Security for Ad Hoc Networks

Hang Zhao

Ad Hoc Networks

- Ad hoc -- a Latin phrase which means "for this [purpose]".
- An autonomous system of mobile hosts connected by wireless links, often called *Mobile Ad hoc NETworks* (MANETs)

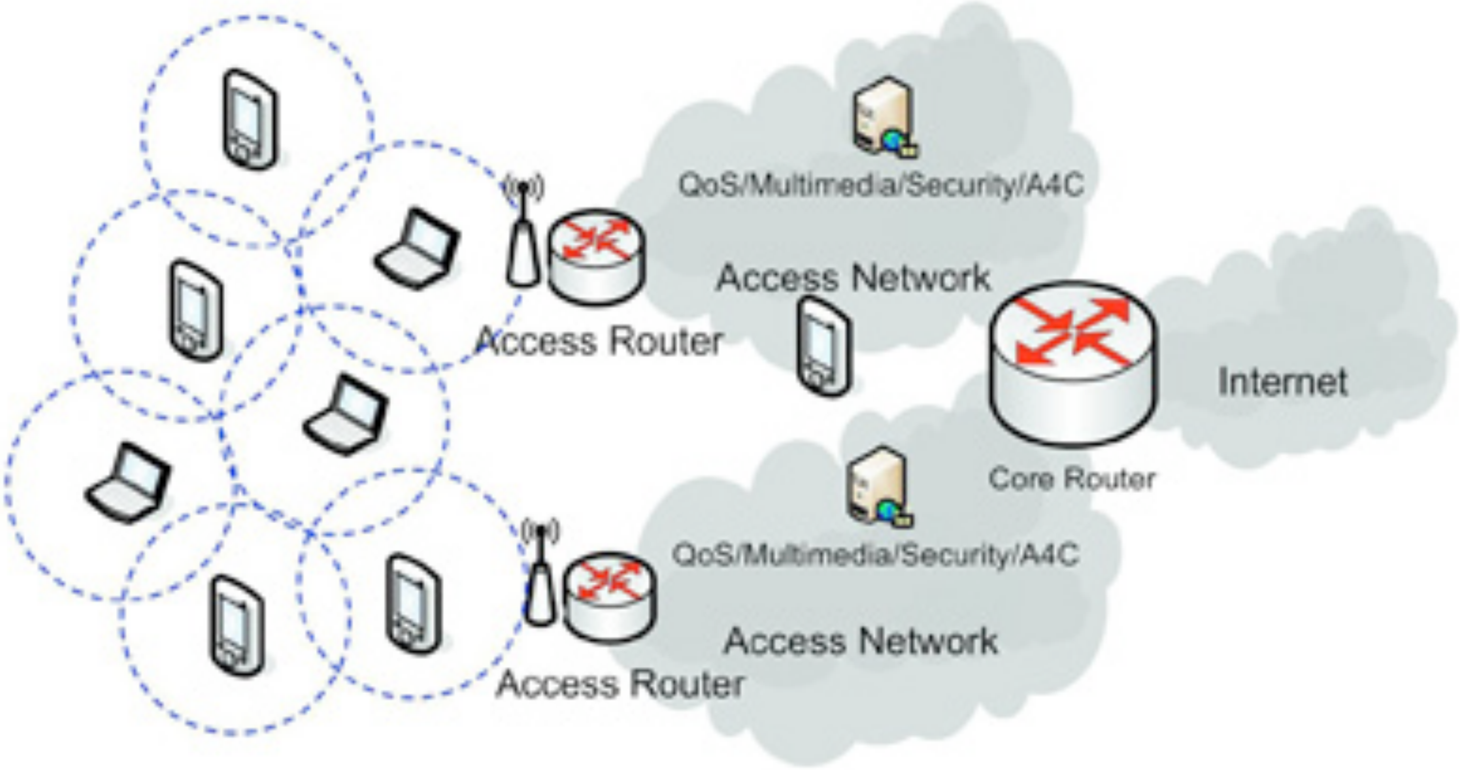
Characteristics

- No fixed infrastructure
- Dynamic changing topology
  - Mobile devices join/leave the network unexpectedly; they can also move freely
- Energy-constrained
- Limited bandwidth
- Each node also serves as router
  - Help to relay packets received from neighbors
- Interoperation with the Internet

Comparison

- MANETs *vs.* Wired networks
  - In MANETs, each node also works as router for forwarding packets
  - In wired networks, routers perform routing task
- MANETs *vs.* Managed wireless networks
  - No infrastructure in MANETs
  - Special node known as *access point* (AP) in managed wireless networks

