International Innovative Research Journal of Engineering and Technology
Vol. 8, Issue. 3, March 2023, pp. 25~32
ISSN: 2456-1983, DOI: 10.32595/iirjet.org/v8i3.2023.171

A Novel Application Service Security Using Peer-to-Peer Trust Slicing Trust Model

Dr. Yassir. S.K. Osman[1], Dr. A. Rajalingam[2], Dr. Jayakumar. M. S[3]
[1]Engineering Department, College of Engineering and Technology
University of Technology and Applied Sciences, Shinas - Oman
[2]Senior Lecturer, Engineering Department, College of Engineering and Technology
University of Technology and Applied Sciences, Shinas - Oman
[3]Lecturer, Engineering Department, College of Engineering and Technology
University of Technology and Applied Sciences Shinas - Sultanate of Oman

Article Info
Article history:
Received Jan 8, 2023
Revised Feb 10, 2023
Accepted Feb 25, 2023

Keywords:
Network Applications
Network Slicing
Secure Distribution
Trust Model
Security

ABSTRACT
Network applications provide services for different user categories in a distributed and shared scenario. The challenge in providing services is security due to the presence of common communication and sharing networks. In such cases, the presence of adversaries is tedious to be identified. In this article, the Slicing-dependent Secure Distribution (SSD) of services is introduced. This method is designed to combat man-in-the-middle adversaries that are present in commonly shared networks. The service network is partitioned into slices for identifying the distribution patterns and security measures. The trust and its allied communication between the consecutive slices are verified in a peer-to-peer (P2P) manner. The performance is verified under the purely naïve and purely collective scenario and against attack.

Corresponding Author:
Dr. Yassir. S.K. Osman,
Engineering Department, College of Engineering and Technology
University of Technology and Applied Sciences, Shinas - Oman
Email: yassir.osman@shct.edu.om

I. INTRODUCTION

A distributed architecture system known as peer-to-peer (P2P) networking distributes duties across peer nodes in a network. Peers voluntarily lend other peer nodes a part of their resources, such as storage, computing power, or network bandwidth. This is accomplished without the need for any servers or other central coordinating techniques. P2P technology is utilized in e-commerce and social media as a recommender system for user authentication, as well as file sharing (BitTorrent and Gnutella), peer-to-peer aided streaming solutions for multimedia (P2PTV and PDTP protocols), and other sectors. In a P2P network, each node functions as both a client and a server. P2P in particular makes resources available for open and dispersed sharing. That results in efficiency and ease, which enhances P2P application adoption [1].

The 3GPP standard defines LTE self-organizing networks, which may also be employed with P2P technologies. Without a doubt, P2P technologies will take on greater significance in 5G networks. Nevertheless, security risks interfere with the system since P2P networks are very prone to rogue users disseminating destructive material. Nodes in a P2P system rely on one another for smooth transactions and communication [2]. When unscrupulous peers exploit this connection, it raises security issues. Peer nodes in P2P share part of their internals with their neighbors to spread workload fairly, but attackers typically take advantage of this to hack the P2P network [3].

The security of P2P networks is at risk due to the ease of carrying out harmful conduct. A more secure environment may be created by developing long-lasting trust among peers, which lowers the risk and unpredictability of upcoming P2P interactions [4]. However, in such a hostile atmosphere, it is challenging to

build confidence with an unknown creature. In addition, trust is a social construct that is hard to quantify with numbers. To indicate confidence in computational models, metrics are required. It's not always enough to categorize peers as trustworthy or untrustworthy. In order to rate peers according to trustworthiness, metrics should be precise. Peer interactions and feedback offer data to calculate peer trust. This work is to provide a slicing-dependent secure distribution model for network applications.

II. RELATED WORKS

[5] suggested a "hybrid trust model" based on the similarity of preferences that combines local and global trust. The comparable random walk method is used to optimize the sparse trust matrix. [6] suggested a traditional universal trust type based on suggestions. The idea of previous trust peers is put forth. In the early stages of the network's setup, it is believed that every peer has a priori trust. Each peer has a distinct universal trust, and each peer using the service of a peer Pi has a local trust. The trust model takes the local trust of each peer into account when calculating the global trust of Pi, but it ignores the dynamic dependability of the network's peers. Its shortcomings include low scalability and excessive computing complexity. Large-scale P2P networks cannot use the model.

