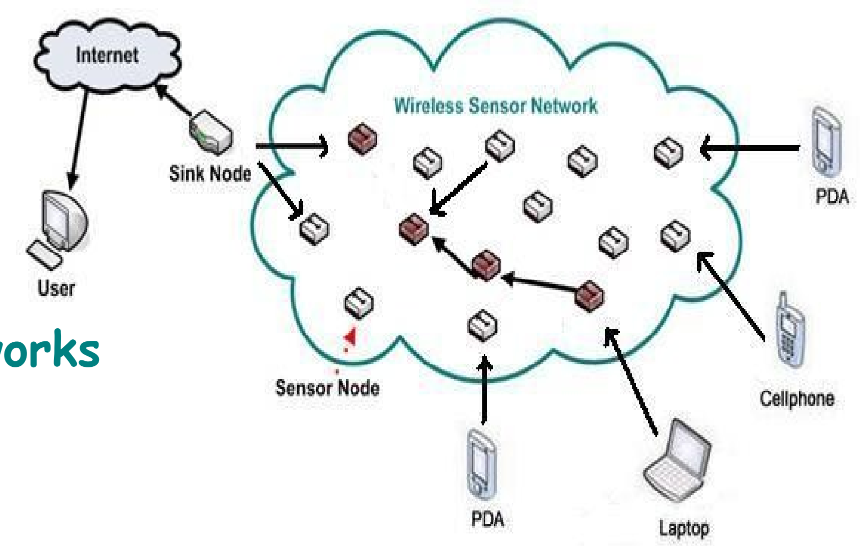
Introduction: Wireless Sensor Networks

- Composed of small low cost resource constrained sensor nodes (motes)
- Monitor and report certain phenomenon
- Adversary can inject false data packets, modify original data packets
- Adversary can also compromise sensor nodes



Introduction: Authentication

- Countermeasure: **Authentication**
  - ❖ Verify claimed message sender
  - ❖ Contents of a message



Authentication in Wireless Sensor Networks

- Base station to sensor nodes
- Sensor node to other sensor nodes
- Outside user to sensor nodes
  - ❖ Session key establishment
  - ❖ Access control enforcement

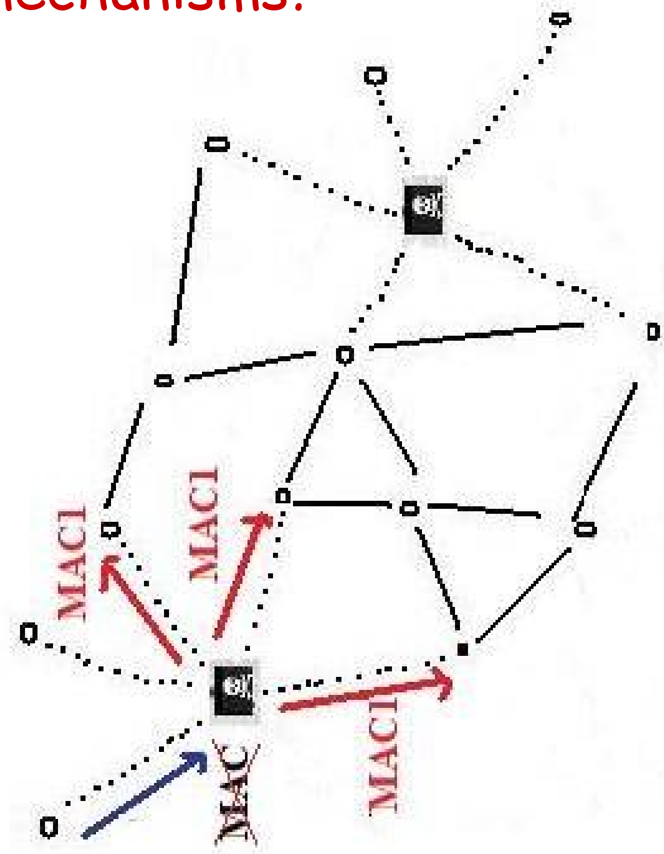
Challenges

Why not use conventional authentication mechanisms?

