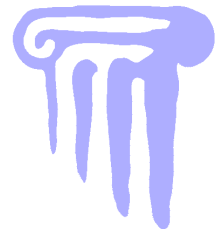


Information Assurance in Manet and Sensor Networks

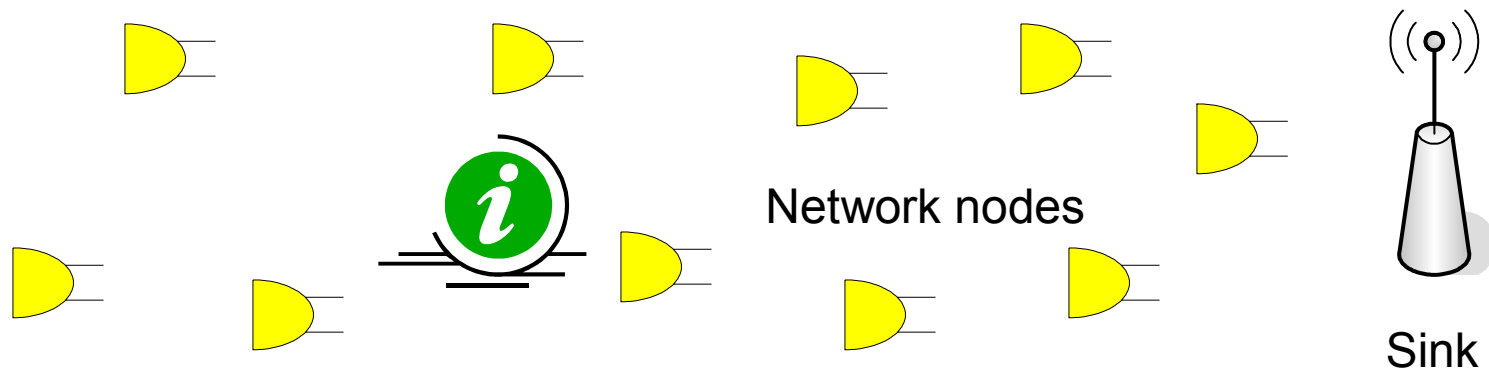
Radha Poovendran
University of Washington
Seattle, WA