A MANET Example



http://www.comp.nus.edu.sg/~xuemingq/research.html

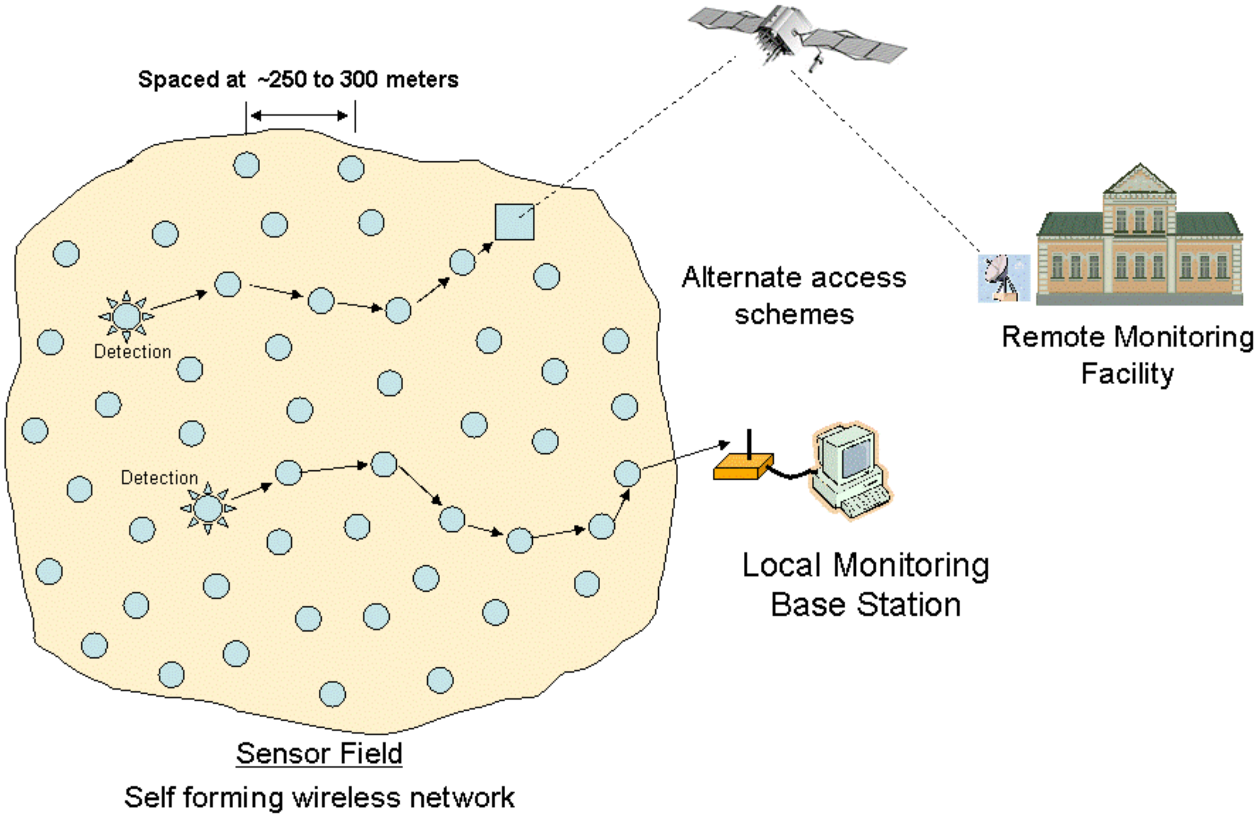
Mobile Devices

- Laptop computers
- Pagers, cellular phones, PDAs
- In-car navigators -Dash Express
  - Dash units talk to each other and form a network that connects to the Internet
  - Traffic speed data is sent back to the company, then broadcast back to all local dash units
- Sensors
- ……

Wireless Sensor Network (WSN)

- An emerging application area for MANETs
- A collection of cheap to manufacture, stationary, tiny sensors
- Network lifetime -- power as a major driving issue
- Battlefield surveillance, environment monitoring, health care, etc.

