Detecting Denial of Service Attacks

Carla Brodley
Clay Shields
Long Fei
Karthik Jaganathan
Electrical and Computer Engineering
Computer Sciences

CERIAS
Purdue University

Denial of Service

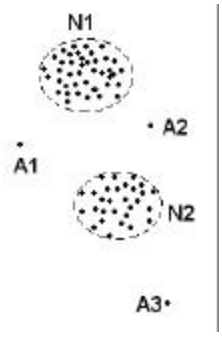
- Attacker tries to prevent legitimate users from gaining access to services by consuming resources
- Examples: Syn flooding, Smurf, Fraggle, fragmentation attacks

Goal: Automatic Detection

- Problem:
  - No reliable DoS detection mechanism
- Current methods:
  - Limited signature based detection
  - Manual scanning of huge logs - looking for a needle in a haystack
- Proposed method: Anomaly detection - deviations from normal patterns might potentially signal DoS

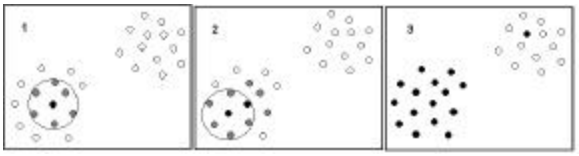
Anomaly Detection Method

- **Outlier:** an observation that deviates significantly from other observations, arousing suspicion that it was generated by a different mechanism.
- **Approach:**
  - Cluster normal traffic
  - Hypothesis: attack data will be outliers
  - Example: N1 and N2 are normal clusters; A1 ~ A3 are outliers

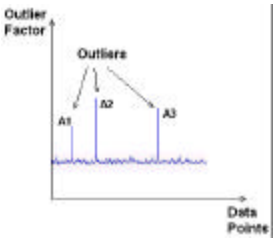


Outlier Identification Method

- DBSCAN: A nonparametric method that uses density to define clusters



- OPTICS-OF ~ Decides which points are too far away from clusters

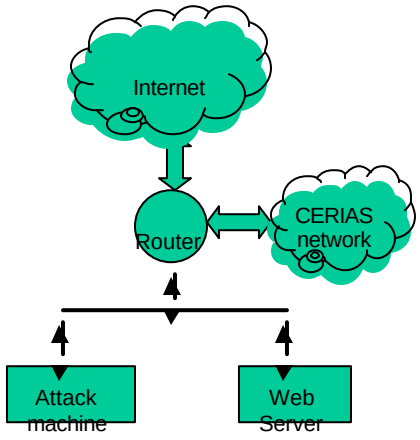


Ester, M., Kriegel, H. P., Sander, J., Xu, X. 1996. A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise. *Proc. of The Second Internal Conference on Knowledge Discovery & Data Mining*, Portland, OR, 1996, pp226-231

Breunig M. M., Kriegel H.-P., Ng R., Sander J.: *OPTICS-OF:* Identifying Local Outliers, *Proc. Conf. on Principles of Data Mining and Knowledge Discovery* , Prague, 1999, in: Lecture Notes in Computer Science, Springer, Vol. 1704, 1999, pp . 262-270.

Data Collection

- Collected real-world data from CERIAS web server
- Attacks conducted on the production network for realistic data
- *Tcpdump* traces of the traffic collected



Traffic Features Collected

- Mean and standard deviation of the inter-arrival time over various window sizes
- IP features
  - source IP address
  - destination IP address
  - protocol
  - fragmentation offset
  - checksum
- Higher layer features
  - ports
  - TCP flags
  - proportion of protocols in traffic

Preliminary Results

- With feature selection, we are able to detect single attacks (some examples):

- DBSCAN

Type of Attack	False Acceptance%	False Alarm%
TFN-ICMP	0	12.98
teardrop	0	1.61

- OPTICS-OF

Type of Attack	False Acceptance%	False Alarm%
TFN-ICMP	0	3.713
teardrop	0.429	4.040