# Modeling and Detection of Network Attacks

George Papageorgiou, Alvaro Cardenas, Huigang Chen, Jia Shiang Zhou, George Theodorakopoulos, John S. Baras

## Worm Spreading

**Worm Characteristics**
The worm periodically picks an IP address at random and sends the worm packet (over UDP). If the receiver host is vulnerable to the attack, it is infected and starts spreading the worm.

**Worm Spreading Simulation Scenario**
•Pareto background data traffic
•Four phases:
- Attack is initiated by a host at time 6sec.
- Shortly, all the vulnerable nodes are infected. The attack is detected in the routers and filtering is initiated at the routers, based on the volume traffic.
- After 4sec all the worm packets are filtered in the routers.
- After 6sec the infected hosts are rebooted and "patched". The network returns to a near-normal condition (some false alarms).

## Distributed Denial of Service

**Distributed Denial of Service (DDoS)**
In a DDoS an attacker compromises a set of Internet hosts and installs a small attack daemon on each host, producing a group of "zombies". Using this basic setup an attacker can generate a coordinated attack from several zombies installed across different AS boundaries, onto a single site, causing excessive amounts of endpoint and possibly transit network bandwidth to be consumed.

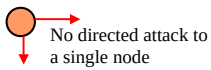
**DDoS Simulation Scenario**
•We monitor a transit network connecting different subnetworks
•Pareto background data traffic
•The attack starts at 10s. It is simulated by a given number of compromised nodes in different subnetworks. During the attack, each of these nodes will start a constant bit rate connection towards a specific node.
•The detection statistics are checked for directionality and correlation in order to reduce the false alarm rates.

## Detection Statistics for Large-Scale Attacks

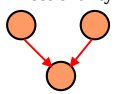
**Change Detection Statistics: Detection of the attack early in its development.**
- Parametric and non-parametric sequential statistics are applied to detect changes in the mean of the packet arrival process (DDoS) and the arrival process to a given port number (Worm).

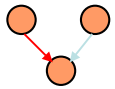
**Reducing False Alarms for DDoS**
- basic idea: at each highly connected node, the data tends to aggregate from the distributed sources towards the destination, giving a sense of "directionality" to the attack, so we have 2 steps for detecting the attack early in its development:

1. **Directionality - Single link:** Only routers with outdegree detection of 1 are considered:

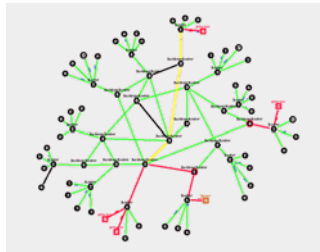

2. **Directionality – Correlation:**

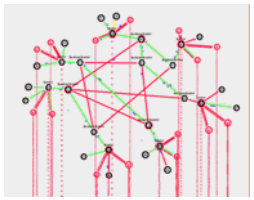



## Simulations

The alarm pattern for a distributed denial of service attack forms a tree in the monitored graph





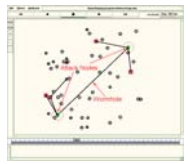
Worm packet filtering after detection

## Wireless Attack: Wormhole

**Scenario**

- **Mobility:** Nodes move according to the Manhattan grid model which resembles movement in urban environments.
- **MAC:** IEEE802.11, 2Mbps shared media.
- **Routing Protocol**: DSDV.
- **Attack:** An attacker records packets at one location of the network and tunnels them to a colluding attacker. At the end of the tunnel certain packets are retransmitted into the network.

Before Attack



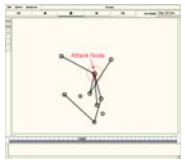
After Attack

## Wireless Attack: Route Falsification

**Scenario**

- MAC: IEEE802.11, 2Mbps shared media.
- Routing Protocol: DSDV.
- **Attack:** One compromised node routinely sends out fake route update message in which claims he is one hop away from every node he knows. So other nodes will try to send data to him to reach their destinations.
- **Detection:** A dynamic model of the hop count distribution is built using multiple HMMs. An abnormality in the model is flagged as an attack detected.
- **Defense:** All nodes start rerouting to "clean" their routing table and disregard the route update message from the attack node.

Before Attack



After Attack