WSN Example


Spaced at ~250 to 300 meters
Detection
Detection
Alternate access schemes
Remote Monitoring Facility
Local Monitoring Base Station
Sensor Field
Self forming wireless network

http://www.alicosystems.com/wireless%20sensor.htm

Other MANETs applications

- Collaborative work
- Crisis-management applications
- Personal Area Networking (PAN)

Security Requirements in MANETs

- *Availability*
- Authorization and Key Management
- Data *Confidentiality*
- Data *Integrity*
- Non-repudiation

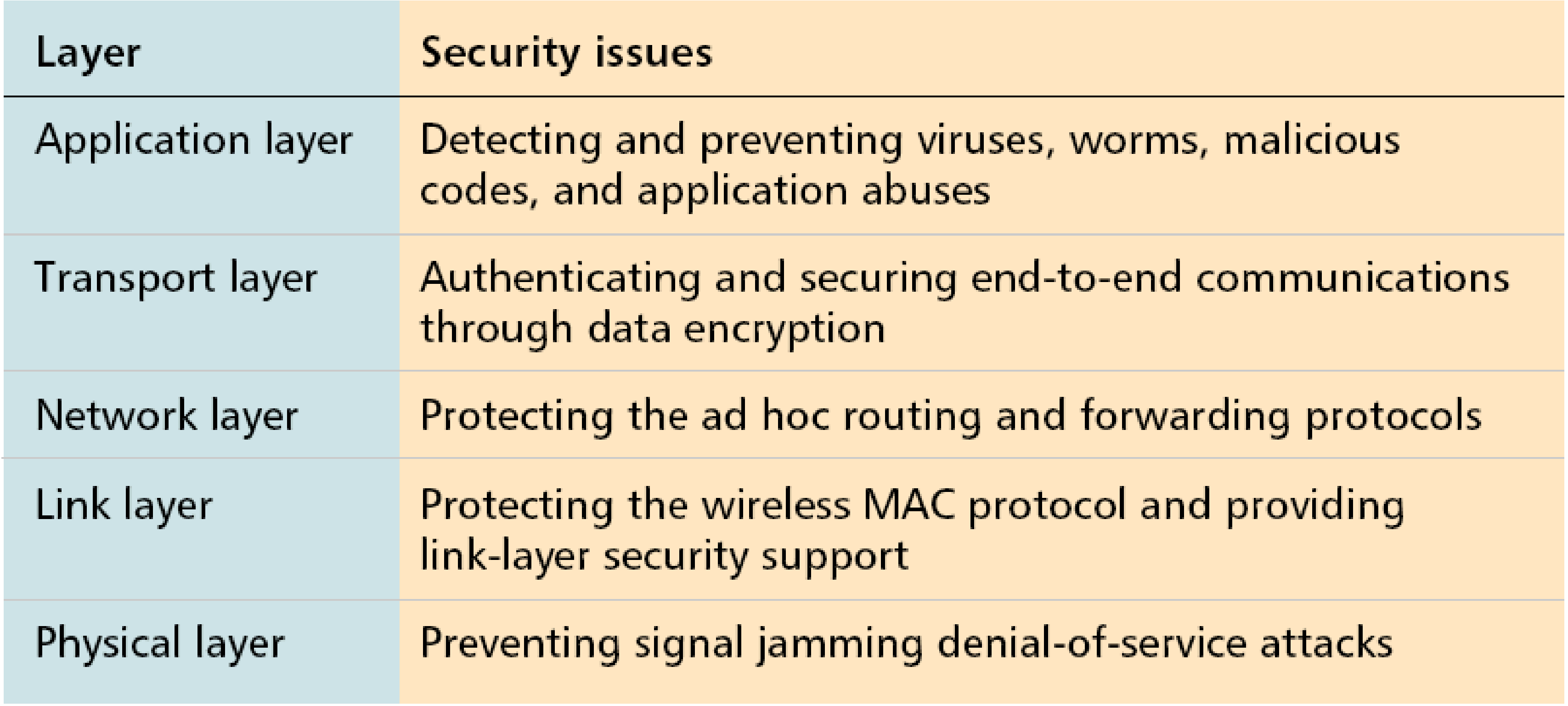
Security Solution Constraints

- Lightweight
- Decentralized
- Reactive
- Fault-tolerant

Challenges

- No infrastructure
- Peer-to-peer architecture with multi-hop routing
- Mobile device physical vulnerability
- Stringent resource constraints
- Wireless medium
- Node mobility

Security Issues



Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions" (2004). IEEE Wireless Communications.

