File Sharing Preference in a Peer-To-Peer Network

Keerthika V
UG Scholar
Computer Science and Engineering
Francis Xavier Engineering College
keerthikav7597@gmail.com

Bibila C
UG Scholar,
Computer Science and Engineering
Francis Xavier Engineering College
barasakthibibila@gmail.com

Manohar E
Assistant Professor
Computer Science and Engineering
Francis Xavier Engineering College
manohar2k@ymail.com

ABSTRACT

Distributed system depicts a common complex system whereupon clients interface together as indicated by their sharing inclination, demonstrated by the assets they shared. In most record sharing frameworks, content appropriation is a brought together one, where the substance is circulated from the incorporated server to all customers asking for the report. Customers send demand to the concentrated server for downloading the record. Server accepts the request and sends the file to the request as a response. The server is a dedicated computer designed to distribute files in its entirety. The proposed system uses analytical methods from complex network theory to investigate user sharing preference as well as correlations between different resource categories in a real peer-to-peer file sharing system, which helps to reduce server complexity in file sharing.

Index terms: peer-to-peer data sharing, file sharing, analytic method

I. **INTRODUCTION** PEER-TO-PEER (P2P) systems

rely on peer cooperation to carry out tasks. Ease of malicious activity is a threat to P2P systems' security. By reducing risk and uncertainty in future P2P interactions, long-term relationships of trust between peers can provide a more secure environment. Peers' interaction and feedback provide information to measure peers' trust. Interactions with a peer provide some infor mation about the peer, but feedback may contain information that is misleading. Evaluating trustworthiness is a challenge. The server is a dedicated computer that stores confidence information securely and defines confidence metrics. Since most P2P systems do not have a central server, peers organize themselves to store and manage each other's trust information. Each peer becomes a trust holder in distributed hash table (DHT) approaches by storing feedback about other peers.The information stored by trustees can be efficiently accessed via DHT. Each peer stores trust information about peers in their neighbourhood or peers who have interacted in the past in unstructured networks. A peer sends trust requests to learn other peers' trust information. A trust query is either flooded into the netw ork or sent to the query initiator's neighbour hood. In general, the trust information calculated is not global and does not reflect the views of all peers. We propose a model which aims to reduce malicious activity in a P2P system by establishing relationships of trust between peers in their vicinity. To leverage trust establishment, no a priori information or trusted peer is used. Peers do not attempt to collect information about trust from all peers. Each peer develops his or her own local view of trust in the past. Good peers thus form dynamic trust groups nearby and can isolate malicious peers. In SORT, peers are supposed to be strangers at the start. After providing a service, such as uploading a file, a peer becomes an acquaintance of another peer. If a peer is unfamiliar, he chooses to trust strangers. SORT defines three confidence metrics. The metric of reputation is calculated according to recommendations. When deciding on strangers and new acquaintances, it is important. Reputation loses importance as acquaintance experience increases. Trust in service and recommendation are the primary metrics for measuring trustworthiness in the context of service and recommendation. When selecting service providers, the service trust metric is used. When requesting recommendations, the trust metric is important. Recommendations are evaluated on the basis of the trust metric for the calculation of the reputation metric.

II. EXISTING SYSTEM

Many researchers worked on file sharing approaches. Protecting a victim (host or network) from malicious trafficking is a difficult problem requiring the coordination of several complementary components, including non-technical (e.g. business and legal) and technical solutions (at the level of the application or network). Filtering network support is a key building block in this effort. For example, an Internet service provider (ISP) may use filtering to block DDoS traffic before reaching its customers in response to an ongoing DDoS attack. Another ISP may want to proactively identify and block traffic carrying malicious code before vulnerable hosts are first reached and compromised. Filtering is a necessary operation within the network in either case. Today, routers already have filtering capabilities via access control lists (ACLs).ACLs allow a router to match a packet header with pre-defined rules and take pre-defined actions on the matching packets, and are currently used to enforce a variety of policies, including infrastructure protection. A filter is a simple ACL rule that denies access to a source IP address or prefix to block malicious traffic. Filtering is implemented in hardware in order to keep up with the high forwarding rates of modern routers: ACLs are typically stored in addressable memory for ternary content (TCAM), which allows parallel access and reduces the number of searches per packet forwarded. TCAM is more expensive than conventional memory and consumes more space and power. TCAM's size and cost limit the number of filters, and this will not change in the near future. With thousands or tens of thousands of filters per path, an ISP alone cannot hope to block the attacks currently witnessed, not to mention the attacks expected in the near future from multi-million-node botnets.