- Sensor nodes are resource constrained devices
  - Low processing capability
  - Low battery power
  - Low storage
  - Low bandwidth

- Hurdle in applying strong cryptographic based authentication schemes e.g., digital signatures

- Compromised sensor nodes do not allow Message Authentication Code



Existing Approaches: μ-TESLA

[Perrig 2002, Liu 2004 & 2005, Drissi 2006, Gu 2007]

Issues with μ-TESLA based Schemes

- Base station to other sensor nodes authentication
- Sensor node broadcasts through base station only
- Not suitable for real time applications
- Delayed authentication
- Denial of Service (DoS) attack
- Multiple senders broadcast turn by turn during predefined time intervals
- Support only limited number of broadcast senders

Existing Approaches: Digital Signature

[Ren 2007, Cao 2008]

Issues with Digital Signature based Schemes

- Public key and certificate management
    - ❖ Send public key and certificate with every message
        - ❑ Low bandwidth
        - ❑ Two signature verifications per message
    - ❖ Store public key of each sender
        - ❑ Storage overhead
        - ❑ Reduces scalability
    - ❖ User authentication also suffer from the same problem
- Message signing expensive in terms of time and energy consumption

Problem Definition

- Authentication mechanism which provides
  - Broadcast or multicast without the involvement of base station
  - Quick broadcast of real time messages
  - Authentication of messages
  - Authentication of any outside user
- Public key and/or certificates management

Proposed Authentication Framework

- An authentication framework which utilizes

  - ❖ Identity-based signatures

    AND

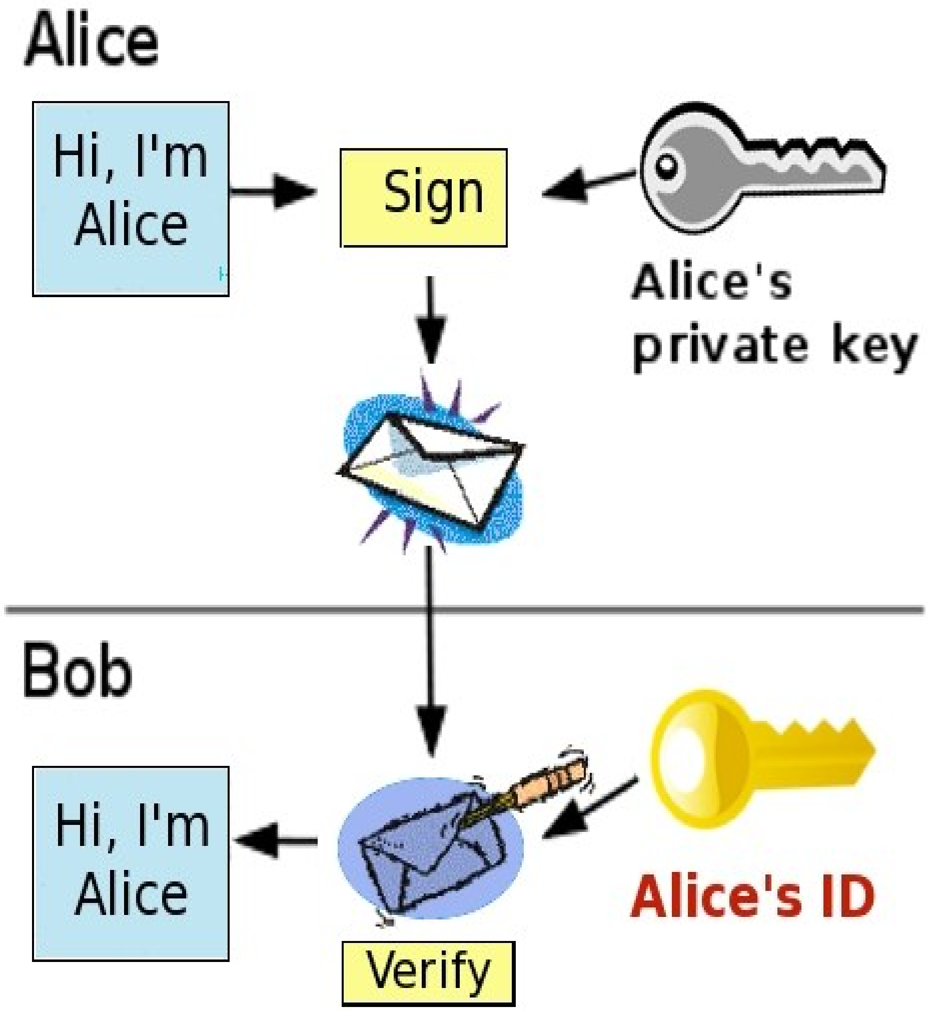
  - ❖ Online/Offline signature schemes

Proposed Authentication Framework

Identity-based Signatures

[Shamir84, …]

- User can use his identity information as his public key
- Corresponding private key generated by a private key generator (PKG)
- Eliminates the need of a certificate



