Research Projects in the Mobile Computing and Networking (MCN) Lab

Guohong Cao
Department of Computer Science and Engineering
The Pennsylvania State University
http://www.cse.psu.edu/~gcao

Mobile Computing and Networking (MCN) Lab

- MCN lab conducts research in many areas of wireless networks and mobile computing, emphasis on designing and evaluating mobile systems, protocols, and applications.
  - Current Projects: wireless sensor networks, vehicular networks, wireless network security, data dissemination/access in wireless P2P networks, resource management in wireless networks.
  - Support: NSF (CAREER, ITR, NeTS, NOSS, CT, CNS), Army Research Office, DoD/Muri, PDG/TTC and member companies Cisco, Narus, Telcordia, IBM and 3ETI.
- Current students: 10 PhD, 2 MS, and 2 honor BS students
  - Alumni: 6 PhD, including faculty members at Iowa State University, Florida International University, Frostburg State University, and students in Motorola, Cisco, Microsoft.
  - 10 MS students went to various companies

Current Research Projects

- Collaborative Data Access in Wireless P2P Networks (with C. Das)
- Data Dissemination in Vehicular Ad Hoc Networks
- Controllable Node Mobility for Mission-Oriented Sensor Networks (with La Porta, Kesidis, Das)
- ARSENAL: A Cross Layer Architecture for Secure and Resilient Tactical Mobile ad hoc Networks (with La Porta)
- A Framework for Defending Against Node Compromises in Distributed Sensor Networks (with Zhu)
- Security and Privacy support for data centric sensor networks (with Zhu)

