# A Reputation-Based Trust Management System for P2P Networks

Author: Ali Aydin Selcuk, Ersin Uzun, Mark Resat Pariente
Department of Computer Engineering
Bilkent University
Ankara, 06800,Turkey
Email:selcuk@cs.bilkent.edu.tr, feuzun,resatg@ug.bilkent.edu.tr

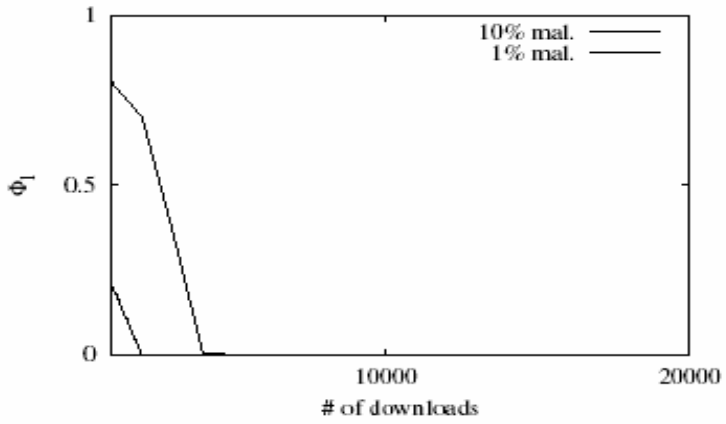
# Summary

- The author developed a reputation - based trust management protocol for P2P networks to identify malicious peers and to prevent the spreading of malicious content.The protocol is based on the query-response architecture of the first generation P2P network.

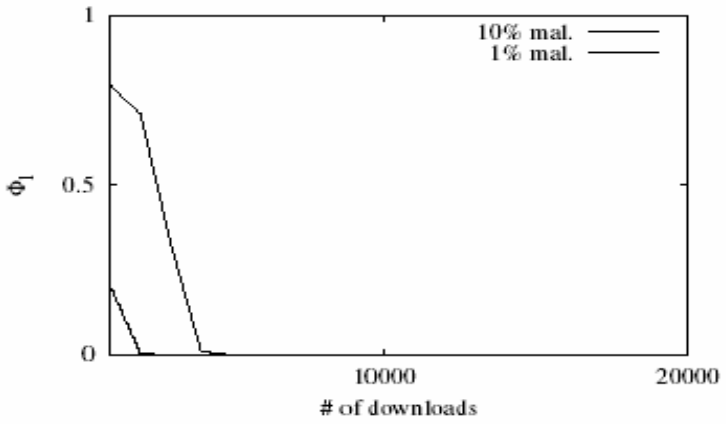
# Four kinds of attackers considered in the simulations are,

- Naïve: who responds to every query with a malicious version of the requested file
- Hypocritical: who acts like a reliable peer most of the time but occasionally tries to send a malicious file
- Collaborative: who collaborate with each other in trust queries,expressing a positive opinion for malicious peers and a negative opinion for others
- Pseudospoofing: who change their pseudonym periodically to escape recognition(this attackers are the hardest to detect and their prevention is possible only after honest peers build a sufficient level of trust among themselves)