[7] presented the distributed trust aggregation approach, proposed the M-Trust model, and evaluated the trust based on recommendations from other peers and peers with direct interaction. Because it is challenging to determine a recommender's reliability in a dynamic P2P network environment, the trust threshold limit needs to be adjusted in accordance with the network's unique characteristics.

[8] introduced the SuperTrust paradigm, which is founded on a compiled set of super peers. Peers are categorized into interest sets in this paradigm, and there are three different types of trust relationships: trust between super peers, trust between super peers and regular peers, and trust between regular peers. They also provided specialized algorithms for measuring trust. However, it is challenging to accurately assess the quality of service since ambiguities in the suggestion information itself are not taken into account.

[9] presented a social Peer-to-Peer network in which each peer may establish long-term stable social interactions with partners they identify using a social tracker based on their shared interests. Additionally, a distributed trust mechanism is suggested. The degree of collaboration between two friends might be reflected in how much they trust one another. They converse with one another. Social trust can resist more types of attacks, but it does not account for nefarious social trackers.

Despite the network's rapidly varying malevolent behaviors, [10] offered a model that can precisely compute peers' dynamic trust. The SecuredTrust model evaluates peer behavior by examining the historical trust between peers and computing the deviation in peer behavior using the average frequency of trust variations. This stops harmful peers from changing their strategy and repeatedly raises or lowers the reputation values of those peers. As a result, if peer behavior fluctuates, peer trust will decrease and a load balancing method should be used. Although it has a high computational complexity, this method distributes service requests across all competent peers, solving the issue of convoluted and overburdened communication amongst peers with high trust. [11] suggested a traditional global trust model based on suggestions. The idea of previous trust peers is put forth. In the early stages of the network's setup, it is assumed that every peer has a priori trust.

III. METHODOLOGY

Peer-to-Peer Trust Model

By analyzing the trust model, or how trust genuinely moves between the parties, it is simple to identify the main issue with intermediaries. All trustworthy interactions in the present account-based client-server paradigm must be mediated by a server, and all parties involved must be integrated with that server. All the participants in the interaction must have faith in whoever manages this server. In Figure 1, the intermediary trust and peer-to-peer trust model are represented.