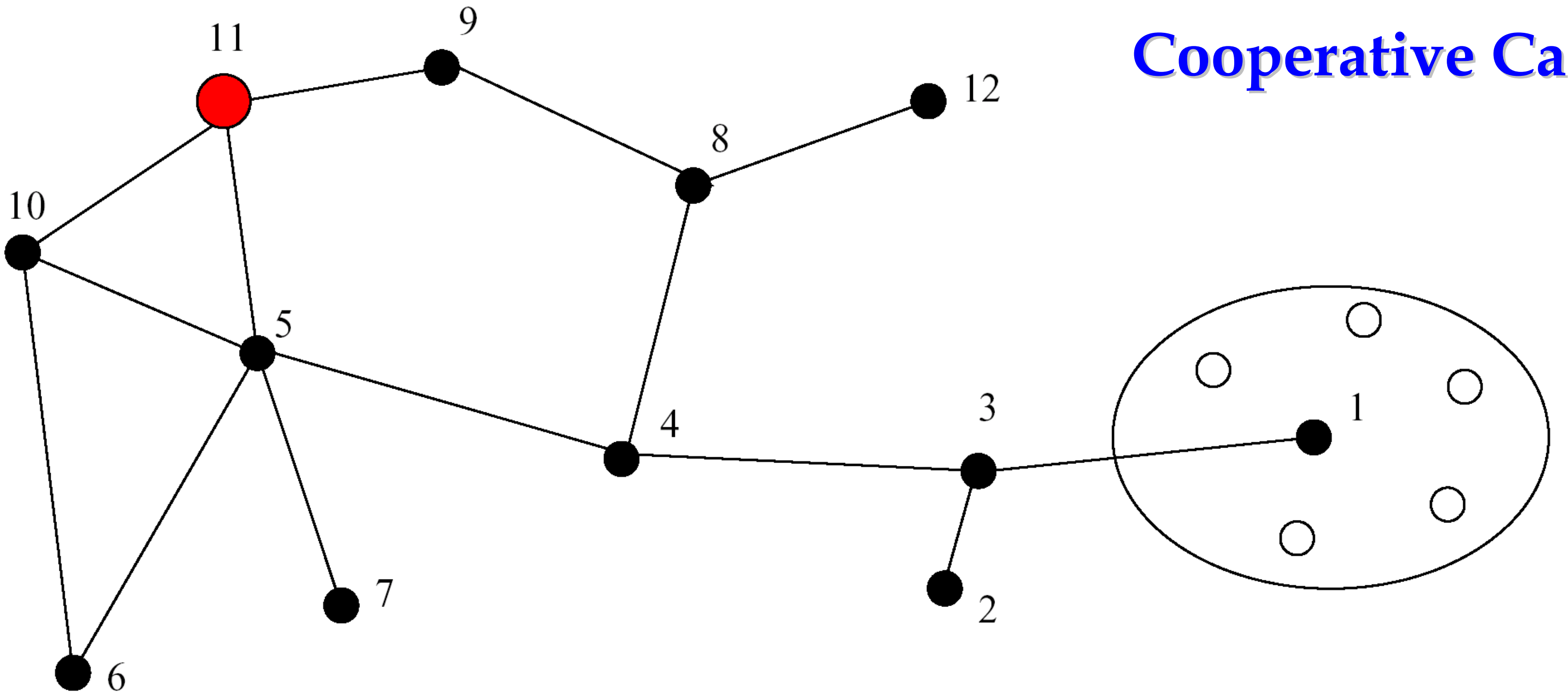
Wireless P2P Networks

- Wireless P2P networks can be mobile ad hoc networks, vehicular networks, sensor networks, mesh networks.
- Although there are differences (e.g., data transmission speed, link and physical layer characteristics) among these networks, they are some common features:
  - Wireless communication (interference issues), and the packets are transmitted through multi-hop relay
  - Applications in these networks are typically peer-to-peer rather than client-server.