Acknowledgements

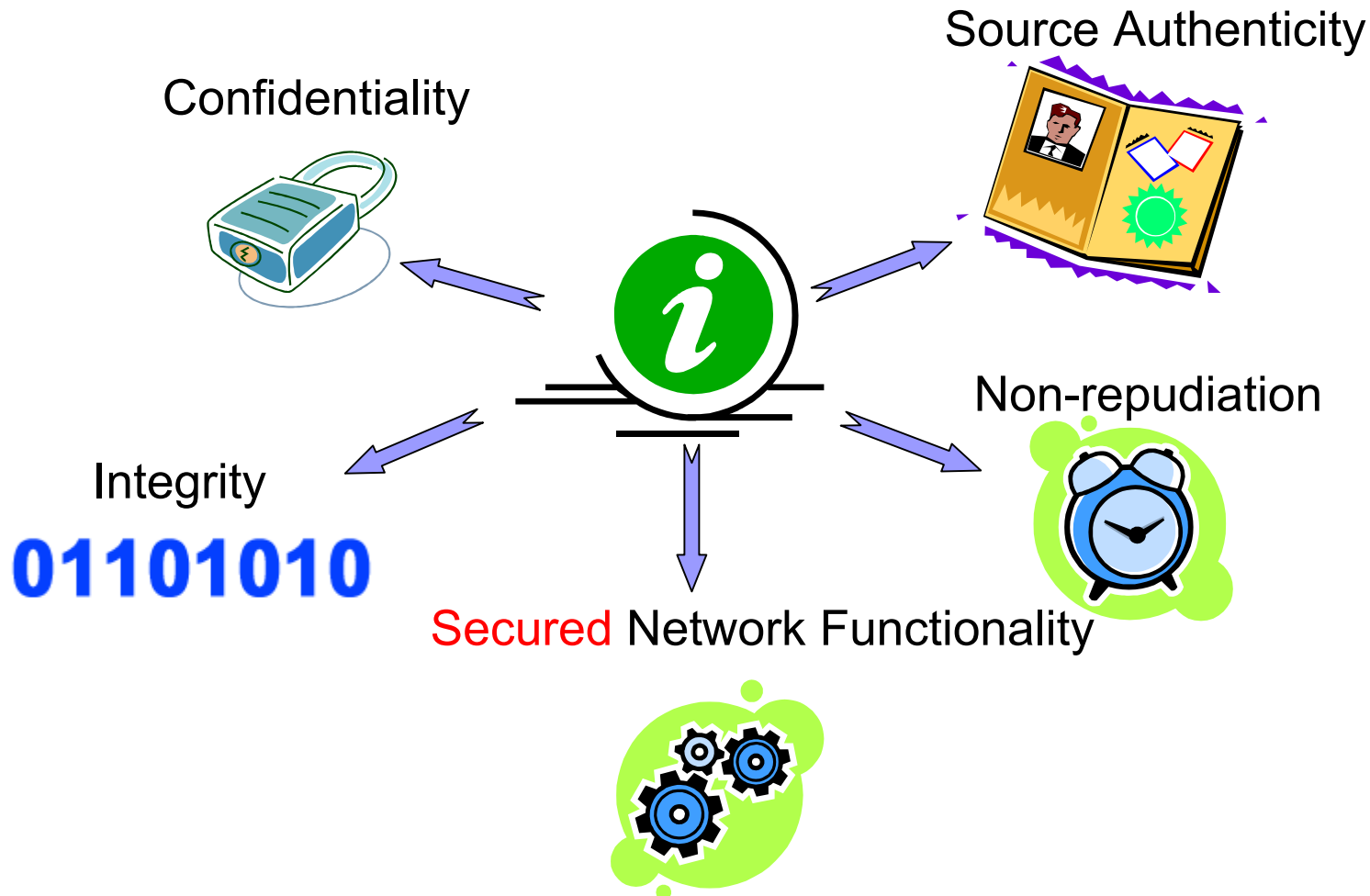
- Following colleagues have influenced this presentation
 - Loukas Lazos, Srdjan Capkun, Tony Ephremides, Cliff Wang, Mingyan Li, Jeff Wieselthier, Cathy Meadows, Peng Ning, Adrian Perrig, Wade Trappe

What is information assurance?



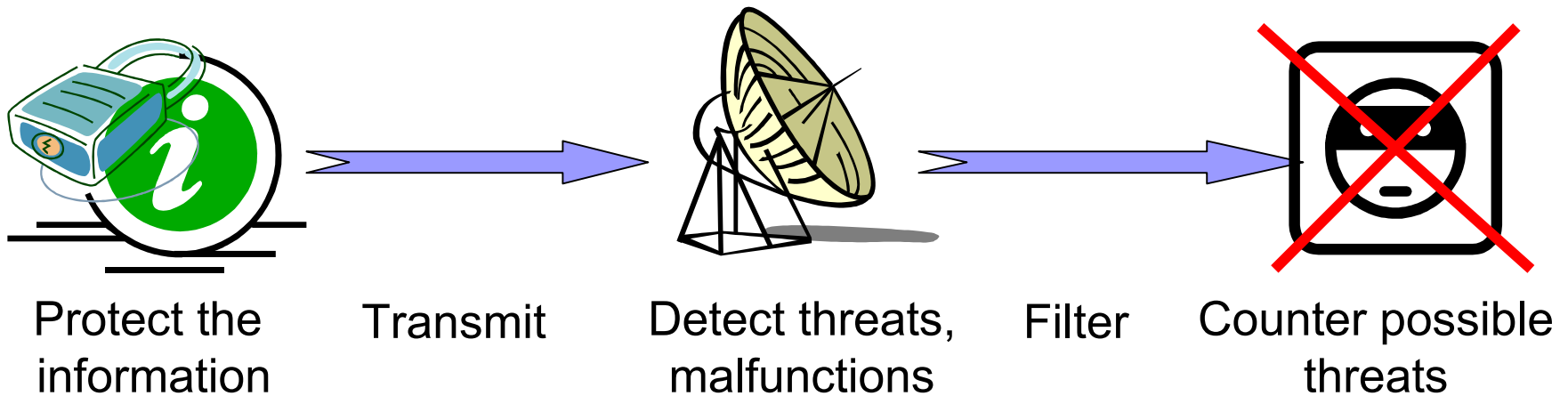
- Depends
 - different needs for civilian and military
- In general
 - Assurance of provision of information services only to authorized users
- Often requires establishment and maintenance of network as well as application services

The Road to Information Assurance



Assurance of information: How is it achieved?