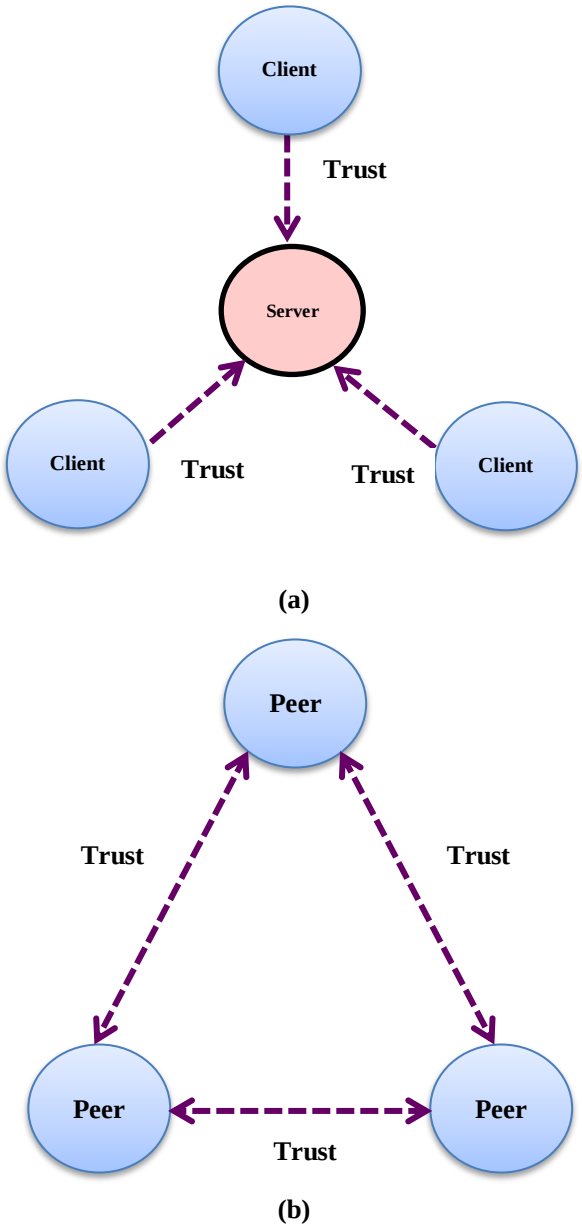

Figure 1. (a). Intermediary Trust (b). Peer-to-Peer Trust

No intermediaries are required in the peer-to-peer trust paradigm. There is no requirement for server integration. Direct bonds of trust are established between each peer and every other peer. Each peer has its own rules for who it will trust. Network slicing is a difficult problem for mobile carriers, commercial enterprises, and next-generation wireless networks. It came next as one of the fundamental components of modern communication technology. It enables mobile carriers to replicate numerous instances of the network utilizing a single base for enhanced service quality. The peer-to-peer slicing-dependernt secure distribution (SSD) model maintains the trust level of the network without any hesitation.

Peer-to-Peer Network Security Issues

The decentralized and anonymous nature of P2P networks makes them particularly susceptible to problems, the majority of which may wreak havoc on them. The primary threats to P2P networks' security include leechers, social assaults, listening queries, DDoS attacks, network verification, and malware. Users who leech are

those who don't share files or resources with others; they simply download from other users. In most P2P networks, a tiny fraction of users bore the lion's share of the sharing load, which creates an imbalance. Inefficient networks with supposedly slower transmission speeds than what is feasible are produced by imbalances **[6]**.

In social attacks, unskilled users unconsciously provide private information about their computers to more knowledgeable P2P users, who may use that information to see their whole hard drives or even steal their passwords. Some users take on the role of super nodes, maintaining a constant internet connection to route messages and maintain a list of shared files for their sub-nodes. These super nodes could create a list of the queries that their sub-nodes submit. This is not the anonymous experience that P2P networks offer because these lists may be utilized to identify a user's identity or usage patterns.

Attacks called DDoS (Distributed Denial of Service) are intended to paralyze a user or network, making it unable to reply to any requests and hence useless. In a DDoS attack, the perpetrator or perpetrators barrage the target with an infinite stream of "bogus" packets, depleting its resources and rendering it unable to provide its services. DDoS attacks are less effective on P2P networks than on server/client networks because of their decentralized nature. If one user is the target of a DDoS attack that overwhelms them, the P2P network as a whole won't be much affected, unlike server/client networks where DDoS attacks are quite successful.

IV. RESULTS AND DISCUSSION

Slicing Dependent Secure Distribution

Peer-to-peer protocols have demonstrated their efficacy in delivering scalable solutions for the deployment of large-scale distributed systems, effectively coping with unreliability and dynamism. Since slicing dependent trust model is logical end-to-end networks, achieving end-to-end security makes sense. Isolation and orchestration share a tight relationship with the idea of end-to-end security. Additionally, it is reliant on the business strategy and, hence, the trust model. As a result, some features of end-to-end security will be covered in the subsections that follow. The service security model using the P2P trust slice trust model is depicted in Figure 2.

