# Intrusion Detection for Mobile Ad Hoc Networks

Tom Chen
SMU, Dept of Electrical Engineering
tchen@engr.smu.edu
http://www.engr.smu.edu/~tchen

# Outline

- Security problems in MANETs
- Role of intrusion detection systems (IDSs)
- General IDS techniques
- Challenges for IDS in MANETs
- Some research problems

# Wireless Security

- Security for wireless networks is much harder than wired networks
  - Radio links are vulnerable to attacks from a distance, whereas wired links require physical access
  - Passive attacks (eavesdropping) are easy
  - Active attacks (masquerading, packet modification/interception, denial of service,…) are easy

# Security in MANETs

- Ad hoc networks present additional security problems
  - Mobile nodes are more vulnerable to capture or compromise
  - Proper routing operation of MANET depends on cooperation of all nodes -- compromised nodes may disrupt entire network
  - No fixed infrastructure to support security, eg, authentication server -- nodes must handle security by themselves

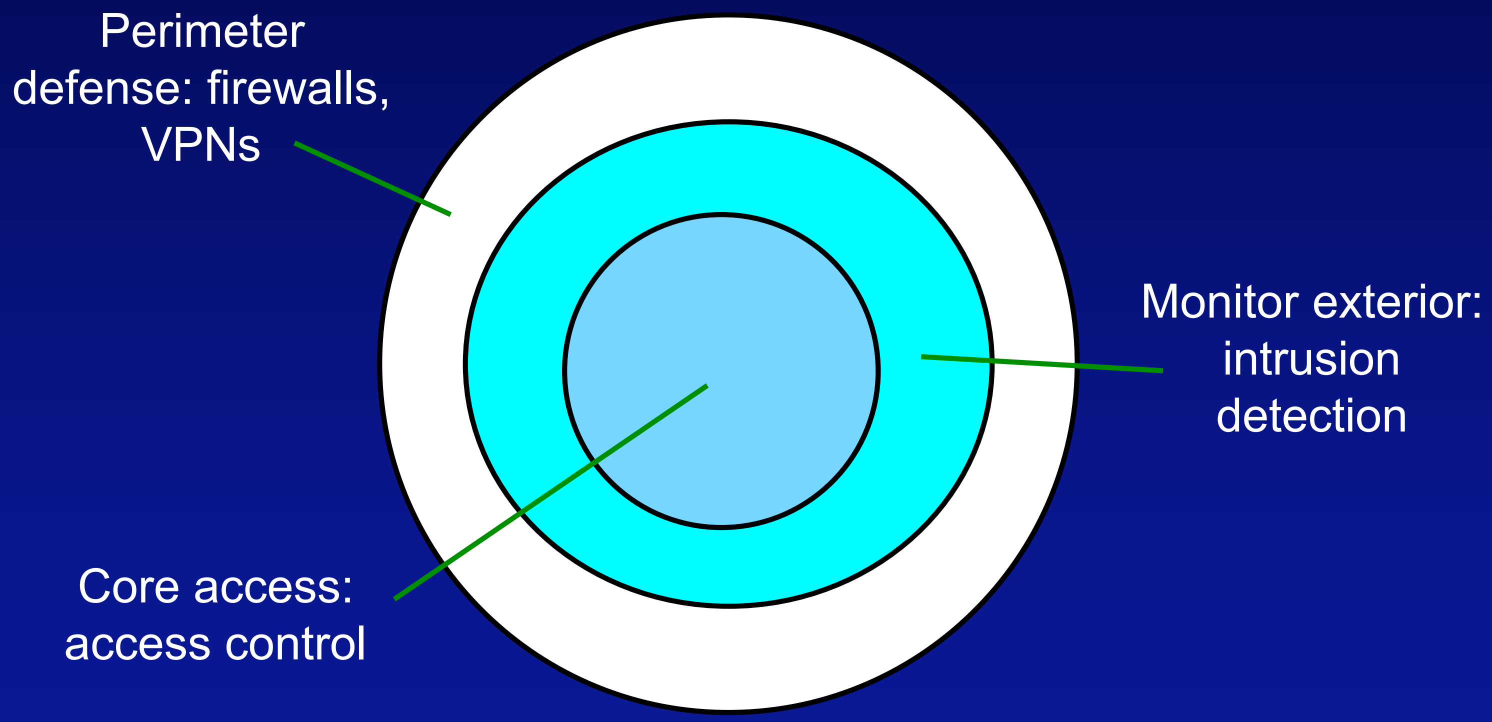
# Role of Intrusion Detection

- Security is based on cryptography which helps to
  - Keep data confidential
  - Authenticate the identity of hosts
  - Validate data integrity
- But cryptography is not sufficient protection - will not prevent attacks or prevent hosts from capture

# Intrusion Detection (cont)

- IDSs are part of typical “defense in depth” strategies
  - Various security components form layers of protection against attacks
  - Goal is not perfect protection, but make attackers spend more effort (cost)