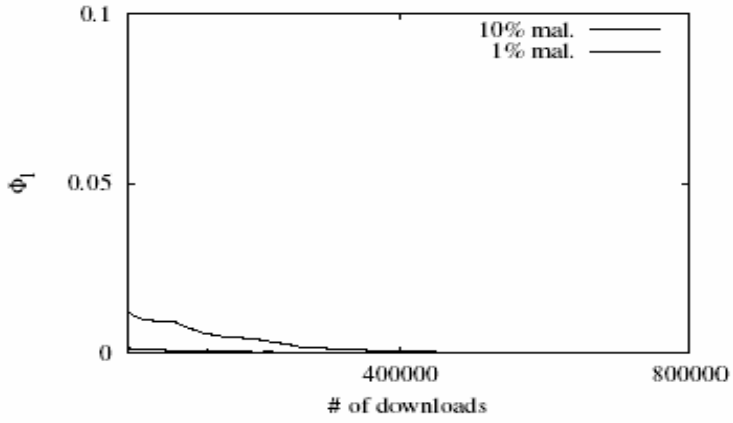
# Simulation results



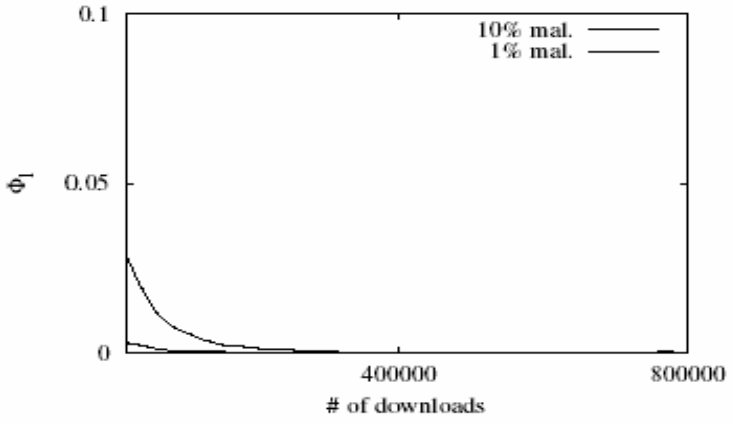

(a) Naive




(b) Collaborative

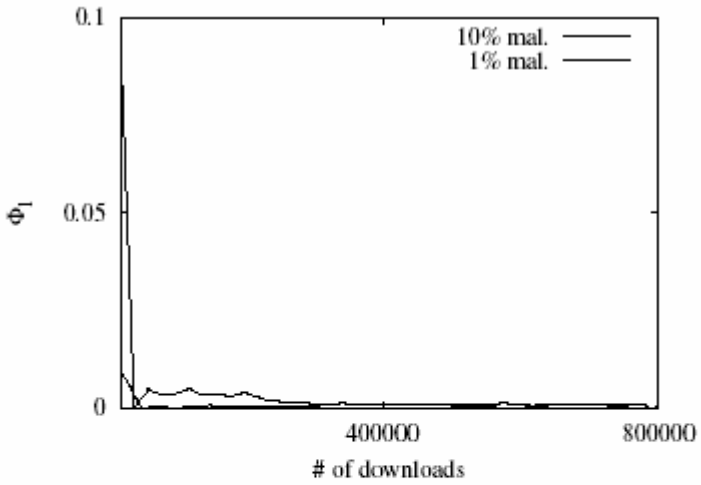



(c) Hypocritical, 10% cheating

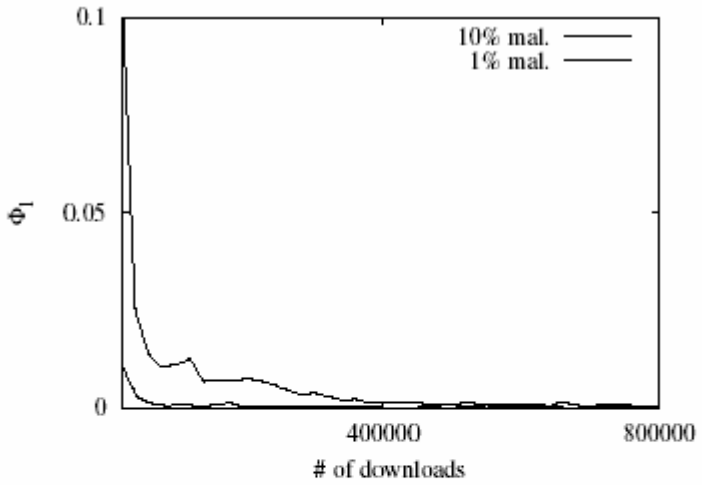



(d) Hypocritical, 25% cheating

# Simulation results(cont.)



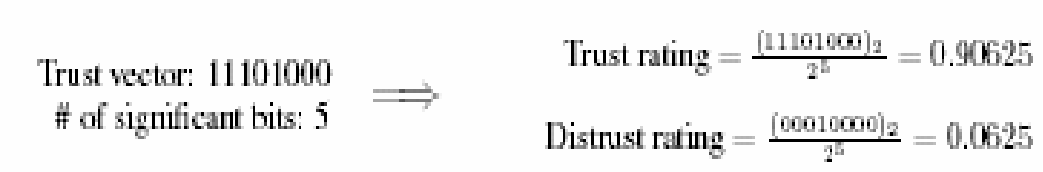

**(e)** Pseudospoofing, at 250 iqt




**(f)** Pseudospoofing, at 100 iqt

**Figure 4:** A graphical summary of the simulation results. Naive attackers can be detected and contained quite rapidly. Hypocritical attackers, operating at a much lower effectiveness level, can evade detection longer; but their activity is also contained once a sufficient level of trust is established among the good peers. Pseudospoofing attackers are also able to continue spreading malicious content for a while but become ineffective as the good peers establish trust among themselves. Collaboration does not seem to be a significant source of benefit to naive attackers.

➢One minor mistake in this article:




It should be: Trust rating=$(11101)_2/2^5$=0.90625

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

The result is correct

# Comment

- The author designed a well organized structure for his protocol, and described its details in a quite clear way.