Threats

- Attacks
  - External attacks
  - Internal attacks
  - Passive attacks
  - Active attacks
- Misbehavior

MANETs Security

- Routing security
- Data forwarding security
- Link layer security
- Key management
- Intrusion detection systems (IDSs)

Routing in MANETs

- Nodes’ mobility -topology changes rapidly
- Large network size -significant amount of network control traffic

MANET Routing Protocols

- Topology-based approaches
  - Proactive routing (table driven)
  - Reactive routing (on demand)
  - Hybrid routing
- Position-based approaches

Comparison

- Proactive routing
  - Classic routing strategies: link state, distance vector
  - Keep track of routes to all possible destinations
  - Changes in link connection updated periodically
  - Minimal delay but substantial fraction of control information
  - E.g. DSDV, WRP, TBRPF, OLSR, etc.

Comparison

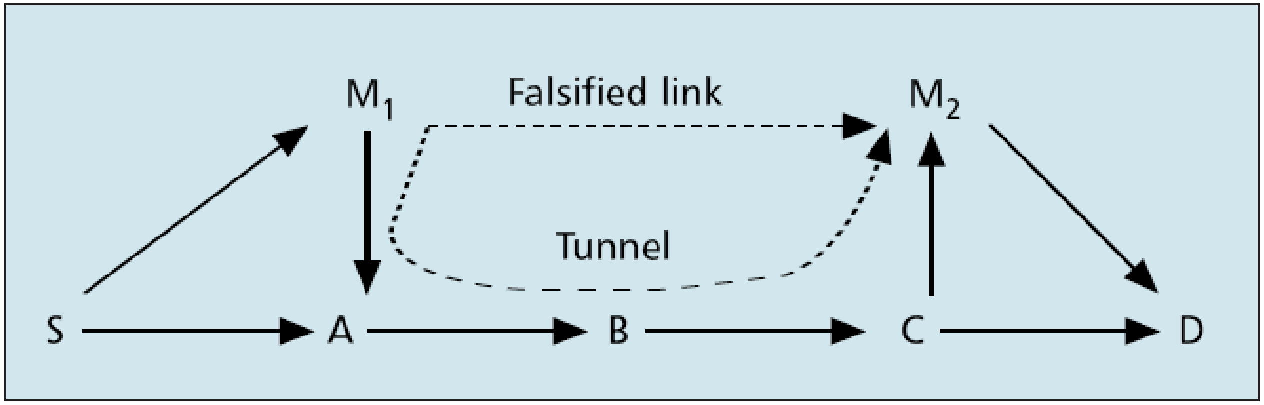
- Reactive routing
  - Only discover routes to destinations on-demand
  - Consume much less bandwidth but experience substantial delay
  - E.g. DSR, ADOV, TORA, etc.

DSR vs. AODV

- Dynamic source routing (DSR)
  - Source broadcasts RREQ through the network
  - Intermediate nodes add its addr to RREQ and continue broadcasting until RREP received
  - Full path chosen by source and put into each packet sent
- Ad hoc on-demand distance vector (AOVD)
  - Hop-by-hop routing
  - Source sends RREQ to neighbors
  - Each neighbor does so until reach the destination
  - Destination node sends RREP follow the reverse path
  - Source doesn’t put whole path but only next hop addr in outgoing packets

Routing Protocol Attacks

- Attacks using modification
  - Redirection by modifying route sequence number
  - Redirection by modifying hop count
  - Source route modification
  - Tunneling