In [1], the project provided a new MCS architecture based on P2P, where sensing data is stored and processed locally on user devices and shared with users in a P2P way. In order to provide necessary incentives for users in such a system, Changkun Jiang et al proposed a market for quality-aware data sharing, where users who perceive data can sell data to others who request data, but do not want to perceive the data. The project used game-theoretic perspective to analyse the dynamics of user behaviour and characterize the existence and uniqueness of the game balance. The project also proposed best response iterative algorithms to achieve a balance with proven convergence. The simulations show that the sharing of P2P data can significantly improve social welfare, particularly in the model with high transmission costs and low trading price.

Mobile devices can be used to store and distribute data files via device-to-device (D2D) communication as an alternative to downloading content from a cellular access network. In [2], Paakkonen et al considered a mobile user storage community based on D2D. Assuming that the transmission of data from a base station to go to a mobile user consumes more energy than that of the transmission of data between two mobile users, the project showed that redundant storage can be beneficial to ensure that data files remain accessible to the community, even if some of the users who store them leave the network. The project resulted in a tractable closed-form equation indicating when redundancy should be used to minimize the expected energy consumption of data recovery. It is found that the replication to be the preferred way to add redundancy rather than regenerate codes. Computer simulations verified the results.

In [3] the Mobile social networking penetrates our everyday lives through the convergence of widespread mobile communications and rapidly growing online social networking. In order to develop a systematic understanding of mobile social networks, Chen et al used social links in human social networks in

order to improve cooperative communication between devices (D2D). In particular, as people carry handheld devices, they used two key social phenomena, namely social trust and social

reciprocity, to promote effective cooperation between devices. With this insight, they developed a coalition game-theoretical framework to develop strategies for D2D cooperation based on social ties. They also developed a network-assisted relay selection mechanism to implement the coalition game solution and show that the mechanism is immune to group

deviations, rational, true and computationally efficient individually.

They evaluated the mechanism's performance using real traces of social data. The results of the simulation confirm that without D2D cooperation, the mechanism could achieve significant performance gains over the case.

For most mobile social network (MSN) applications, such as content distribution and information search, effective data transmission is critical [4]. However, if the privacy protection of users is applied, it could be severely interrupted or even disabled, as users become mutually unrecognizable and social links and interactions are no longer traceable to facilitate the transfer of cooperative data. It is therefore a difficult problem of how one can enable efficient user cooperation in MSNs without interfering with user privacy. In 2012, Liang et al addressed this issue by introducing social morality, which is a fundamental social feature of human society, to MSNs and accordingly design a three-step protocol suite to achieve both privacy preservation and cooperative data forwarding. First, the developed protocol adopts a new route-based authentication scheme that preserves privacy and notifies the public of anonymised information on mobility from a user. Secondly, it measures the proximity of the mobility information of the user to the destination of a specific packet and evaluates the capacity of the user to forward the packet. Third, it determines the optimal data transfer strategy based on the level of morality and payoff of users using a game - theoretical approach. Using analyses and examples, the project showed that the developed protocol suite can effectively protect user personal data such as identity and locations visited. Finally, they carried out extensive trace-based simulations and demonstrate that the proposed protocol suite is effective in exploring user cooperation efficiently and achieving near-optimal data transmission performance.