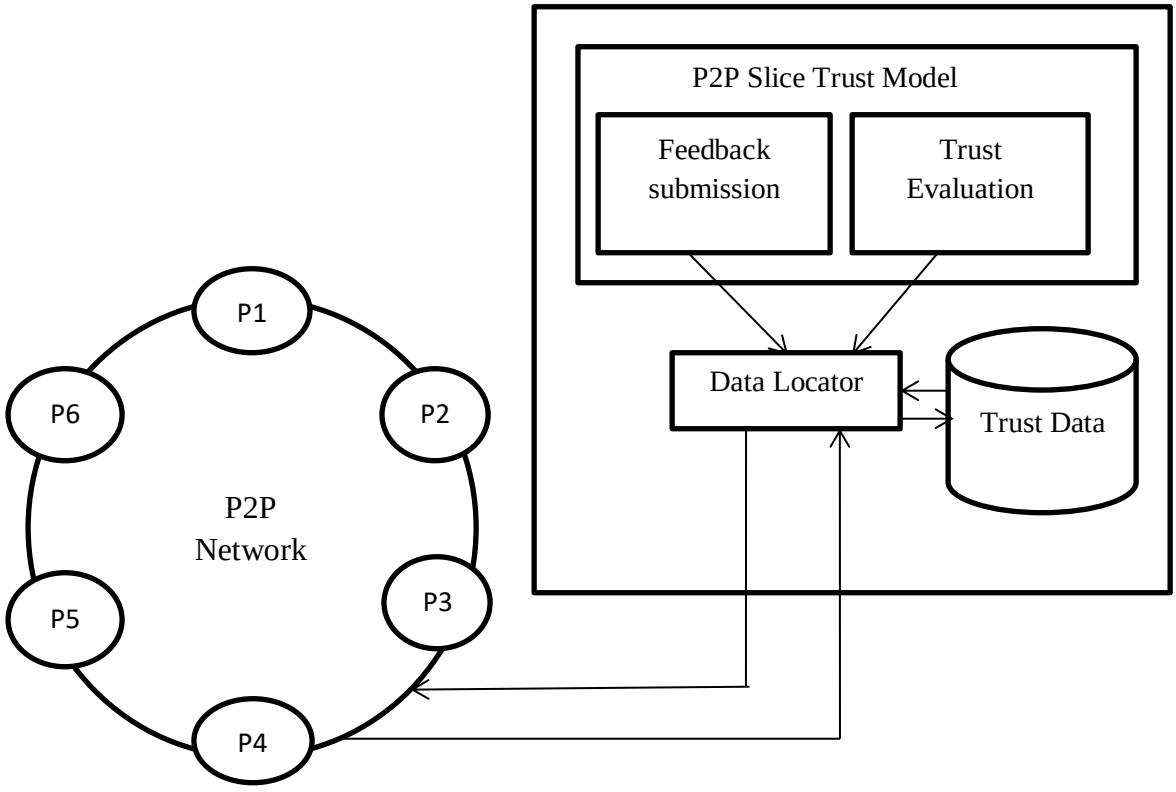

Figure 2. Security in the P2P Slice Trust Model

Peer collaboration is a key component of peer-to-peer (P2P) systems. Peers rely on one another to carry out tasks like downloading and uploading files and routing file search requests. A hostile peer can, however, abuse others' confidence for their own gain and impair a system's functionality. Without cooperation, it might be challenging to identify harmful actions. The simple framework of the slice-dependent trust model is produced in Figure 3 [12].