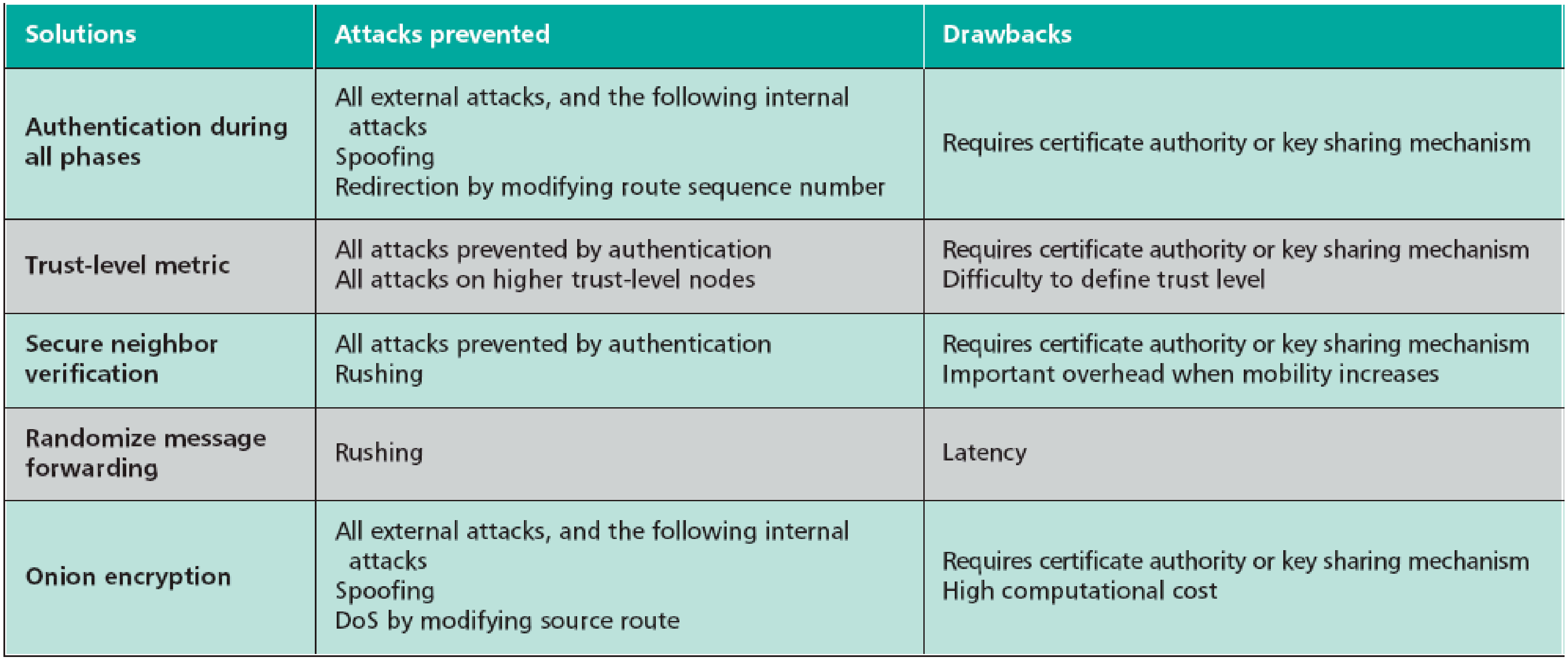


D. Djenouri, L. Khelladi and A.N. Badache. “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks”, Communications Surveys & Tutorials, IEEE

Routing Protocol Attacks

- Attacks using fabrication
  - Falsifying route errors
  - Broadcast falsified routes
- Spoofing attacks
- Rushing attacks

Solutions to Secure Routing Protocols



Solutions	Attacks prevented	Drawbacks
Authentication during all phases	All external attacks, and the following internal attacks Spoofing Redirection by modifying route sequence number	Requires certificate authority or key sharing mechanism
Trust-level metric	All attacks prevented by authentication All attacks on higher trust-level nodes	Requires certificate authority or key sharing mechanism Difficulty to define trust level
Secure neighbor verification	All attacks prevented by authentication Rushing	Requires certificate authority or key sharing mechanism Important overhead when mobility increases
Randomize message forwarding	Rushing	Latency
Onion encryption	All external attacks, and the following internal attacks Spoofing DoS by modifying source route	Requires certificate authority or key sharing mechanism High computational cost

D. Djenouri, L. Khelladi and A.N. Badache. "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks", Communications Surveys & Tutorials, IEEE

Data Forwarding Security

- Threats
  - Eavesdropping (passive attacks)
    - cryptography can help to prevent but how to detect eavesdropping is still an open research topic
  - Dropping data packets (similar to selfishness)
  - Selfish behavior on data forwarding
    - Drops other nodes' packets to preserve its resources, e.g. battery power

Detection Solution against Selfishness

- End-to-end feedbacks
- Monitoring in promiscuous mode (watchdog)
- Activity-based overhearing
- Mutually according admission in neighborhood
- Reputation based solution
- Probing

Preventive Solution against Selfishness

- Nuglets
  - Nodes who use the service must pay for it to nodes that provide the service
- Data dispersal
  - Adding redundancy to the messages to send; thus partial reception can lead to successful reconstruction of messages