Social network sites are becoming great through millions of users and the users have collected information [5]. This information offers their friends and spammers equal advantages. Twitter is one of the most popular social networks that can send short text messages to users, namely tweet. Research has shown that this network is more subject to spammers than other social networks and more than 6% of its tweets are spam. So it's very important to diagnose spam tweets. In 2013, Yue et al determined different features for spam detection in this research and then identify spam tweets using a clustering algorithm based on the data stream. Previous work on spam tweets was carried out using classification algorithms. It is the first time an algorithm clustering data stream is used for the detection of spam tweets. Den stream Algorithm can cluster tweets and take outsourcers as spam. The results show that if this algorithm is correctly set, the accuracy and accuracy of the detection of spam tweets will improve and the false positive rate will reach the minimum value compared to previous works.

In [6] due to D2D's potential ability to improve spectrum and energy efficiency in existing cellular infrastructure, device-to-device communications have recently attracted wide attention. D2D user equipment (DUEs) themselves, lacking sophisticated control, are not powerful enough to resist eavesdropping or combat security attacks. The work by Wang et al examined the selection of jamming partners for D2D users to prevent social outcasts from receiving D2D overlays by using social relationships to improve the rate of secrecy. By selecting the jammer node while allocating transmit power for both source and jammer, they maximized the secrecy rate of the worst case. They presented a solution based on heuristic genetic algorithms to directly assess the problem. They also showed approximate optimization solutions by taking into account the power allocation of upper and lower limits to simplify the problem, using the Dinkel bach-type algorithm based on fractional programming (GFP). Numerical results show that by finding an appropriate partner, the schemes could achieve better performance.

The paper [7] examined the problem of the allocation of resources and power in device-to-device (D2D) underlays in the light of a specific restriction on the secrecy rate. The objective was to optimize the combination of D2D links with the uplink channel resources of cellular user equipment (CUE) and to allocate their respective powers to combat eavesdroppers to improve the secrecy rate. In order to reduce the number of combinatorial sharing options, the method introduced by Wang et al first determined a set of candidate D2D links with the required signal-to-interference-plus-noise ratio for each CUE. An optimization problem is subsequently formulated to maximize the overall secrecy rate under user power constraints and minimum requirements.

The application of the principles of information theoretical security and signal processing to secure physical layer systems has recently been of significant interest [8]. While the community has made progress in understanding how the physical layer can support confidentiality and authentication, it is important to realize that many important issues need to be addressed if real and practical security systems are to adopt physical layer security. In 2015, Trappe briefly made review on several different flavours of data security and then identified aspects in which security must be strengthened. This paper made security of physical layer.

III. FEASIBILITY STUDY

It is wise to consider the feasibility of any problem we are facing. Feasibility is the impact study, what happens through the development of a system in the organization. The impact may be positive or negative. The system is considered feasible when the positive dominates the negative. The feasibility study is carried out in three ways.

A. Technical Feasibility

We can firmly say that this is technically feasible, as it will not be very difficult to obtain the necessary resources for the development and maintenance of the system. All resources are available for the development and maintenance of the software. We use the resources that are already available here.

B. Economic Feasibility

This application can be developed economically. We don't need to spend much money on the project because the resources needed to develop the system are already available. The only thing to do is to create an environment with effective supervision for development. If we do this, the maximum usability of the corresponding resources can be achieved. The system is therefore economically viable.

C. Operational Feasibility

The system proposed is beneficial if and only if it can be converted into a system that meets the operating requirements. If the system is developed and installed, the best feasibility asks if it will work. The objective of the operational feasibility study is to determine if the new system is developed and implemented. The proposed system is frequently used since it meets all communication requirements, thus ensuring operational feasibility.

IV. PROPOSED SYSTEM

To overcome the drawbacks of existing systems, the project uses an approach when the peers are registered and connected to the network, all the peers get information about all other peers. Different modules are used to perform those tasks. Blocking concept is included which helps in secure transfer of data between peers. Trust relationships are developed by peers to get the peer that performs malicious activity. If a system performs any unwanted activity it is automatically block listed. Users are also allowed to block other users. If a user wants to share data or files to selected users he/she can block other users from the list. The blocked users cannot see information of other users as seen previously before being block listed. The users could see which of the other users are online and can communicate with them.

