Privacy-Preserving AIS for Network Security

Karthik S
Chandan Yeshwanth

February 9, 2016

Desired System Properties

- Self-behaviour for a node: valid connections that it receives
- Self-behaviour of individual nodes used to develop common set of detectors
  - This is done without revealing self-behaviour
- Once tolerized, an anomalous connection can be detected without revealing it

System Model

- n nodes/parties in a fully connected network
- At least t nodes required to reconstruct shared values
- Failure-free and non-malicious nodes (no deviation from protocol)

Approach

- Generate random secret-shared set of detectors
  - Each node contributes its share of randomness
- Tolerize generated set by using secret-shared self-antigens from each node
  - Use privacy-preserving affinity function to check for matches without revealing additional information
- Use trained, secret-shared detectors to identify secret-shared anomalous connections

Feedback Received

- KDD dataset: reliable, widely used in academic studies
- Implementation: make sure possible
- Computational efficiency: not very important as this is a theoretical framework
- Ensure properties of both systems, i.e, AIS and privacy-preserving computation mechanism, are conserved