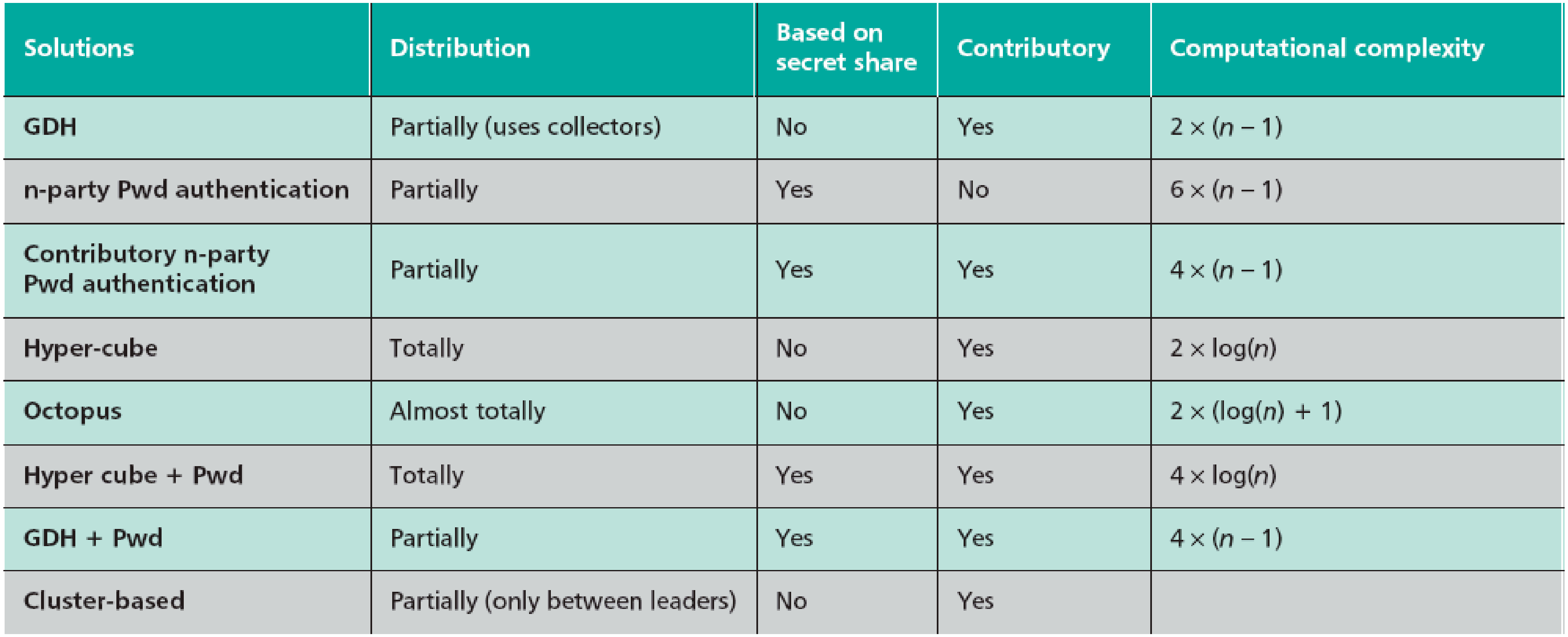
Link Layer Security

- IEEE 802.11 MAC
  - Vulnerable to DoS attacks
  - Attacks can exploit its binary exponential backoff scheme to launch DoS
  - A security extension to 802.11 was proposed
    - Backoff time at the sender is provided by the receiver
- IEEE 802.11 WEP -discussed in wireless security

Key Management

- Most of the solutions for secure routing and data forwarding rely on cryptography
- Key management is problematic because of the lack of any central infrastructure
  - Private key infrastructure
  - Public key infrastructure