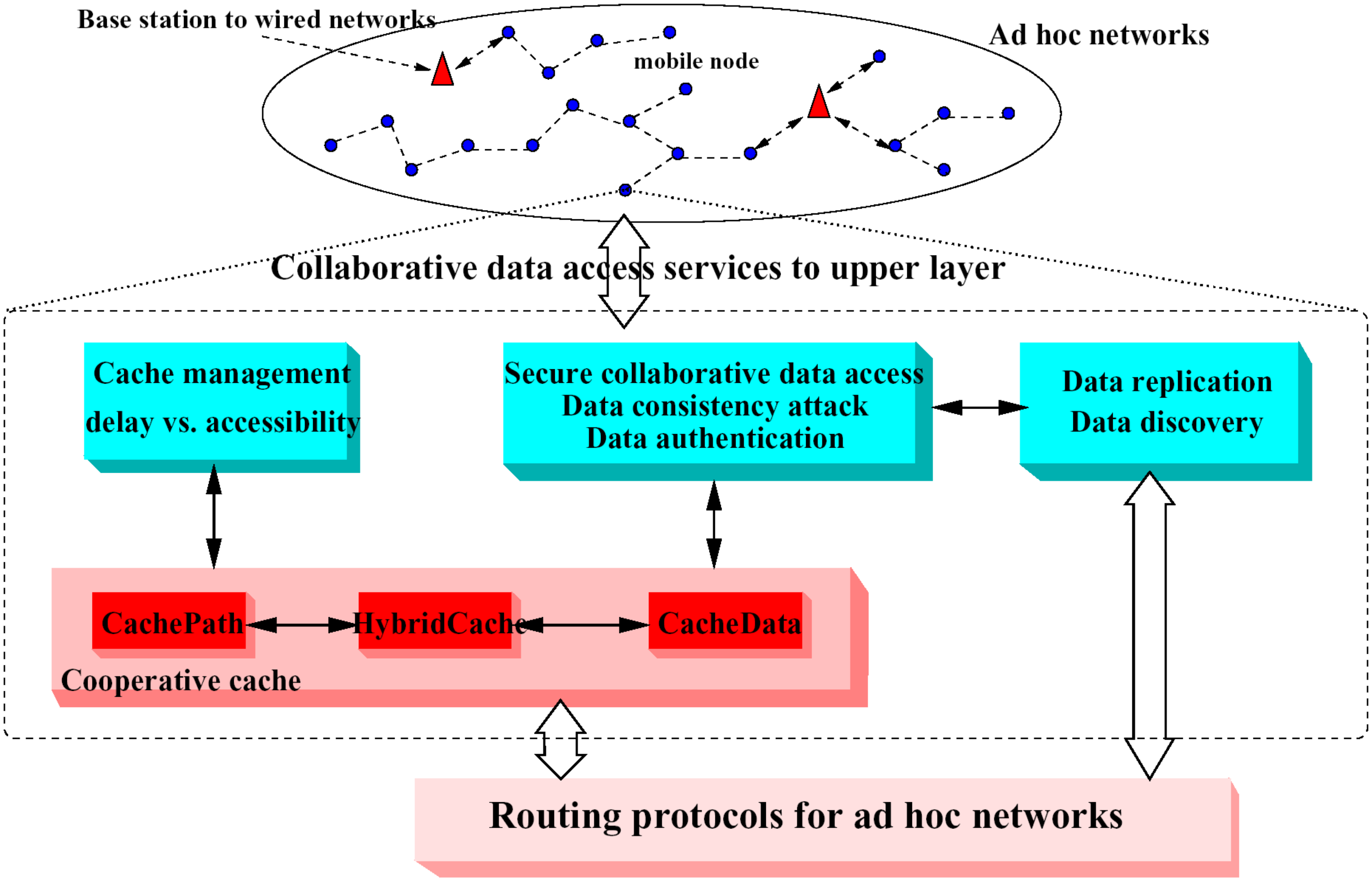
Data Access in wireless P2P Networks

- Most of the previous researches in wireless P2P networks focus on routing or MAC issues.
- Data access is also very important, since the ultimate goal of using the networks is to provide information access to mobile nodes.
- In Battlefield, after a soldier obtains enemy information (e.g., battlefield map, enemy distribution) from the commander (data center), it is very likely that nearly soldiers also need the same information.
  - Bandwidth and power can be saved if these data access are served by the soldier with the cached data instead of the data center which may be far away.
- Other examples: emergency rescue, file sharing in residential area, or infostation.