# Defense in Depth



Perimeter defense: firewalls, VPNs

Monitor exterior: intrusion detection

Core access: access control

# Role of Intrusion Detection

- By analogy, castle is protected by walls, locked doors, moat, vault -- **preventive layers**
- IDSs serve as burglar alarms -- **reactive layer**
  - Useful complement to preventive layers

# Intrusion Detection (cont)

- 1980 James Anderson wrote report for US Air Force proposed a method for filtering computer audit trails and detecting unusual usage patterns through statistical analysis
- 1986 Dorothy Denning and Peter Neumann developed real-time IDES (Intrusion Detection Expert System) for US Navy and prototyped at SRI Int.

# Intrusion Detection (cont)

  - Anomaly detector characterized statistics of abnormal behavior
  - Expert system applied rules to detect security violations

- 1990 UC Davis developed NSM (Network System Monitor), first IDS to analyze network traffic

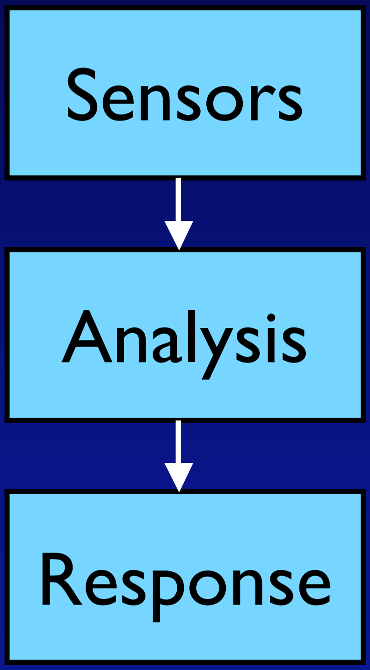
# Intrusion Detection (cont)

- 1992 DIDS (Distributed Intrusion Detection System) was large-scale R&D project between various labs and military agencies
  - In response to 1988 Morris worm
  - Goal to integrate IDSs across networks to centrally track security violations and intrusions

# Intrusion Detection (cont)

- 1998 DARPA sponsored an Intrusion Detection Evaluation of many IDSs
  - Found to be somewhat effective but some attacks not detected
  - More R&D needed to improve accuracy
- 2000 research on intrusion detection for ad hoc networks -- open problem