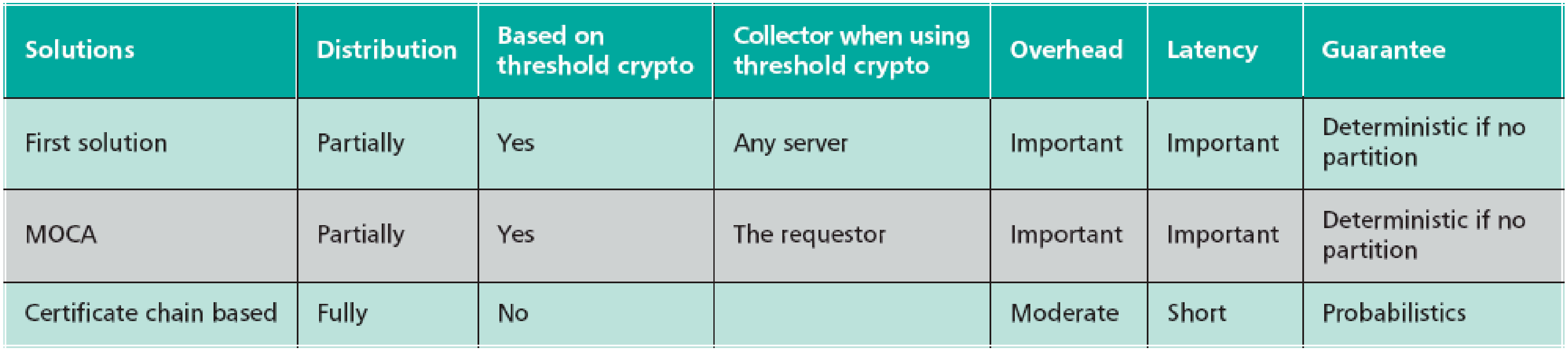
Private Key Infrastructure



Solutions	Distribution	Based on secret share	Contributory	Computational complexity
GDH	Partially (uses collectors)	No	Yes	$2 \times (n - 1)$
n-party Pwd authentication	Partially	Yes	No	$6 \times (n - 1)$
Contributory n-party Pwd authentication	Partially	Yes	Yes	$4 \times (n - 1)$
Hyper-cube	Totally	No	Yes	$2 \times \log(n)$
Octopus	Almost totally	No	Yes	$2 \times (\log(n) + 1)$
Hyper cube + Pwd	Totally	Yes	Yes	$4 \times \log(n)$
GDH + Pwd	Partially	Yes	Yes	$4 \times (n - 1)$
Cluster-based	Partially (only between leaders)	No	Yes	

D. Djenouri, L. Khelladi and A.N. Badache. “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks”, Communications Surveys & Tutorials, IEEE

Public Key Infrastructure



Solutions	Distribution	Based on threshold crypto	Collector when using threshold crypto	Overhead	Latency	Guarantee
First solution	Partially	Yes	Any server	Important	Important	Deterministic if no partition
MOCA	Partially	Yes	The requestor	Important	Important	Deterministic if no partition
Certificate chain based	Fully	No		Moderate	Short	Probabilistics

D. Djenouri, L. Khelladi and A.N. Badache. “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks”, Communications Surveys & Tutorials, IEEE

Intrusion Detection Systems (IDSs)

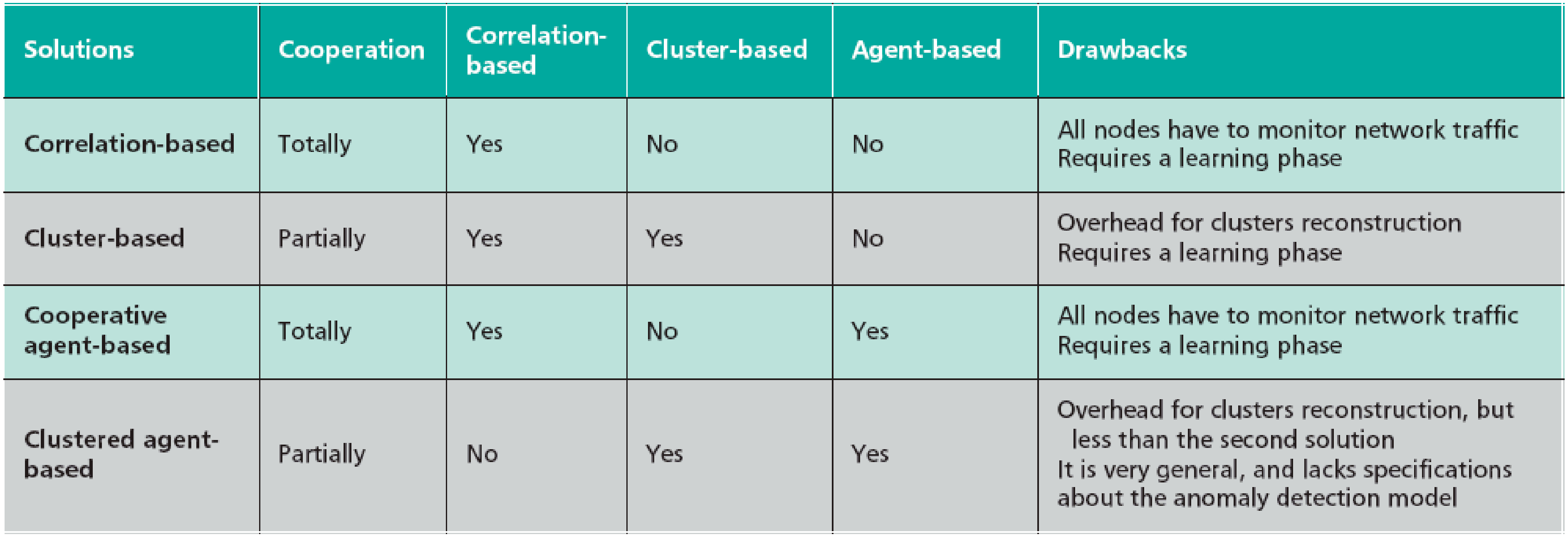
- Proactive solutions cannot eliminate attacks (secure routing layer, link layer mechanism)
- IDS presents a second wall of defense
- Assumptions
  - User and programs are observable
  - Normal and intrusion activities can be distinguished