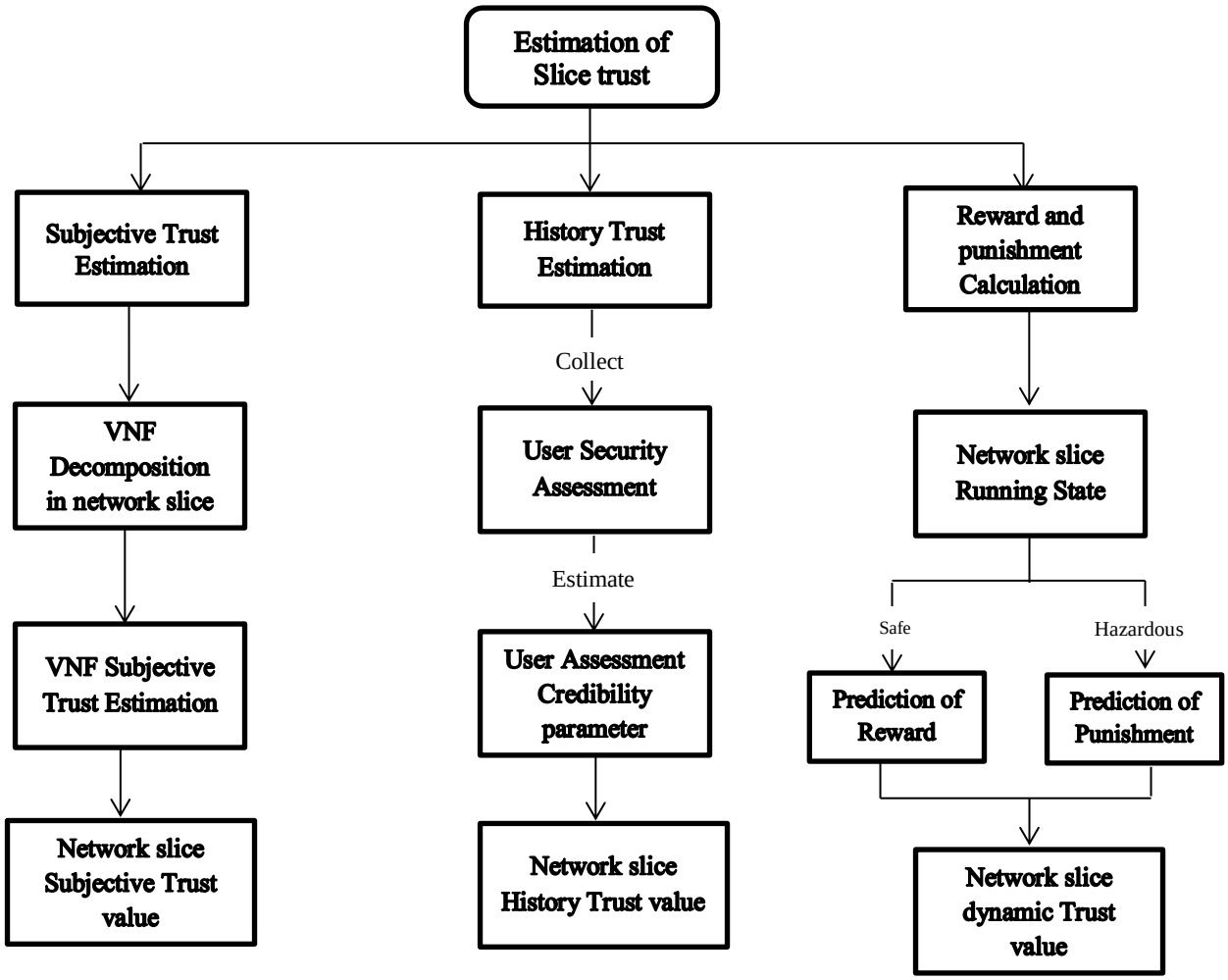

Figure 3. Framework of Slice Dependent Trust Model

The initial slice trust model degree calculation is as follows:

$$Tr = \gamma . ST + \theta . TR \qquad (1)$$

Where ST is the proposed models' slice subjective trust rate, TR is the slice history trust rate. The weights of the subjective trust rate ad historical trust rate are represented by γ and θ respectively. $\gamma + \theta = 1$ and $0 \leq \theta < 0.5$.

The peer-to-peer slice history trust rate calculation formula is as follows:

$$\text{TR} = \frac{\sum_{m=1}^{n} \sum_{c \in C} (C, S_m) \varphi (C, S_m)}{n \; X \; \acute{C}} \qquad (2)$$

$\varphi(C, S_m)$ represents the user c credibility factor for the slice security characteristic S_m trust assessment, to avoid possible malicious assessments and false assessments. Ć specifies the number of users contributing in the assessment. For each security issue in a slice operation, a distinct security weight should be taken into account.

In this research work, we considered a four-tuple slice trust level model to assess the trust rates and determined its trust degree utilizing threshold boundary judgment. Every node has a four-tuple trust level that is specified as $L = [l1, l2, l3, l4]$. This may be expressed as ("zero trust," "poor trust," "partial trust," and "complete trust"] correspondingly, and is shown in Table 1.

Table 1. A Four Tuple Slice Trust Level Band

Four Tuple (L)	Ranges (%)	Trust Level
l1	$\geq 0\ and \leq 35$	Zero Trust
l2	$\geq 36\ and \leq 65$	Poor Trust
l3	$\geq 66\ and \leq 90$	Partial Trust
l4	$\geq 91\ and \leq 100$	Complete Trust

Nodes in the l4 tuple are ideal for trustworthy communication according to the P2P slice trust model, but nodes in the l3 tuple, while generally good, may exhibit certain mixed-element behaviors. It doesn't rely on nodes in the l2 and l1 tuples, but if nodes in the l4 and l3 categories are not accessible, it utilizes nodes in the order of l2 and l1 to maintain reliable communications.

The simulation results of the trust algorithms' merely naive and collective efficacy measures for a 100-node network are shown in Figure 4. The P2P slice trust model performed better (0.965) and took 1.5 seconds to complete in the fully naive case. Additionally, P2P still outperformed EigenTrust (0.931) in terms of trust effectiveness under the purely collective scenario (0.95).

