

Trust But Verify : A Framework for the Trustworthiness of Distributed Systems

¹ M Vineela, ² Shreya Patthi, ³Talla Sai Vaishnavi

¹Associate Professor, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India

^{2,3}Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India

ARTICLE INFO

Article History:

Accepted: 01 July 2023

Published: 10 July 2023

Publication Issue

Volume 9, Issue 4

July-August-2023

Page Number

102-105

ABSTRACT

Distributed networking technologies have gained popularity as a mechanism for users to share files without the need for centralized servers. A Distributed network provides a scalable and fault-tolerant mechanism to locate nodes anywhere on a network without maintaining a large amount of routing nodes. This can allow for a variety of applications beyond simple sharing of file. This includes multicast systems, and communication systems, and caches of web. We survey security issues that occur in the underlying Distributed routing protocols, along with fairness and trust that occur in file sharing and other Distributed systems. Here we discuss how techniques, ranging from cryptography techniques, to randomize network guessing, can be used to address these problems. Open nature of Distributed systems exposes them to malicious activity. Defining trusty relationships among peers can mitigate attacks of malicious peers. This paper presents distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions. System peers create their own trust network in their proximity by using local information available and do not try to learn global trust information. Two contexts of trust context, service context, and recommendation, these are defined to measure trustworthiness in providing services and giving recommendations. These recommendations are derived based on priority, history, and peer satisfaction. Moreover, nodes trustworthiness and confidence about a recommendation are considered while evaluating recommendations. Effective experiments on a file sharing application show that the proposed model can mitigate attacks on 16 different malicious behavior nodes.

Keywords : Distributed Systems, Trust Management, Reputation, Security, Cryptography

I. INTRODUCTION

Distributed systems rely on collaboration of peers to complete tasks. Way of performing malicious activity is a threat for security of distributed network. Creation of trust relationships among peers can provide a more secure environment by reducing risk and uncertainty in future distributed interfaces. But, creating a trust relationship in an unknown entity is difficult in such a malicious system. The trust maintenance is a social concept and it is hard to measure with numbers. It requires matrix to represent trust in mathematical models. The peers are classified as either trustworthy or untrustworthy is not sufficient in all cases. These metrics should have functionality depending upon which peers can be ranked according to trustworthiness. Peer satisfaction and feedbacks of peers provide information to measure trust among peers. Peer satisfaction provides some useful information about the communicating peer but feedbacks might contain deceptive information.

A central server is a traditional way to store and manage trust data of peers, e.g., eBay. These servers centrally and securely stores trust data and evaluate trust metrics. As in most distributed systems there is no central server, so peers organize themselves to store and evaluate trust information about each other [1], [2]. Management of trust data is dependent to the structure of system network. The distributed system uses hash table based methodologies; each peer becomes a trust information holder by storing feedbacks and interaction about other peers [1], [3], [4].

We present a self-organizing trust model (sort) which focuses to reduce malicious activity in a peer to peer distributed system by maintaining trust relations among peers in their surroundings. In this system peers do not try to collect trust information from remaining all peers. Here every peer develops its own local computation of trust about the peers interacted in the past. Like this, good peers form dynamic trust groups evaluated in their surroundings and can remove malicious peers from system. As peers generally tend to

interact with a small set of peers [7], forming trust relations in region of peers helps to overcome attacks in a distributed system.

SORT generally based on three trust metrics. First one is reputation metric which is calculated based on recommendations of peers. It is important while deciding strangers and new nodes among all peers. Second, service trust metrics and recommendation trust metrics which are primary metrics to compute trust relation in the service and recommendation surroundings. The service trust metric is used while deciding service providers. The recommendation trust metric is used while requesting recommendations. While we are evaluating the reputation metric, recommendations are calculated on the basis of recommendation trust metric.

II. RELATED WORK

Most existing distributed systems are built on traditional security models, including the two most widely used models the mandatory access control (MAC) and the discretionary access control (DAC) models [5]. While these models aim at the enforcement of access control of system resources, they are not concerned about the system utility on which they do have a direct impact. This is because malicious behaviours can happen even after the authorization stage [9].