Proposed Authentication Framework

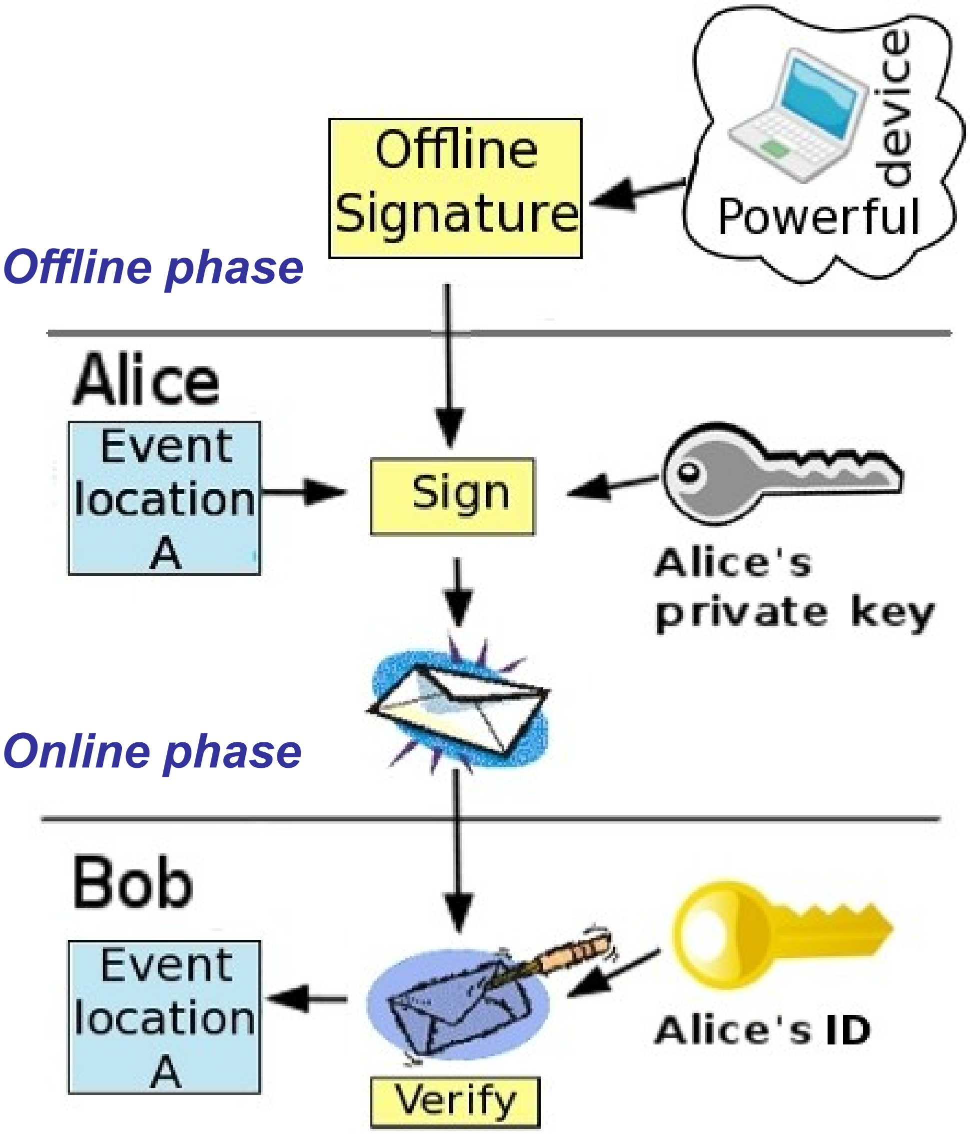
Online/Offline Signatures

[Even 1989, …]

- Message signing is divided into two phases:
  - *Offline* phase
  - *Online* phase

- Offline phase performed by a resourceful device

- Suitable for resource constrained signer



Proposed Authentication Framework

The proposed authentication framework

- Comprised of two authentication schemes
  - ❖ Sensor Broadcast Authentication
  - ❖ Outside User Authentication
- Utilizes
  - ❖ ID-based online/offline signature (IBOOS) for sensor broadcast authentication

AND

  - ❖ ID-based signature (IBS) for outside user authentication

Sensor Broadcast Authentication Scheme

- Base station, a resourceful and trustworthy entity, plays the role of PKG
- First two phases are performed before the deployment

1. System Initialization

- Base station computes:
  - msk SK_{PKG}, mpk PK_{PKG}, system parameters SP

2. Key Generation

- Base station computes:
  - private keys D_{ID} corresponding to user ID
- ID, D_{ID}, PK_{PKG} and SP are stored on sensor nodes before deployment