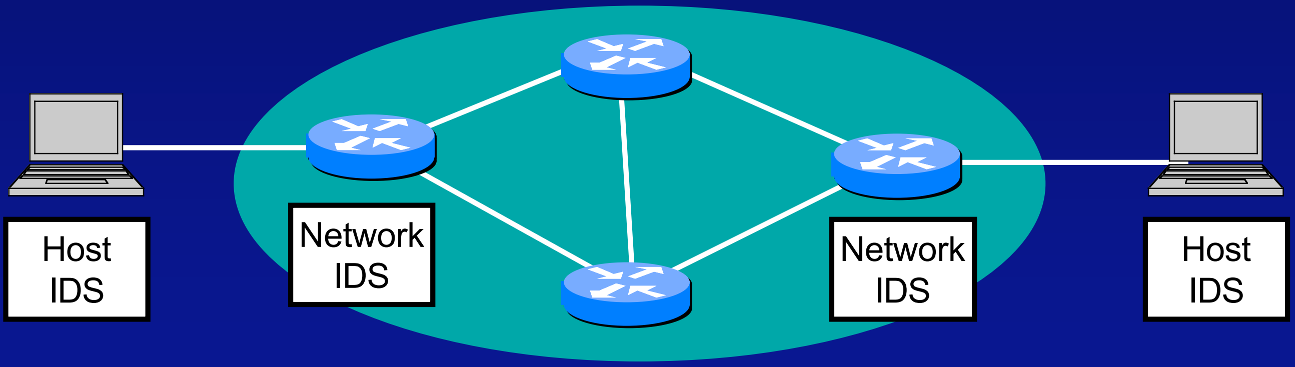
# IDS Basic Functions



- Continually monitor activities (packet traffic or host behavior)
- Automatically recognize suspicious, malicious, or inappropriate activities
- Trigger alarms to system administrator

# Types of IDSs

- IDSs can be classified according to their sensing: host-based or network-based



# Types of IDSs (cont)

- Host-based IDS: monitor host activities (audit trails)
  - Most reliable detection, but does not scale well (with increasing number of hosts)
- Network-based IDS: monitor packet traffic
  - Scalable but detection accuracy is problematic

# Types of IDSs (cont)

- IDSs can also be classified according to their analysis
  - Misuse (signature-based) detection
    - Monitored activity is compared to set of signatures (patterns) for known attacks
    - Alarm if a signature matches

# Types of IDSs (cont)

- Anomaly (behavior-based) detection
  - Any behavior outside of a “normal profile” is considered suspicious
  - Typically statistical analysis

# Misuse Detection

- Most common approach
- Definition of signatures is critical
  - Too narrow or incomplete signatures will miss some attacks -- **false negatives**
  - Too broad signatures will raise false alarms -- **false positives**
- Unknown new attacks will likely be missed -- need constant updating

# Anomaly Detection

- Potential to detect new types of attack that are different from “normal” behavior
  - Very difficult in practice because normal behavior is hard to define
- Non-normal behavior may be suspicious but not malicious -- high **false positives** rate
  - Additional processing to identify malicious

# MANET Challenges for IDSs

- No natural points for monitoring (usually routers, firewalls, base stations, and other traffic concentration points in fixed networks)
  - Sensors may not see all traffic
- Hosts are more vulnerable to capture or compromise
  - Host-based IDS may be compromised

# MANET Challenges (cont)

- Hosts may be disconnected at times
  - Signature updates cannot be reliably distributed
- Dynamically changing topology makes centralized analysis and correlation difficult
  - Nodes must depend on own analysis

# IDS Functions Distributed

- Sensing
  - Each mobile host relies on own observations and cannot fully trust other hosts
- Analysis
  - Each mobile host relies on own analysis
- Response
  - Mostly independent but cooperation possible