The notion of utility and its application in distributed computing is not new. Marsh introduced the notion of utility as a member of a set of input parameters used for constructing his trust model for distributed systems, where utility was actually used as one of the input parameters for the trust calculation used for cooperation decisions [14]. The notions of utility and trust have also been used by other researchers in security context for grid based computing [13].

However, risk management has not been considered in these Studies. Sonntag. Have proposed a payment based scheme for mobile agent based e-commerce applications. In this scheme utility is considered.

Depending on the trustworthiness of the requesting entity, different prepaid amounts may need to be submitted by the agent's home server to the remote server in order to gain access which otherwise could not be granted. The prepaid amounts are set to be more than the lost caused by any potential malicious behaviours. This proposal has introduced the notion of dynamic authorization in a sense that permissions to agents are granted according to the trustworthiness of the agent and these permissions demand prepayments to insure against potential damages (utility loss). However this scheme does not deal the utility maximization explicitly. A formal model of trust based on sociological foundations is defined by Marsh [11]. In this model, an agent uses own experiences when building trust and does not consider information of other agents. Abdul-rahman and Hailes' trust model [3] evaluates trust as an aggregation of direct experience and recommendations of other parties. Trust metrics are defined in discrete domain. A semantic distance measure is defined to test accuracy of recommendations. Zhong [13] proposes a dynamic trust concept based on McKnight's social trust model [12]. Uncertain evidences can be used when building trust relationships. Second-order probability and Dempster Shaferian framework helps in evaluating uncertain evidences. Reputation is first used as a method of building trust in e-commerce communities. Resnick et al. [1] point out limitations and capabilities of reputation systems. Ensuring long-lived relationships, forcing feedbacks, checking honesty of recommendations are some difficulties in reputation systems. Dellarocas [2] explains two common attacks on reputation systems: unfairly high/low ratings and discriminatory seller behavior. Controlled anonymity and cluster filtering methods are proposed as countermeasures. Despotovic and Aberer [10] study an online trade scenario among self-interested sellers and buyers. Trust-aware exchanges can increase economic activity since some exchanges may not happen without trust establishment. Terzi et al. [2] introduces an algorithm to classify users and assign them roles based

on trust relationships. Yu and Singh's model [12] propagates trust information through referral chains. Referrals are the primary method of developing trust in others. Mui et al. [14] propose a statistical model based on trust, reputation and reciprocity concepts. Reputation can be propagated through multiple referral chains. Jøsang et al. [4] discusses transitivity of trust with referrals. Recommendations based on indirect trust relations may cause incorrect trust derivation. Thus, trust topologies should be carefully evaluated before propagating trust information.

III. PROPOSED SYSTEM

We define secure routing and outline our solution. Throughout this paper, most of the analyses and techniques are presented in terms of this model and should apply to other structured overlays except when otherwise noted. We define an abstract model of a structured Distributed routing overlay, designed to capture the key concepts common to overlays such as CAN, Chord, Tapestry and Pastry. The protocol routes messages with a given key to its associated root. To route messages efficiently, all nodes maintain a routing table with the node IDs of several other nodes and their associated IP addresses. Moreover, each node maintains a neighbour set, consisting of some number of nodes with node IDs nearest itself in the id space. Pastry node IDs are assigned randomly with uniform distribution from a circular 128-bit id space. Given a 128-bit key, Pastry routes an associated message toward the live node whose node ID is numerically closest to the key. Each Pastry node keeps track of its neighbor set and notifies applications of changes in the set.