Problems with Traditional IDSs in MANETs

- Infrastructureless nature of MANETs
  - No traffic concentration points for monitoring
- Resource limitation of mobile devices
- Lack of clear separation between normalcy and anomaly
  - as nodes move around, the topology changes;
  - so each node should expect different traffic pattern from its neighbors

Proposed Solutions

- Distributed, host-based, anomaly-based, and cooperative



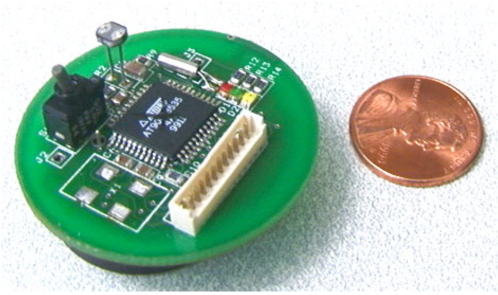
Solutions	Cooperation	Correlation-based	Cluster-based	Agent-based	Drawbacks
Correlation-based	Totally	Yes	No	No	All nodes have to monitor network traffic Requires a learning phase
Cluster-based	Partially	Yes	Yes	No	Overhead for clusters reconstruction Requires a learning phase
Cooperative agent-based	Totally	Yes	No	Yes	All nodes have to monitor network traffic Requires a learning phase
Clustered agent-based	Partially	No	Yes	Yes	Overhead for clusters reconstruction, but less than the second solution It is very general, and lacks specifications about the anomaly detection model

D. Djenouri, L. Khelladi and A.N. Badache. "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks", Communications Surveys & Tutorials, IEEE

Wireless Sensor Network (WSN) Security

- Consists of thousands or millions of tiny devices:
  - signal processing circuit,
  - micro-controller,
  - wireless transmitter/receiver,
  - embedded sensor

MICAZ Mote



http://agent.cs.dartmouth.edu/scalable/DSCN0022.JPG

More Stringent Performance Requirement

- More stringent performance requirement
  - Energy efficiency *-network lifetime*
  - Auto-organization
  - Scalability to a high number of nodes

Security Issues

- Key distribution and management
  - Scalable to a large number of sensor nodes
  - Remains to be unsolved
    - Key pre-deployment
    - Shared key discovery
    - Path-key establishment
  - Alternatives
    - Probabilistic key sharing protocols

More Issues

- Secure routing
  - Most routing protocols are quite simple in WSN, thus more vulnerable to attacks. Some new attacks are:
    - Sinkhole attacks
    - Hello flood attacks
  - Solutions
    - SPINS -two building block security protocols: SNEP and μTESLA
    - INSENS -intrusion-tolerant routing protocol

More Issues

- Secure data aggregation
  - Key theme in design and development of WSNs
  - Aggregators collect raw data, process it locally, and forward only the result to end-user
  - Aggregation can take in any places, and must be secured
- Denial of service
  - Jammed by adversaries: jam the entire network by broadcasting a high enough energy signal
- Resilience to node capture

Summary

- What we have discussed
  - Characteristics of MANETs, WSNs
  - Security issues in MANETs and WSNs
- MANETs is a growth area of research; the security issues in MANETs attract a lot of researchers; we'll be definitely seeing more of these problems in near future.

More Readings

- H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, “Security in mobile ad hoc networks: Challenges and solutions” (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.
- D. Djenouri, L. Khelladi and A.N. Badache. “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks”, Communications Surveys & Tutorials, IEEE, Vol. 7, Issue 4, pp. 2--28, Fourth Quarter 2005.
- Yih-Chun Hu , Adrian Perrig, “A Survey of Secure Wireless Ad Hoc Routing”, IEEE Security and Privacy, v.2 n.3, p.28-39, May 2004