Securing Ad Hoc Wireless Networks

- Introduction
- Cryptography
  - Example
- IDS
  - Example1
  - Example2

Types of attacks:

Passive (affects confidentiality)

- eavesdropping

Active (integrity, non-repudiation, availability,freshness, and authentication)

- Deleting, modifying and injecting messages
- Jamming (DoS)
- energy exhaustion

Sources of attacks:

- Internal
- External

Security mechanisms: (two lines of defense)

Cryptography and authentication:

- prevention but no detection
- reduces attacks but does not eliminate them
- protects against some types of external attacks
- doses not work against malicious internal nodes

Intrusion Detection (ID):

- a second wall of defense
- detect and may prevent attacks
- works against both internal and external attacks

Example one

(cryptography and redundancy)

Secure Data Transmission in Mobile Ad Hoc networks (SMT)

Communication phases that need to be secured:

1. The route discovery
2. The data transmission

Two protocols compared for secure data transmission:

1. SMT (presented)
2. SSP (Secure Single Path) (for comparison)

SMT Assumptions:

1. Secure routing protocol
2. An initial trust between source and destination
   may be via public key cryptography
3. A shared finite field for purposes of data dispersion
   pre-computed set of columns

SMT description:

Source:

1. Discovers the Active Path Set (ASP) to the destination
2. Add redundancy to the massage
3. Disperse the message into multiple pieces
4. Guard the pieces with a MAC
5. Transmit each piece across a different route to the destination

Destination:

1. Set a timer upon reception of the first piece
2. Verify the integrity and authenticity of each received piece
3. Send a disperse and redundant feed back for each received piece

SMT Description …

Source:

1. A successful feedback means operational path
2. An unsuccessful feed back means broken or compromised path
3. Based on the feed back each path is given a rating

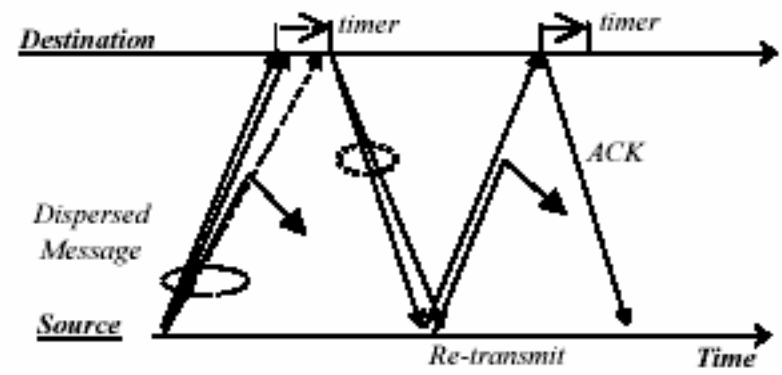
Destination:

1. Reconstruct the message if sufficient pieces are received or,
2. Ask for retransmission if timer runs out

Source:

1. Sets a counter for retransmission
2. Repeat retransmission trials until success or counter runs out

SMT description …



SMT message dispersion:

Raw data (message) is viewed as a stream of m-bit characters

divide the message into L messages each of length M

add padding if necessary

establish an M×L matrix (B)

Establish an N×M matrix (A), N>M

any M combination of rows are independent

row *k* of A = $\{1, u_k, \ldots, (u_k)^{M-1}\}$, u_k is random from field

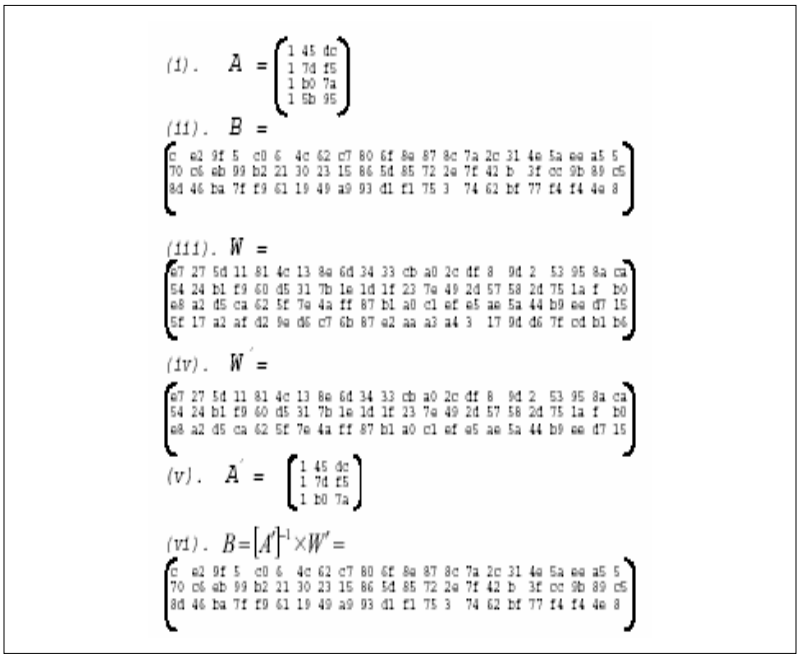
Each piece sent $w_i = a_i \times B$, a_i the ith row of A