Secure routing ensures that (1) the message is eventually delivered, despite nodes that may corrupt, drop or misroute the message; and (2) the message is delivered to all legitimate replica roots for the key, despite nodes that may attempt to impersonate a replica root. Secure routing can be combined with existing security techniques to safely maintain state in

a structured Distributed overlay. For instance, self certifying data can be stored on the replica roots, or a Byzantine-fault-tolerant replication algorithm [10] can be used to maintain the replicated state. Secure routing guarantees that the replicas are initially placed on legitimate replica roots, and that a lookup message reaches a replica if one exists. Similarly, secure routing can be used to build other secure services, such as maintaining file metadata and user quotas in a distributed storage utility. The details of such services are beyond the scope of this paper.

IV. CONCLUSION

Individual, collaborative, and pseudonym changing attackers are studied in the experiments. Damage of collaboration and pseudo spoofing is dependent to attack behavior. Although recommendations are important in hypocritical and oscillatory attackers, pseudos' proofers, and collaborators, they are less useful in naive and discriminatory attackers. SORT mitigated both service and recommendation-based attacks in most experiments. However, in extremely malicious environments such as a 50 percent malicious network, collaborators can continue to disseminate large amount of misleading recommendations. Another issue about SORT is maintaining trust all over the network. If a peer changes its point of attachment to the network, it might lose a part of its trust network. These issues might be studied as a future work to extend the trust model.

V. REFERENCES

- [1]. K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM), 2001. R. Caves, *Multinational Enterprise and Economic Analysis*, Cambridge University Press, Cambridge, 1982. (book style)
- [2]. F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a DISTRIBUTED Network," Proc. 11th World Wide Web conf. (WWW), 2002.
- [3]. S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in DISTRIBUTED Networks," Proc. 12th World Wide Web Conf. (WWW), 2003.
- [4]. L. Xiong and L. Liu, "Peertrust: Supporting Reputation-Based Trust for Distributed Ecommerce Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 004
- [5]. B. Yu and M. Singh, "A Social Mechanism of Reputation management in Electronic Communities," Proc. Cooperative Information Agents (CIA), 2000
- [6]. Z. Despotovic and K. Aberer, "Trust-Aware Delivery of Composite Goods," Proc. First Int'l Conf. Agents and Distributed Computing, 2002
- [7]. F. Cornelli, E. Damiani, S.C. Vimercati, S. Paraboschi, and P. Samarati, "A reputation-based approach for choosing reliable resources in Distributed networks," In CCS02, Washington DC, USA 2002.
- [8]. K. Aberer, A. Datta, and M. Hauswirth, "P-Grid: Dynamics of Self-Organization Processes in Structured DISTRIBUTED Systems," Distributed Systems and Applications, vol. 3845, 2005.
- [9]. R. Zhou and K. Hwang, "Powertrust: A Robust and Scalable Reputation System for Trusted Distributed Computing," IEEE Trans. Parallel and distributed Systems, vol. 18, no. 4, pp. 460-473, Apr. 2007.
- [10]. M. Gupta, P. Judge, and M. Ammar, "A Reputation System for Distributed Networks," Proc. 13th Int'l Workshop Network and Operating Systems Support for Digital Audio and Video (NOSSDAV), 2003.

- [11]. S. Staab, B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, M. Sloman, T. Dillon, E. Chang, F.K.Hussain, W. Nejdl, D. Olmedilla, and V. Kashyap, "The Pudding of Trust," IEEE Intelligent Systems, vol.19, no. 5, pp. 74-88, 2004.
- [12]. M. Virendra, M. Jadliwala, M. Chandrasekaran, and S.Upadhyaya, "Quantifying Trust in Mobile Ad-Hoc Networks," Proc. IEEE Int'l Conf. Integration of Knowledge Intensive Multi-Agent Systems (KIMAS),2005
- [13]. E.J. Friedman and P. Resnick, "The Social Cost of Cheap Pseudonyms," J. Economics and Management Strategy, vol. 10, no. 2, pp. 173-199, 2001.

Cite this article as :

M Vineela, Shreya Patthi, Talla Sai Vaishnavi, "Trust But Verify : A Framework for the Trustworthiness of Distributed Systems", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 4, pp.102-105, July-August-2023.