Sensor Broadcast Authentication Scheme

3. *Message Broadcast*
   - Offline phase: performed on base station (before hand)

     $$S \leftarrow \mathit{OffSign}\,(D_{ID}, SP)$$

   - Online phase: performed on sensor node

     $$s \leftarrow \mathit{OnSign}\,(m, S, TS)$$

4. *Authentication*
   - On receiving a message, sensor node
     - ❖ Verifies time stamp *TS*
     - ❖ Verifies signature using signer's ID and system parameters

       $$0/1 \leftarrow \mathit{Ver}\,(m, ID, s, SP)$$

Outside User Authentication Scheme

- Base station, a resourceful and trustworthy entity, plays the role of PKG

1. *System Initialization*

   Same as in first scheme

2. *Key Generation*

   Same as in first scheme

3. *User Registration*
   - Performed every time when a new user is registered with the system
   - Base station computes:
     - private key D_{ID} corresponding to user ID
   - User U receives ID_U, D_{ID_U}, PK_{PKG} and SP from base station through a secure channel

Outside User Authentication Scheme

4. *User Request*

- User U signs his request and sends to sensor node N

$$U \rightarrow N: \{RM, TS, ID_U, \sigma\}, \text{ where}$$

$$\sigma \leftarrow \mathit{Sign}((RM, TS, ID_U), D_{ID_U})$$

5. *User Authentication*

- On receiving a user request, sensor node
  - ❖ Verifies time stamp TS
  - ❖ Verifies signature using user's ID and system parameters

$$0/1 \leftarrow \mathit{Ver}(m, ID_U, \sigma, SP)$$

Outside User Authentication Scheme

6. *Session Key Establishment*

- We propose to use ID-based one-pass session key establishment protocol
- During authentication phase, user also sends his ephemeral key E_U
- After successful user authentication, sensor node computes session key using E_U
- The only message exchanged is signed by the user, verified by the sensor node
- Designed our own new ID-based one-pass key establishment protocol

Comparison with Existing Schemes

Schemes	Signature Schemes	Energy Cost (Offline) mW	Energy Cost (Online) mW	Computation Time (Online) s	Storage Overhead
Existing Broadcast Authentication Schemes					
CAS [Ren2007]	ECDSA	0	26.96	0.89	-
DAS [Ren2007]	ECDSA	0	26.96	0.89	22N = 1.2MB
IDS [Ren2007]	Pairing based	0	87.09	3.47	-
IMBAS [Cao2008]	BNN	0	72.90	2.43	-
Proposed Sensor Broadcast Authentication Scheme					
Proposed	IBOOS [Ren2008]	φ*	5.62	0.19	-
Proposed	IBOOS [Xu2005]	48.60	ε*	ε*	-

N = 50,000, φ* shows the cost of underlying signature scheme and ε* shows negligible cost

Comparison with Existing Schemes

Schemes	Signature Schemes	Energy Cost (mW)	Verification Time (s)	Storage Overhead (Bytes)	Session Key
Existing User Authentication Schemes					
RRUASN [Benenson2004]	ECDSA	106.84	3.54	0	No
DP^{2}AC [Zhang2009]	RSA	14.05 + TE	0.47 + TT	10*T	No
Proposed User Authentication Scheme					
Proposed	IBS [Cao2008]	72.90	2.43	0	Yes

TE = Transmission Energy

TT = Transmission Time

T = Used Tokens

Importance of Work and Advantages

- First attempt to handle the problem of authenticated broadcast by sensor nodes
- First application of online/offline signature to wireless sensor networks

- Primary advantages of the proposed authentication framework:
  - Reusability
  - Efficiency
  - Public keys and certificates management
  - Scalability

Conclusion & Future Work

- Proposed authentication framework
  - ❖ Efficient in terms of computation time and energy consumption
  - ❖ Solves the problem of public keys and certificates
  - ❖ Provides scalability