If we receive M pieces ($v_1, \ldots, v_M$) each correspond to an a_i

establish an M×L matrix (W`)

establish from them an M×M matrix (A`)

$B = [A`]^{-1} \times W`$



APS adaptation:

Each path has short-term rating r_s and long-term rating r_l

r_s is increased by a constant β up to r_{max} with each success and decreased by a constant α down to r_{th} with each failure

r_l = successfully received / total sent

If either r_s or $r_l < r_{th}$, the path discarded

BWL (bandwidth loss) = failed/(success+failed) = f / (s+f)

All the constants are protocol selectable

Simulation results compared to SSP:

SMT delivers more messages

SMT has much lower end-t-end delay

The more static the network the worse the adversary effect for both SMT and SSP

Discussion:

Each source is assigned a fixed destination throughout the simulation !

The size of the buffer at the source is infinite !

The attacker drops all data packets it receives (very simple attacker) !

The attacker does not interfere with the routing traffic !

What about sensor networks ?

The overhead of multi-path discovery !

The overhead of the acknowledgment !

The overhead of pre-processing the data !

The overhead of redundant data !

The overhead of undetectable attacker !

Second Wall Of Defense

IDS

Classification of IDS:

Based on data collection mechanisms:

Host-based: OS audits and system and applications logs

Network-based: Packets captured from network traffic

Based on detection techniques:

Signature-based (misuse-detection) : Known attacks

Anomaly-based: deviation from normal behavior

Specification-Based: deviation from a set of predefined constraints

Classification of IDS …

Based on decision-making mechanisms

Collaborative

- \- prone to DoS and spoofed intrusion attacks (any malicious node can trigger full-forced response affecting the entire network)
- \+ the amount of information obtained about each node participating in the network is sufficient.

Independent

- \- the amount of information obtained is limited.
- \+ far less prone to spoofing attacks

Primary assumptions in IDS:

User and program activities are observable

Normal and intrusion activities have distinct behavior

IDS for Wired networks:

Distributed Probing

(e.g. a router detects neighboring routers)

Conservation of Flow:

Watcher runs on each router

Statistical Anomaly detection

Protocol Analysis:

Finite State Machine models that register the transition states of the protocol and alarms when anomalous state detected

General problems of IDS:

High Cost due to local management

Failure to exhibit scalability

Fine tuning requirements (based on particular system needs)

Need for frequent Database updates

Passive behavior (no decisions about the actions to be undertaken)

Why Wireless ad-hoc networks is more difficult?

Wireless communication (open media)

Cooperation among nodes is necessary (lack of centralized author.)

Don't rely on existing infrastructure

Have many operational limitations:

- Transmission Range and Bandwidth
- Energy, CPU, and Memory

Autonomous units capable of roaming independently

- easily captured and compromised without physical protection
- very expensive and not scalable if physically protected

Why Wireless ad-hoc networks is more difficult?

Usually used in situations where rapid deployment is necessary

Usually deployed in hostile (not physically protected) places

Dynamic topology change (due to mobility)

Lack of key concentration points (e.g. switches and routers)

No firewalls or gateways

Difficult to distribute and update signatures (detection database)

Questions to develop a viable IDS in Ad-hoc networks:

What is the good architecture ?

What are the appropriate audit data sources ?

How to model the activities to distinguish anomaly from normalcy?

Architecture of IDS in Wireless Ad-Hoc Networks:

Stand alone:

each node has an independent IDS

no cooperation or sharing between different nodes

Distributed and cooperative IDS:

each node has an independent IDS (local decisions)

cooperatively participate in global intrusion detection

Hierarchical IDS:

for multi-level ad-hoc networks

cluster heads / control nodes / main stations

IDS for wireless Ad-Hoc Networks:

Watchdog: (e.g. on DSR to verify that the next node forwards the packet)

Control Messages:

(e.g. adding two control messages to DSR;
CREP and CREQ)

Neighborhood watch:

either by listening to the transmission or observing route protocol behavior

Statistical Anomaly detection

IDS

Example1

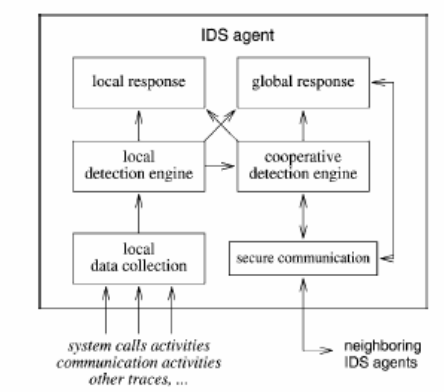
Intrusion Detection Techniques for mobile Ad Hoc Wireless Networks

