Aditya Vutukuri

A Reputation-Based Trust Management System for P2P Networks

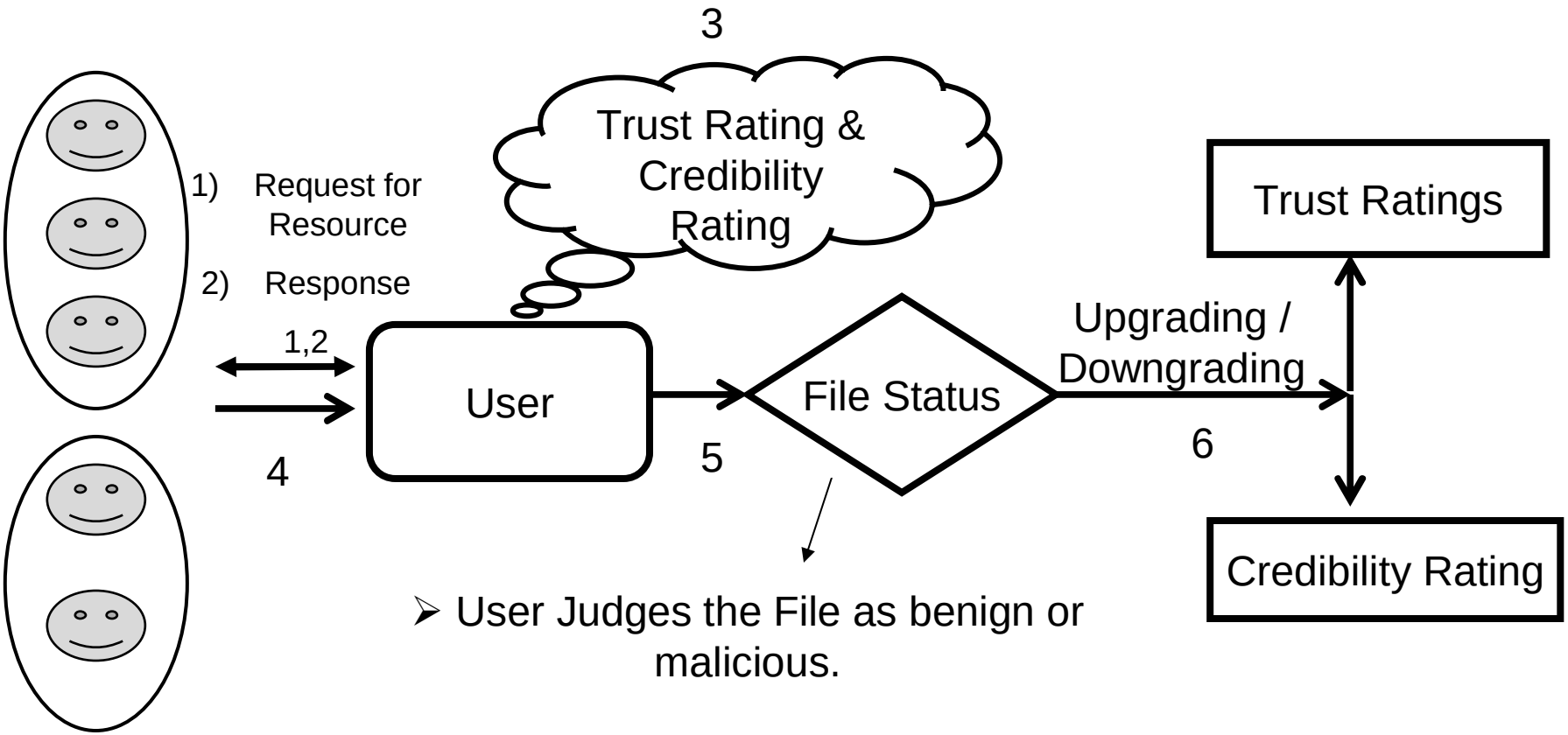
Ali Aydin Selçuk Ersin Uzun Mark Reşat Pariente