- In future,
  - ❖ Implementation on real sensor nodes
  - ❖ Access control

References

1. Z. Benenson, "Realizing robust user authentication in sensor networks," in Proc. REALWSN '05, 2005.
2. X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks," Computer Communications, vol. 31, no. 4, pp. 659 - 667, 2008.
3. J. Drissi and Q. Gu, "Localized broadcast authentication in large sensor networks," in Proc. ICNS '06. IEEE, p. 25.
4. S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line digital signatures," in Proc. Advances in Cryptology CRYPTO '89, LNCS, vol. 435. Springer Berlin, 1990, pp. 263–275.
5. D. Liu and P. Ning, "Multilevel mTESLA: Broadcast authentication for distributed sensor networks," ACM Trans. Embed. Comput. Syst., vol. 3, no. 4, pp. 800–836, 2004.
6. D. Liu, P. Ning, S. Zhu, and S. Jajodia, "Practical broadcast authentication in sensor networks," in Proc. MobiQuitous '05:Networking and Services. IEEE Computer Society, pp. 118–132.
7. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.
8. K. Ren,W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 6, no. 11, pp. 4136–4144, Nov. 2007.
9. K. Ren, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," in IEEE SECON '07, pp. 223–232.
10. Q. Ren, Y. Mu, and W. Susilo, "Mitigating phishing with ID-based online/offline authentication," in Proc. Australasian conference on Information Security, AISC '08, pp. 59–64.
11. A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO '84 on Advances in cryptology, LNCS. NY,USA: Springer-Verlag, 1985, pp. 47–53.
12. S. Xu, Y. Mu, and W. Susilo, "Efficient authentication scheme for routing in mobile ad hoc networks," in Proc. EUC '05 Workshops, LNCS, vol. 3823. Springer, 2005, pp. 854–863.
13. R. Zhang, Y. Zhang, and K. Ren, "DP2AC: Distributed privacy preservingaccess control in sensor networks," in Proc. IEEE INFOCOM '09. IEEE, 2009, pp. 1251–1259.

Existing Approaches

μ-TESLA [Perrig 2002]

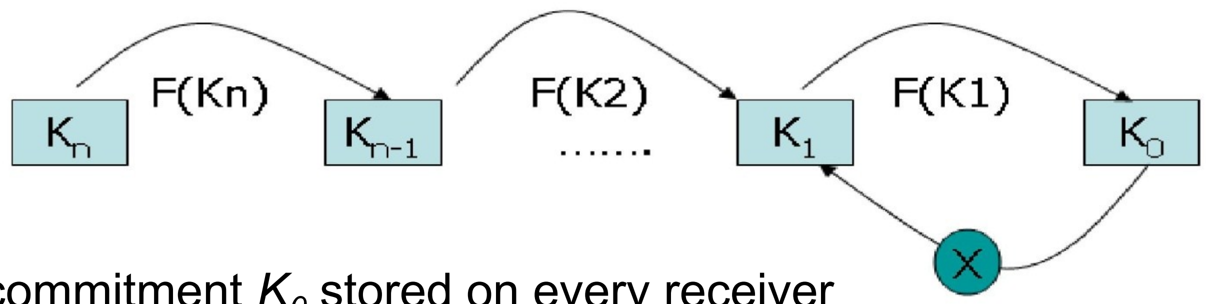
- Micro Timed Efficient Stream Loss-tolerant Authentication
- Message Authentication Code (MAC)
- Symmetric cryptography introduces asymmetry
- Base station to sensor nodes broadcast authentication

Existing Approaches

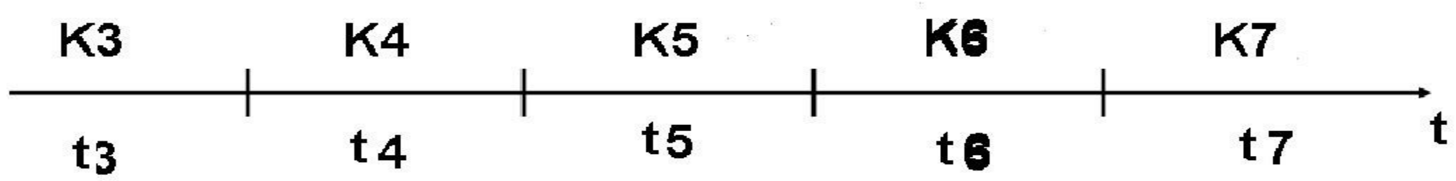
μ-TESLA (continued)

Sender Setup

- One-way hash key chain



- Key commitment K_0 stored on every receiver
- Time divided into n equal parts
- Each key from key chain assigned to one time slot



Existing Approaches

μ-TESLA (continued)

Broadcasting Authenticated Packets

- In time interval i, the sender uses key K_i to compute MAC
- Same MAC key for all packets in that interval
- In time interval $(i + \delta)$, the sender reveals key K_i
- δ depends on round trip time between the sender and the receivers

Existing Approaches

µ-TESLA (continued)

Authenticating Broadcast Packets

- ➢ Sender and receivers need to be loosely time synchronized
- ➢ Receivers need to know the key disclosure schedule
- ➢ A packet verification involves three steps
  - ❖ First, to see if packet is safe
  - ❖ Second, to verify the received MAC key
  - ❖ Third, to verify MAC using verified MAC key