ZHANG, LEE, HUANG

- The architecture
- The Model

Example…

The architecture



Architecture …

Data collection:

system and user activities within the mobile node

communication activities by this node

communication activities within the radio range

Local detection:

analyses local data traces

can use both misuse and anomaly detection

can initiate anomaly response if it has strong evidence

Architecture …

Cooperative detection

If the evidence is weak or inconclusive

Initiates a global detection procedure,

This procedure propagates intrusion detection state information among neighboring nodes

The passed state may be:

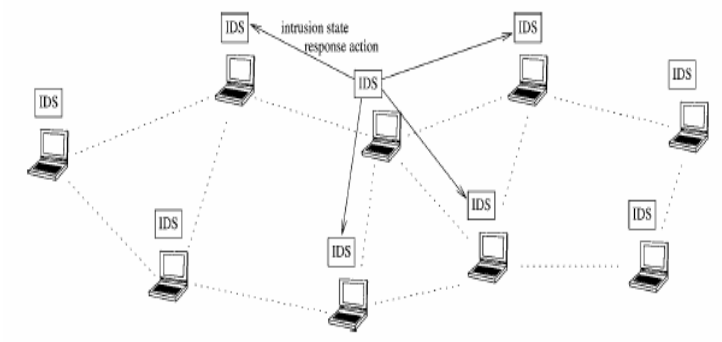
> a mere level-of-confidence value p% that there is anomaly or, a specific state that node A is compromised, or a complicated record including the complete evidence

Decision at each node is build based on majority opinion

Any node that detects anomaly can initiate a response

Architecture …

cooperative detection



Architecture …

Intrusion response:

Depends on:

- the type of intrusion,
- the type of network protocols and applications,
- and the confidence of the evidence

Could be (examples)

- reinitializing communication channels
- Identifying the compromised nodes and reorganize the network to exclude them

Anomaly detection model in mobile Ad-hoc networks:

Framework:

Uses entropy and conditional entropy to:

- describe the characteristics of normal and abnormal data flows

Uses classification algorithms to build the model

Details:

- select audit data with low entropy
- transform the data to construct high information gain features
- build classifier using training data
- apply classifier to test data
- post-process alarms to produce intrusion reports

Attack models:

Route logic compromise by manipulating routing information

- misrouting
- false route update

Traffic pattern distortion

- packet dropping
- generate packets with fake source address
- corruption on packet contents
- denial-of-service

Audit data:

- Local routing information
- Position locator or GPS

Classifier:

- RIPPER
  - applied directly to the feature space
- SVM Light (more accurate)
  - creates new features

Examples of used features:

PCR : the % of changed routes

PCH : the % of changes in the sum of hops of all the routes

VELOCITY: velocity

DISTANCE: distance from last log

RDC : relative distance change.

…

Protocols studied:

DSR

AODV

DSDV

Issues and Discussion:

Efficient Host-Based monitoring requires

- large amount of CPU processing power
- large a mount of energy

Efficient Network-Based monitoring requires:

- Traffic bottlenecks
- does not exit in wireless media
- Thus monitoring at every node is required!
- which is not bandwidth nor energy efficient

Anomaly based model

- built on a long-term monitoring

Issues and Discussion …

Ad-hoc may not have sufficient life time to do so

mobile networks are very dynamic in structure (hard to build a reliable normal behavior)

Misuse requires

extensive database of attack signatures

must be replicated among all nodes

Another Example on IDS

Effective Intrusion Detection Using Multiple Sensors in Ad Hoc Wireless Networks

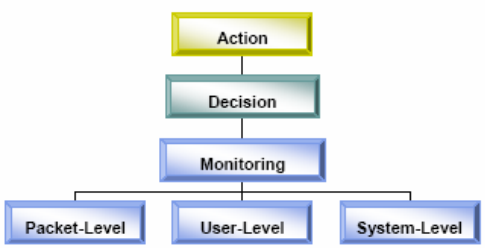
Paper contributions:

Restrict the computation intensive Analysis to a few nodes

A protocol to dynamically select cluster heads

A Selected cluster collect packets within its communication Range

Modular architecture



Modular Architecture:

Network monitoring

- only certain nodes have these agents
- network packet monitoring

Host monitoring

- every node has this agent
- monitors the node itself (system and application activities)

Decision Making

- every node decides locally on intrusion levels it detect
- certain nodes collect intrusion alarms and make collective decision

Action : every node will have an action model

References:

Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, MobiCom'2000, pp. 275-283.

O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad-Hoc Networks", Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03).

O. Kachirski and R. Guha, "Intrusion Detection Using Mobile Agents in Wireless Ad-Hoc Networks", Proceedings of the IEEE Workshop on knowledge media networking.

"Intrusion detection techniques for mobile wireless networks", Yongguang Zhang, Wenke Lee, Yi-An Huang. In Wireless Networks Journal, September 2003.

"Secure routing: Secure data transmission in mobile ad hoc networks", Panagiotis Papadimitratos, Zygmunt J. Haas. In ACM Workshop on Wireless Security, September 2003.

"Securing ad hoc networks", L. Zhou, Z.J. Haas. In IEEE Network, Nov-Dec 1999.