Cooperative Cache

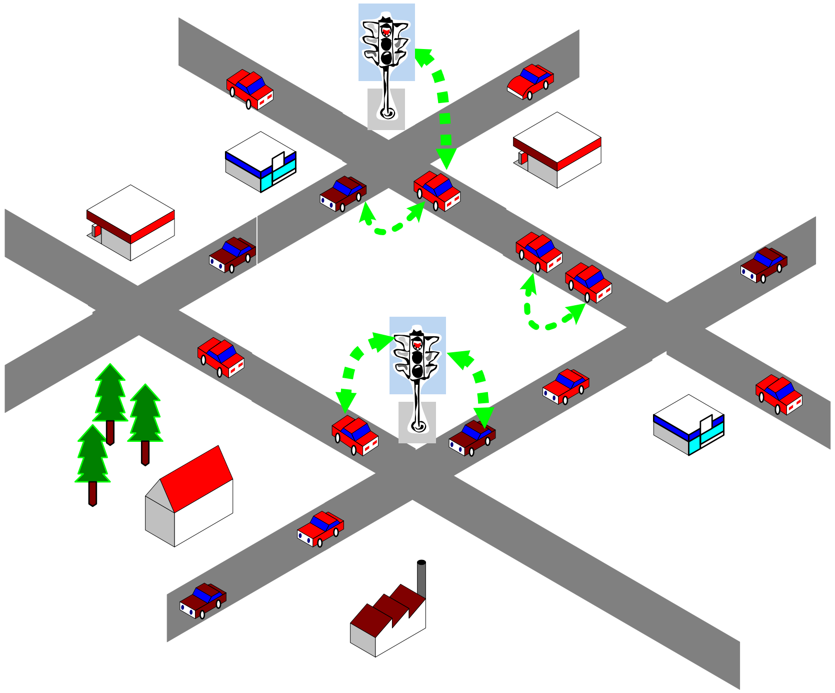


- CachePath: Cache the data path.
  - Suppose N_1 has requested a data item from N_{11}. N_3 knows that N_1 has the data. Later if N_2 requests for the data, it forwards the request to N_1 instead of N_{11}.
- CacheData: Cache the data
  - In the above example, N_3 caches the data, and forwards the data to N_2 directly.
- Many technical issues not shown here.


Base station to wired networks
Ad hoc networks
mobile node
Collaborative data access services to upper layer
Cache management
delay vs. accessibility
Secure collaborative data access
Data consistency attack
Data authentication
Data replication
Data discovery
CachePath
HybridCache
CacheData
Cooperative cache
Routing protocols for ad hoc networks

Vehicular Ad Hoc Networks (VANET)

- Ad hoc networks composed of vehicles and roadside units
  - Vehicle to vehicle communication
  - Vehicle to roadside communication
  - Roadside to roadside communication
- FCC assigns Dedicated Short Range Communications (DSRC), 75MHz radio spectrum (at 5.9 GHz).
- IEEE 802.11p

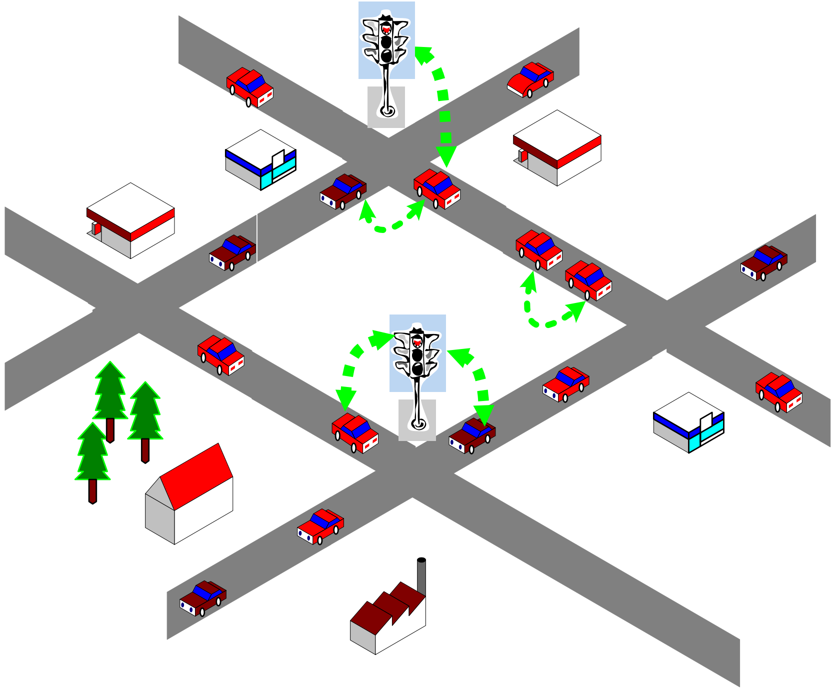


VANET Applications

- Safety
  - Fact: 6 Million crashes, 43,000 fatalities in U.S. per year
  - Example: propagate emergency warning to drivers behind a vehicle (or incident) to avoid multi-car collisions.
- Traffic Control
  - Congestion: 3.5 Billion hours delay, 5.7 Billion gal. wasted fuel per year in U.S.
  - Example: Alert drivers to potential traffic jams, providing increased convenience and efficiency.
- Travelers and business entities
  - Obtain location based information
  - E-Advertisement

Data Access/Dissemination in VANET

- Data dissemination in sparsely connected networks
- Infrastructure-assisted data dissemination
  - Data pouring with intersection buffering
  - Scheduling of data access in RSU
  - Improving performance with relay