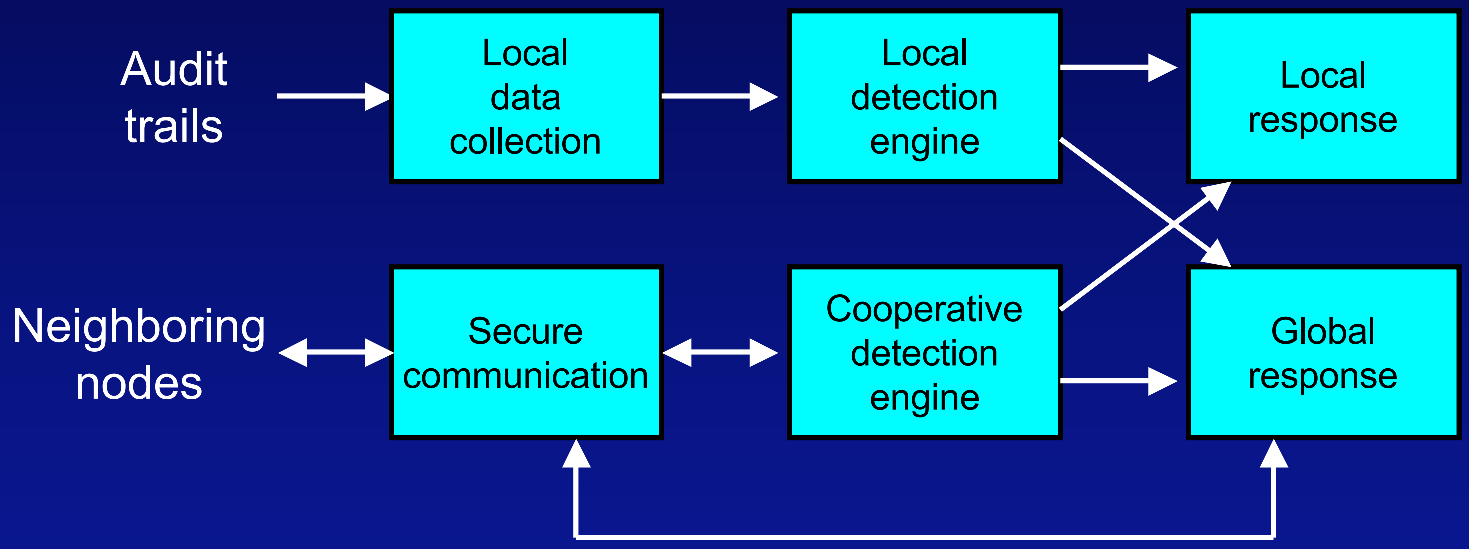
# Some Research Problems

- Most research focus on detecting and reacting to attacks by compromised nodes on ad hoc routing protocols
  - Interference with route discovery process
  - Advertisements of false routing information
  - Packet misrouting or dropping
  - Packet corruption is possible but protectable by cryptographic methods

# Basic Approach

- Each mobile node runs an IDS independently
  - Observes behavior of neighboring nodes
  - Looks for signs of intrusion locally
  - Makes decisions and takes actions independently
  - Can request data or actions from neighboring nodes if needed

# IDS Functional Model



# IDS Functions

- Data collection:
  - Collect local audit traces and activity logs
- Local detection engine:
  - Analyzes local data for anomalies
- Cooperative detection engine:
  - Requests data from other hosts if necessary

# IDS Functions (cont)

- Local response:
  - Alarms communicated to other nodes
- Global response:
  - Coordinated actions with neighboring nodes, triggered by any received alarms
- Secure communication:
  - Private, secure messaging with other hosts

# Interference with Routing

- False routing info could come from external attackers
  - Protectable by usual cryptographic authentication methods (digital signatures) to verify source identity of routing info
- More serious problem is false routing info or misrouting behavior from (internal) compromised hosts

# Routing Interference (cont)

- Verifying identity of internal host does not mean it can be trusted
  - Compromised hosts can own legitimate keys
  - Assume that compromised hosts will behave differently
  - Even if a node appears to be advertising invalid routing info, very hard to determine whether node is compromised or out of sync due to topology changes

# Approach to Detection

- General approach is to monitor behavior of neighboring nodes (sometimes called a “watchdog”) and rate their trustworthiness
  - Measure frequency of dropping or misrouting packets, or invalid routing info advertisements (open problem)
  - Rate trustworthiness of nodes

# Approach (cont)

- A “pathrater” keeps track of trustworthiness rating of every known node
  - Calculates path metrics by averaging node ratings in the path -- goal to avoid untrustworthy nodes
  - Other path metrics are possible, eg, exclude paths with untrustworthy nodes (open problem)

# Some Open Problems

- IDS accuracy is always critical issue
  - Most IDSs suffer from high rate of false positives or false negatives
  - Can misbehaving or compromised ad hoc nodes be identified reliably?
- When IDSs are so distributed in MANETs, and nodes cannot be trusted, can intrusion detection be guaranteed to work?

# Open Problems (cont)

  - Would like to use some kind of distributed trust model -- a majority consensus of nodes can be trusted
  - But if majority of mobile nodes are compromised, intrusion detection may fail

- Protection of IDS against attacks
  - Knowledgable attackers might defeat IDS by overloading, evasion, etc.