# Comment(cont.)

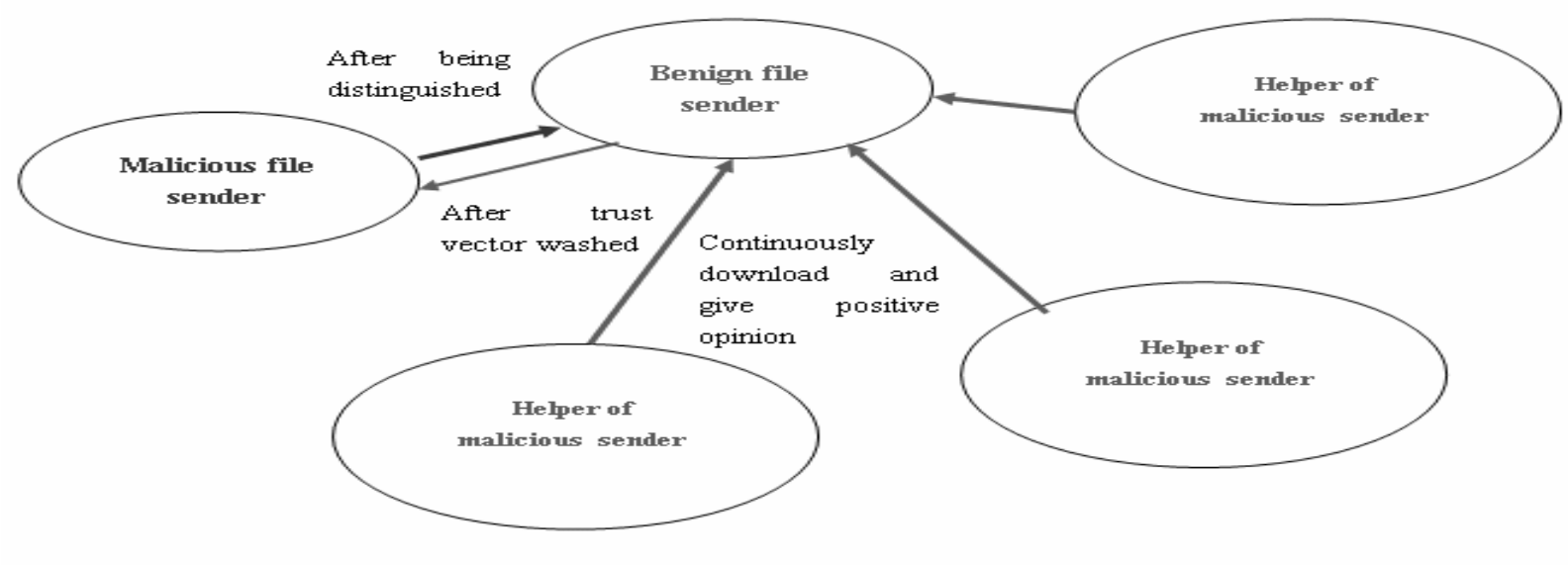
- The presumption of the protocol is that users can correctly find out attack in time. In that case, the protocol can reduce the risk of Naive, Collaborative, Hypocritical and Pseudospoofing attack.

  The author claimed that many attacks in P2P systems are discernible by the user. However, since there are lots of malicious viruses which have latent period can not be detected by users at once, and no one can promise that the attackers of P2P system will not use or develop such kinds of malicious files. So in my opinion the presumption of the author is not sufficient.

# Comment(cont.)

- Even if the presumption that users can correctly find out attacks in time is satisfied, future attackers still can easily develop a scheme to overcome it.

# One possibility of future attackers(combination of hypocritical,collaborative and pseudospoofing attackers )



# Explanation

In this protocol,if the helper directive give the malicious file sender positive opinion,it will downgrade the helpers credibility rate too.It is the way to prevent collaborative attack in this protocol. However, if the attacker use the hypocritical way and the helpers continuously down load and give positive opinions when attacker in the benign file sender state, they can bypass part the restrict of the protocol and recover malicious file sender in a short period. Then the attacker can attack users again other than those who were hurt already. Because those helpers only give positive opinions to the benign files, they can gain higher credibility rate than those who were cheated. When quite a lot of users were hurt, they can change their pseudonym and established their reputations quickly by sending and downloading benign files with each other and other users.

# Conclusion

- Although the system itself is well organized, in my opinion, it can not resist attackers in a p2p environment.

# Question

- Do you think that we can really prevent malicious attackers in an anonymous environment by reputation?

# My answer

- In my opinion, the answer is no. Let’s look at the following examples,
- Will a bank issue a credit card just by the name given by the customer himself without any credential files like passport or driver license? (The bank can also reject that person if he cheat once. But the cheater can change his name and cheat again. )
- If you were the attacker, would you like the idea that sending somebody 100 benign files and then put one backdoor file in his computer? (Sending 100 benign files will cost you no much money,but with the backdoor file, maybe you can find the credit card number, secrete files … ☺)
- Do you agree with me now?

# Thanks