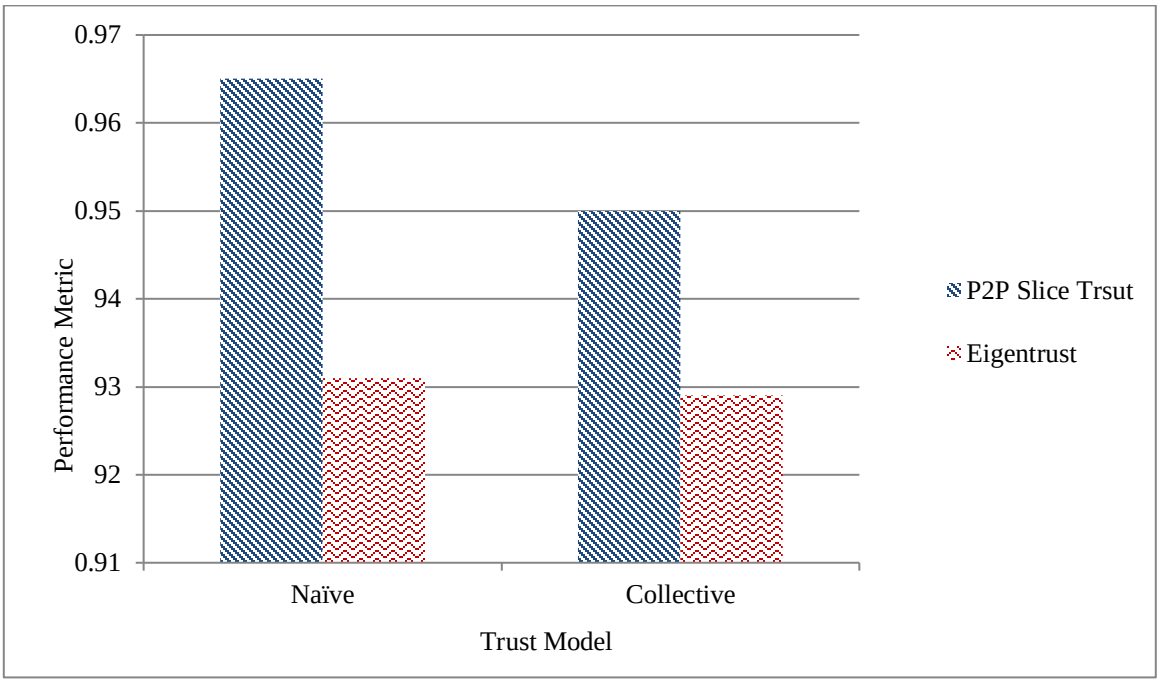

Figure 4. Slice Trsut Model Performance of a 100-node Network

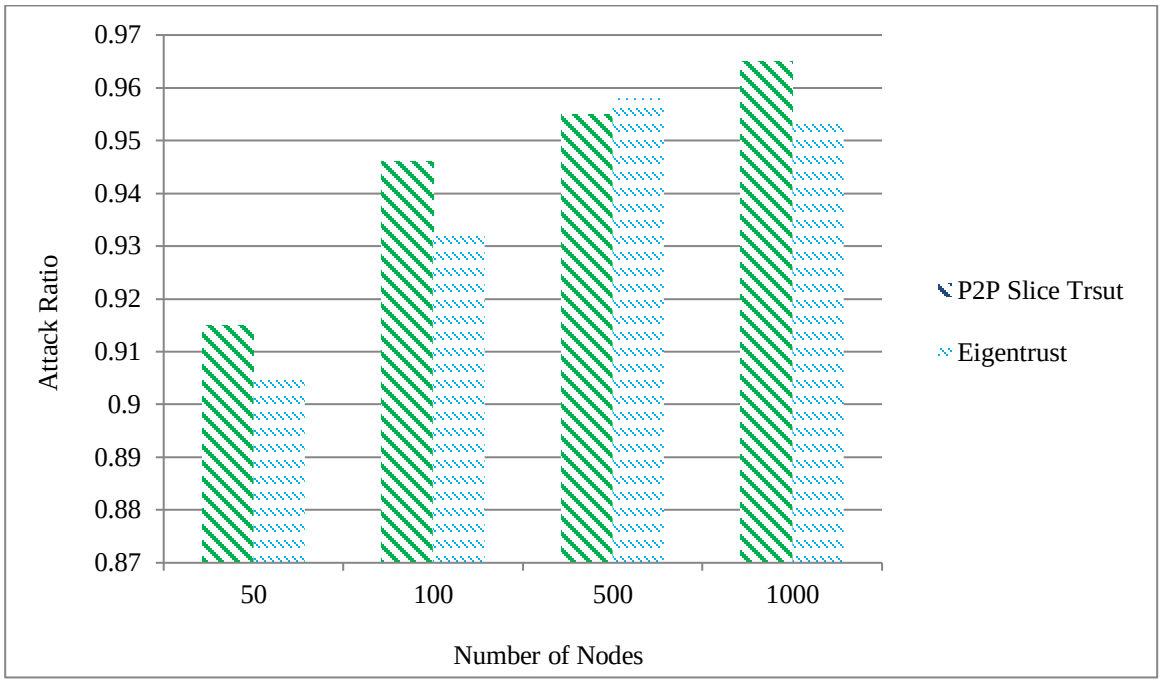

Figure 5. Performance of Slice Trust Model Against Attacks

The relative performance of EigenTrust and P2P Slice trust in the naïve and collective situation is shown in Figure 6. Again, throughout the simulation on the 50, 100, 500, and 1000 nodes, the proposed P2P slice-dependent trust model maintained superior trust effectiveness, consistent performance, and scalability over EigenTrust.

V. CONCLUSION

This paper proposes a slice-dependent trust model for application service security in peer-to-peer networks that relies on how packets are forwarded by peer nodes. Slice's trust model and EigenTrust's trust-based efficacy and performance tests were compared. P2P slice-dependent secure distribution model outperformed EigenTrust in terms of performance in both cases (the fully naive and the strictly collective). Based on the results of the simulation, we draw the conclusion that the suggested strategy, as it is described in this research, has demonstrated potential efficacy and efficiency in trust management even in the presence of adversaries.

REFERENCES

[1] Khan, S., *et al.*, "Highly accurate and reliable wireless network slicing in 5th generation networks: a hybrid deep learning approach," *Journal of Network and Systems Management*, vol. 30, no. 2, pp. 29, 2022.

[2] Airehrour, D., *et al.*, "SecTrust: A trust and recommendation system for peer-2-peer networks," International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISeL), 2018.

[3] Bhoir, AS., & Vaidya, S.M, "A Comprehensive Proliferation on Cloud Computing with Models," *International Journal of Research Publication and Reviews*, vol. 2, no. 8, pp. 960-963, 2021.