- To provide information assurance a system should be able to



The MANET Network Environment

- Ad hoc, distributed network with no central management
- Dynamic network topology
- Constrained in resources
 - Energy constrained
 - Bandwidth and Power constrained
 - Computationally limited

The Sensor Network Environment

- Compared to MANET
 - Mostly static networks
 - Though no fixed infrastructure, often there exists a hierarchical architecture
 - Even more scarce in resources
 - Easy to capture and compromise nodes

Threats in MANET and Sensor Networks

- Threats can be classified per layer
 - Against the physical layer, MAC layer, network layer, application layer
- But, Cross-layer designs in network functions for achieving resource efficiency result in *Cross-layer threats*
 - E.g. Attacking the physical layer denies functionality of the network layer

Threats in the Physical layer

- Jamming the link
 - Inherently brute force with constant power expended by the jammer
 - Does not exploit any feature of the communication protocol
- Solutions do not lead to sophisticated prevention schemes
 - Detect location of jammer and remove!

Threats in the MAC Layer

■ Jamming

- Exploits the MAC layer protocol specific features
- Can be modeled and detected using MAC protocol details (SBK WiSe 2005)

■ Jammer needs to be clever to avoid detection

- Higher probability of being detected if only the sensing mode is used

Threats in the network layer

- Attacks target to disturb
 - Neighbor discovery
 - Single and multihop link establishments
 - Effectively disturbing the secure network service establishment
- Solution requires
 - Secure Network Initialization and trust establishment among the nodes

Threats in the application layer

- Attacks on distributed computing or communication
 - Data Aggregation
 - Data/Source Authentication
 - ...
- Solutions make use of
 - Cryptographic approaches
 - Secure location information
 - Secure Time synchronization

Cross-layer effect of threats

- Often higher layer functionalities rely on lower layers
 - Hence, vulnerabilities that exist in lower layer can serve as stepping stones
- Example
 - Incorrect estimation of single and multihop neighbors leads to
 - Incorrect forwarding tables
 - Misroute the application data

Privacy Issues in WSN

■ Context-Oriented Privacy

- Problem arises since an adversary can observe the context surrounding creation and transmission of a sensor message.

■ Examples of privacy in WSN

- Location information privacy
- Temporal information privacy
- Traffic information privacy

Privacy Issues in WSN

- Not too difficult to show that we may not be able to provide 100% privacy
- We need to be able to characterize the privacy breach in terms of the network parameters

Incomplete List of Challenges

■ *Resource-Efficient Secure Network Services*

- *Network Initialization, single/multihop neighbor discovery*
- *Multihop path establishment & Routing*
- *Supporting application services*

Incomplete List of Challenges

- Security mechanisms for fundamental services
 - Clock synchronization
 - Secure location discovery and verification of claims
 - Location privacy
 - Secure aggregation and in-network processing
 - Cluster formation/cluster head election
 - Middleware

Incomplete List of Challenges

- Modeling vulnerabilities
 - Current state of understanding is not enough
 - Example: Sybil, wormhole
 - Required to eliminate context based attacks

Robust Designs for WSN

- Attacks and compromise of network are reality
 - Misconfiguration cannot be fully eliminated
 - We may not be able to distinguish between failure and attack
 - Not every device can implement maximum-strength solutions
- Opt for application dependent detection and functioning even in the presence of attacks
 - Quantify detection in terms of system parameters

Some final thoughts

- Manets and WSN are distributed environments
 - Some challenges will remain open!
 - Solutions often require application specific details
- Results in cross-layer directions
- Results in exploitation of duty cycles
- Combining QoS with security
 - Possibly for MANET if not WSN at present