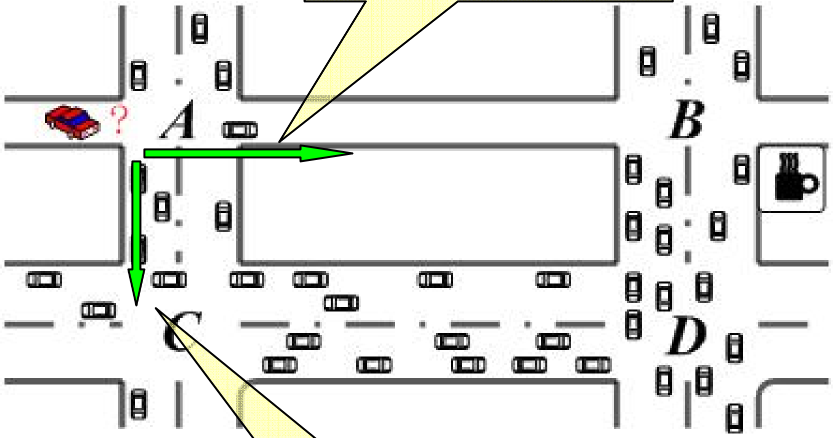


Data Dissemination in Sparsely Connected Network

- Task: to deliver a message from mobile vehicle to the fixed site several miles away.
  - A driver may want to find out the sale information in a store, the room availability in a hotel.
- Challenges:
  - There may be network partitions due to mobility or traffic condition
  - End-to-end connection through multi-hop is hard to set up. Most existing ad hoc routing protocols such as DSR/AODV may not work well.
- Mobility creates opportunities
  - Buffer and carry the packet when no routes
  - Forward the packet to the nodes moves into the vicinity which can help packet delivery
  - Possible to deliver the packet without an end-to-end connection
- Different from existing store-carry forward protocols, we make use of the predictable traffic pattern and vehicle mobility to assist data delivery.

Vehicle-Assisted Data Delivery (VADD)

- Key issue
  - Select a forwarding path with smallest packet delivery delay
- Why not GPSR?
- Guidelines
  - Make the best use of the wireless transmission
  - Forward the packet via high density area
  - Use intersection as a opportunity to switch the forwarding direction and optimize the forwarding path