[4] Priyadarshini, T.B., *et al.*, "A Novel Architecture for Peer-To-Peer System to Provide Security," *IJCST*, vol. 6, no. 1, pp. 44-47, 2015.

[5] T. Shen, *et al.*, "Identifying collusion attack based on preference similarity in mixed reputation recommendation model," *Human Centered Computing*, vol. 74, Springer International Publishing, Cham, Switzerland, 2016.

[6] Balfe, S., *et al.*, "Trusted computing: Providing security for peer-to-peer networks, " In *Fifth IEEE International Conference on Peer-to-Peer Computing (P2P'05)* (pp. 117-124), IEEE, Aug 2005.

[7] Kumar, M. V., *et al.*, "Early-stage detection of cancer in breast using artificial intelligence," *Revista Gestão Inovação e Tecnologias*, vol. 11, no. 2, pp. 2016-2028, 2021.

[8] Tian, C. Q., *et al.*, "A novel super-peer based trust model for peer-to-peer networks," *Chinese journal of computers*, vol. 33, no. 2, pp. 345-355, 2010.

[9] Hu, Y., *et al.*, "SocialTrust: Enabling long-term social cooperation in peer-to-peer services," *Peer-to-Peer Networking and Applications*, vol. 7, pp. 525-538, 2014.

[10] Das, A., & Islam, M. M., "SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems," *IEEE transactions on dependable and secure computing*, vol. 9, no. 2, pp. 261-274, 2011.

[11] D. Kamvar and T. Schlosser. "EigenRep: reputation management in P2P networks, " in *Proceeding of the 12th ACM International World Wide Web Conference*, Budapest, Hungary, pp. 123–134, 2003.

[12] Niu, B., *et al.*, "5G network slice security trust degree calculation model", In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, IEEE, pp. 1150-1157, Dec 2017.