Privacy-Preserving AIS for Network Security

Karthik S
Chandan Yeshwanth

February 18, 2016

Notation

- Each detector as well as incoming connection has an l-bit binary representation
- Each detector denoted as a vector of its bit representation:$\vec{d_i} = [d_{i1}, d_{i2}, \ldots, d_{il}]$
- Secret sharing scheme : additive and bitwise
- Bitwise secret sharing of $\vec{d_i}$ denoted by $[\![\vec{d_i}]\!] = [[\![d_{i1}]\!], [\![d_{i2}]\!], \ldots, [\![d_{il}]\!]]$

Detector construction

- Let q, l, n be the initial number of detectors, encoding bit length and number of parties respectively
- Let $u = n/q$
- P_i generates a random set of detectors $D_i = \{\vec{d}_{i1}, \vec{d}_{i2,}, \ldots, \vec{d}_{iu}\}$
- P_i then bitwise secret shares $d \in D$ among other parties
- At the end of the random detector construction phase each party has shares of q bit-wise additive secret shared detectors, i.e., $\{[\![\vec{d}_1]\!], [\![\vec{d}_2]\!], \ldots, [\![\vec{d}_q]\!]\}$

Next Steps

- Define the actual secret-sharing scheme to be used
- Describe the black-box affinity function
- Tolerize random set of detectors on shared self-behaviour using affinity function