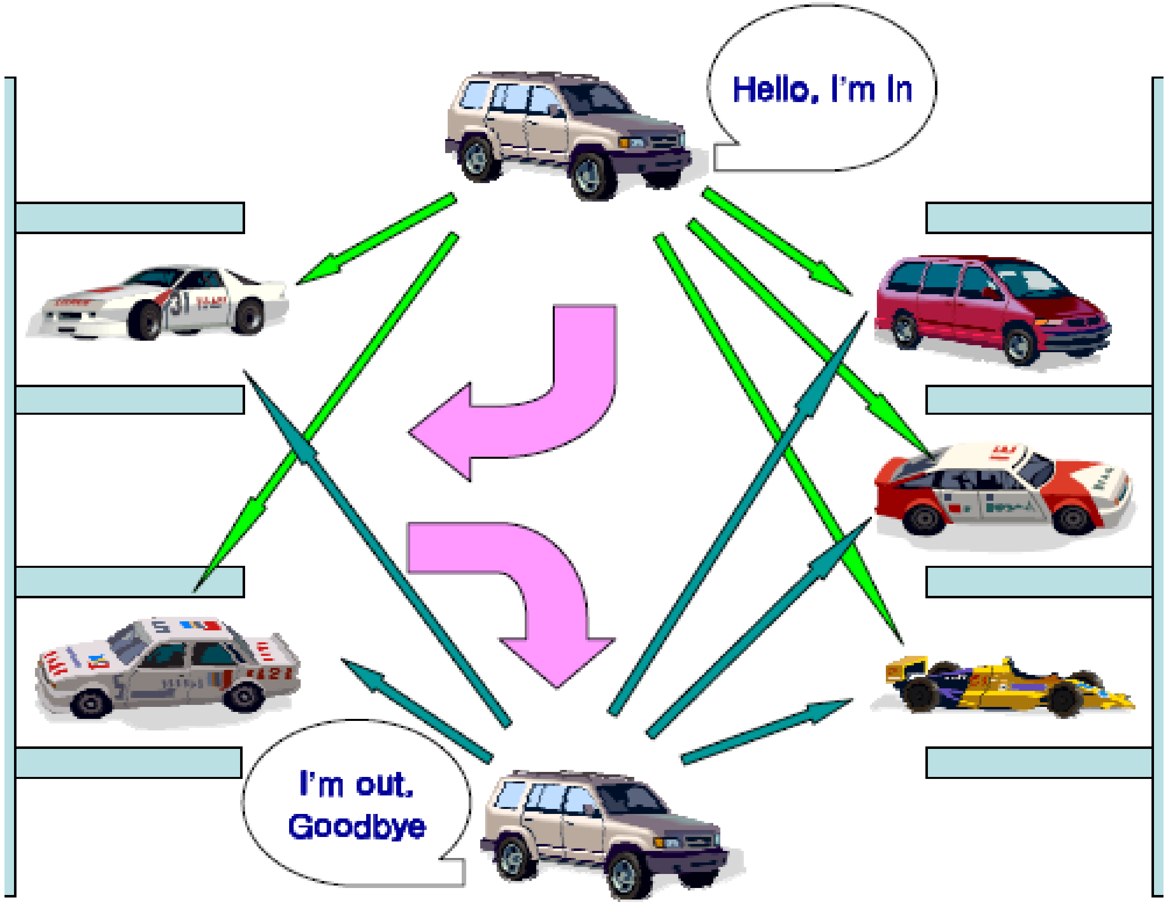
Geographically shortest path

Fast speed wireless communication

SVATS: A Sensor-network-based Vehicle Anti-Theft System

- Current vehicle anti-theft systems have some limitations.
  - Lock devices, car alarm system, tracking system
- Solution: use sensor nodes and let vehicles monitor other vehicles.
  - Sensors in the vehicles that are parked within the same parking area first form a sensor network, then monitor and identify possible vehicle thefts by detecting unauthorized vehicle movement.
  - When an unauthorized movement is detected, an alert will be reported.
  - Sensors inside the vehicle can be used for tracking the stolen vehicle.