Department of Computer Engineering
Bilkent University

Summary

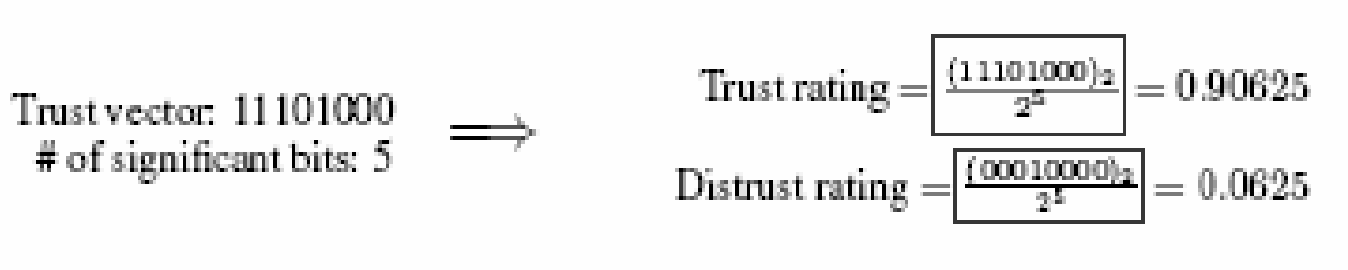
- The aim of this protocol is to distinguish the malicious responses from benign ones by using the reputation of the peers providing them and thus preventing the malicious peers from spreading malicious content.
- In reputation based systems, this is done by:
  1) Considering the Information provided by third parties on the queried peer.
  2) And thus track their performance to predict their future behavior.

General Working of the Protocol



Critical Comments

Few mistakes in the article



Trust rating = $(11101)_2/2^5 = 0.90625$

Distrust rating = $(00010)_2/2^5 = 0.0625$

[10] A. A. Selçuk, E. Uzun, and M. R. Pariente. Reputation-based trust management for P2P networks. Technical Report BU-CE-0402, Department of Computer Engineering, Bilkent University, 2004.

BU-CE-0403

Critical Comments

In case of Queried trust score formula:

$$\frac{\sum_{i=1}^{k} c_i t_i}{k} \longrightarrow \frac{\sum_{i=1}^{k} (c_i - d_i) t_i}{k}$$

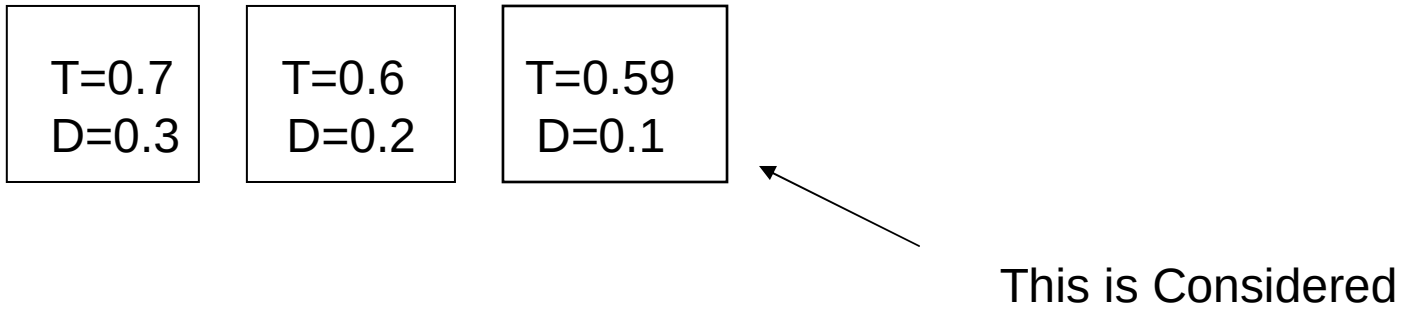
Where d_i is discredibility rating

Appreciative Comments

- Separate Handling of Trust and Distrust Rating and more importance is given to distrust rating.
- In the end of evaluation, the file versions are sorted by “min-distrust-max-trust” criterion.

for example

Let T denote trust rating and D denote distrust rating of a peer.



Attackers Considered in the simulation

- naive: responds to every query with a malicious version
- hypocritical: mostly acts reliable but occasionally sends malicious version
- collaborative: collaborate with each other in trust query and express positive opinion for malicious peer and negative opinion for others
- pseudospoofing: changes pseudonym periodically to escape recognition

Question

- How much time does it take for a user to detect an attack i.e. detect a malicious file?

- And what is the seriousness of pseudospoofing attack with collaborators scenario?

i.e. pseudospoofing peers are supported by a group of “collaborators” who normally act as trustworthy peers but give their strongest support to the malicious peers when they receive a relevant trust query.

Queries ?