The data set includes the settings from EigenTrust paper by Sepandar D. Kamvar, Mario T. Schlosser and Hector Garcia-Molina (2002).

For the threat models A, B, C, D; the sets include one trace file per setting. 36 different trace services in total. Each is randomly generated and the generator seeds are given in the trace file header. Although they not read by the TraceSimulator, the service popularities and the neighbor list of the nodes are given for the users.

The traces are generated using TraceGenerator submodule.

The service request distributions follow zipf distribution. The connection network is a power-law network.

For each trace file, the corresponding simulation results are given in the files with respective extensions for No-Trust (.none), EigenTrust (.eigen), PeerTrust (.PeerTrust), TNA-SL (.tnasl), M2MTrust (.M2MTrust)

The Simulations are run using the TraceSimulator submodule. The TraceSimulator runs the Trust Model’s feedback functions after each transaction and runs the propagation procedure with certain intervals (such as once per 20 transactions, etc.)

The specific settings for each attack model are given below.

***Thread Model A (Independently Malicious):***

Malicious nodes always provide bad services and dishonest ratings.

SETUP

* 60 + %x Nodes (60 to 200)
* %x of total machines is malicious.
  + 0% up to 70% (8 instances)
* 3 Pre-trust Nodes
* 20 Services
* 1500 Transactions (750 Warmup Transactions)
* Connection Network
  + Good Nodes have at least 2 neighbors
  + Malicious Nodes have 10 neighbors
  + Pre-Trust Nodes have 10 neighbors
* 0.4 Zipf Constant

***Threat Model B (Malicious Collectives):***

Malicious nodes always provide bad services and form a malicious collective to get high ratings.

SETUP

* 60 + %x Nodes (60 to 200)
* %x of total machines is malicious.
  + 0% up to 70% (8 instances)
* 3 Pre-trust Nodes
* 20 Services
* 1500 Transactions (750 Warmup Transactions)
* Connection Network
  + Good Nodes have at least 2 neighbors
  + Malicious Nodes have 10 neighbors
  + Pre-Trust Nodes have 10 neighbors
* 0.4 Zipf Constant

***Threat Model C (Malicious Collectives with Camouflage):***

Malicious nodes provide good service in f% time but dishonest ratings always and form a malicious collective.

SETUP

* 73 Nodes
* 20 Malicious Nodes
* Malicious Nodes provide authentic services f% of the time. (0% - 90%; 10 instances)
* 3 Pre-trust Nodes
* 20 Services
* 1500 Transactions (750 Warmup Transactions)
* Connection Network
  + Good Nodes have at least 2 neighbors
  + Malicious Nodes have 10 neighbors
  + Pre-Trust Nodes have 10 neighbors
* 0.4 Zipf Constant

***Threat model D (Malicious spies):***

Two types of Malicious nodes: (i) malicious collectives; (ii) Spy nodes that provide good services but dishonest ratings.

SETUP

* 103 Nodes
* 40 Malicious Nodes total
  + Threat Model B + D together (10 instances)
  + 40-0; 39-1; 36-4; 35-5; 30-10; 25-15; 20-20; 15-25; 10-30; 5-35
* 3 Pre-trust
* 20 Services
* 1500 Transactions (750 Warmup Transactions)
* Connection Network
  + Good Nodes have at least 2 neighbors
  + Malicious Nodes have 10 neighbors
  + Pre-Trust Nodes have 10 neighbors
* 0.4 Zipf Constant