SVATS: A Sensor-network-based Vehicle Anti-Theft System

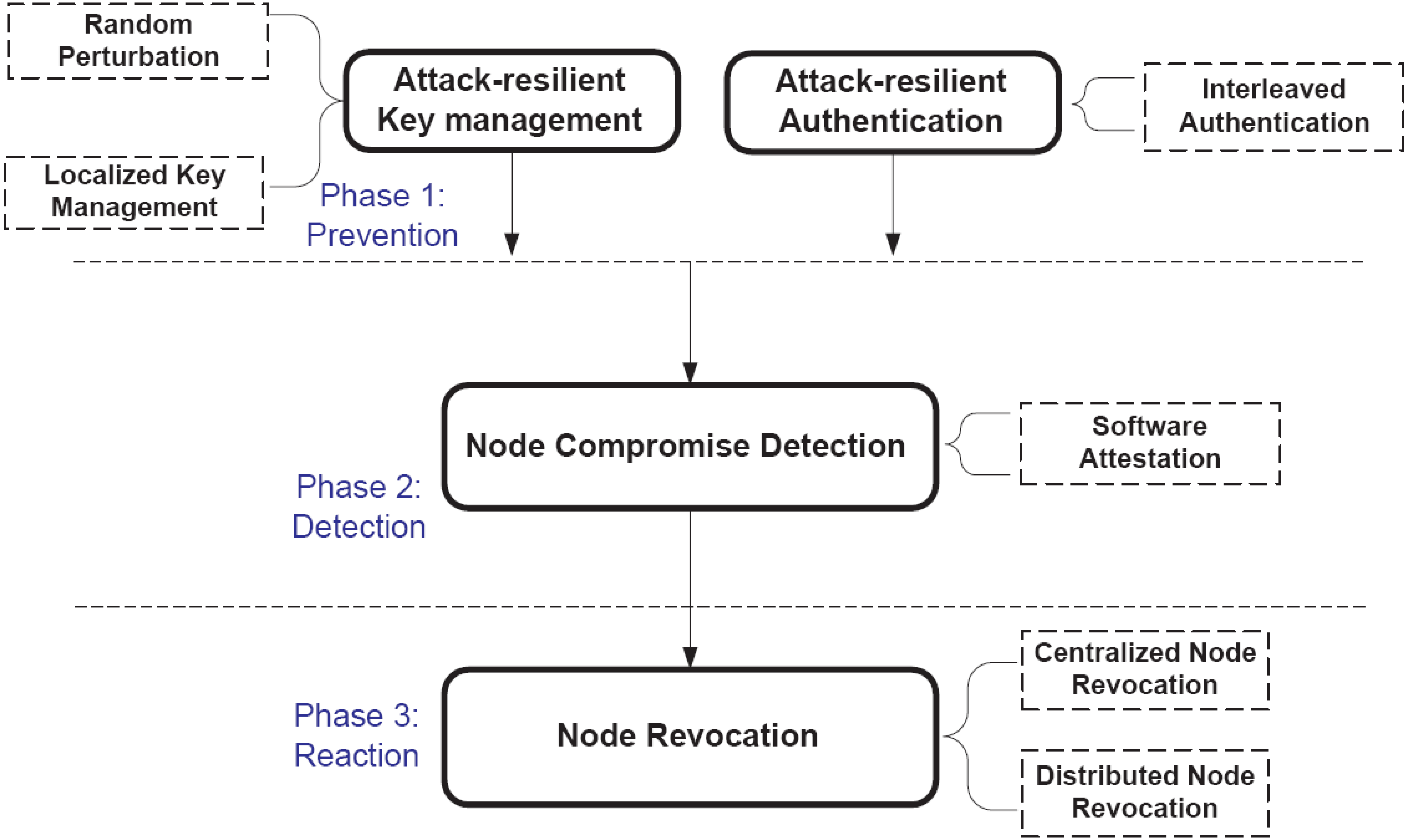


Vehicle Tracking

- Sensors in the stolen vehicle send signals to other vehicles, or APs on the road to track the stolen vehicle.
- Since the sensor is attached to the vehicle power, its position is known and may be destroyed by the thief, and then cannot report problems for tracking.
- We also add slave sensors, which can be put at several hidden places inside the vehicle so that the thief cannot locate them in a short time. Slave sensors are used to monitor the master sensor, and to report vehicle theft when master sensor is destroyed.
- Research issues: Network topology management, vehicle theft detection, intra-vehicle networking, vehicle tracking.

Secure Sensor Networks

- It is a big challenge to secure wireless sensor networks because of the network scale, the highly constrained system resource, and the fact that sensor networks are often deployed in unattended and hostile environments.
- We propose to develop a framework for defending against node compromises in unattended sensor networks. The framework consists of a suite of security mechanisms spanning three phases:
  - prevention
  - detection
  - reaction
- This research will provide fundamental security services covering key management, authentication, compromise detection, and revocation.


Random Perturbation
Localized Key Management
Attack-resilient Key management
Attack-resilient Authentication
Interleaved Authentication
Phase 1: Prevention
Node Compromise Detection
Software Attestation
Phase 2: Detection
Node Revocation
Centralized Node Revocation
Distributed Node Revocation
Phase 3: Reaction

A Framework for Defending Against Node Compromises in Distributed Sensor Networks