SYSTEM ANALYSIS ARCHITECTURE

The Fig 1. represents the system architecture of the proposed system.

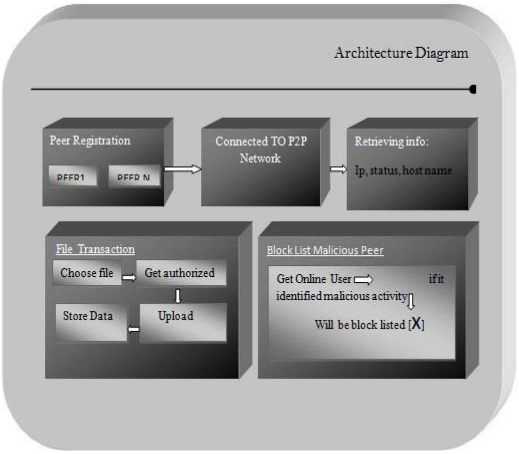

Fig. 1 Architecture

A. Module Description

SORT includes seven basic modules.

- Peer Registration
- Get Online User
- User Info
- Chatting
- File transaction
- Acknowledgement
- Block Listing

Peer Registration

All user needs to register himself with connected network.

Get Online User

In this every user will be displayed to each one. By this each one directly communicates.

User Info

It will show the user's IP Address, Status of the node, Host Name.

Chatting

Before file uploading user can intimate the type of file going to transmit by chat application. So while transmitting other user can identify easily.

File Transaction

Now peer going to upload the data, first respective node will get which node is communicating him. After authorizing, others can send and receive the data.

Acknowledgement

Acknowledgement is sent by every peers after successful transaction. It is sent when the peers receive the files successfully.

Block Listing

If the node appeared as untrusted will be block listed**.** So he won't get any info about other peer which was seen already.Also untrusted peer rejected from network and cannot able to communicate further.

V. CONCLUSION

A trust model for P2P networks in which a peer can develop a trust network nearby is proposed. A peer can isolate malicious peers while building relationships of trust with good peers. They are then block listed. The capability of block listing results in improved security of peer-to-peer communication.

REFERENCES

1. Changkun Jiang, Lin Gao, LingjieDuan and Jianwei Huang. (2018). Scalable mobile crowdsensing via peer to peer data sharing. IEEE Transactions on Mobile Computing (Volume: 17, Issue: 4, April 1 2018)
2. Paakkonen, J., Hollanti, C., &Tirkkonen, O. (2013, December). Device-to-device data storage for mobile cellular systems. In Globecom Workshops (GC Wkshps), 2013 IEEE (pp. 671-676). IEEE.
3. Chen, X., Proulx, B., Gong, X., & Zhang, J. (2015). Exploiting social ties for cooperative D2D communications: A mobile social networking case. IEEE/ACM Transactions on Networking, 23(5), 1471-1484.
4. Liang, X., Li, X., Luan, T. H., Lu, R., Lin, X., &Shen, X. (2012). Morality-driven data forwarding with privacy preservationinmobilesocial networks. IEEE Transactions on Vehicular Technology, 61(7), 3209-3222.
5. Yue, J., Ma, C., Yu, H., & Zhou, W. (2013). Secrecy-based access control for device-to-device communication underlaying cellular networks. IEEE Communications Letters, 17(11), 2068-2071.
6. Wang, L., Wu, H., Liu, L., Song, M., & Cheng, Y. (2015, June). Secrecy-oriented partner selection based on socialtrustindevice-to-device communications. In Communications (ICC), 2015 IEEE International Conference on (pp. 7275-7279). IEEE.
7. Wang, L., Wu, H., Peng, M., Song, M., &Stuber, G. (2015, December). Secrecy-oriented resource sharing for cellular device-to-device underlay. (GLOBECOM), 2015 IEEE (pp. 1-5). IEEE.
8. Trappe, W. (2015). The challenges facing physical layer security. IEEE communications magazine, 53(6), 16-20.