International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.41-56
http://dx.doi.org/10.14257/ijsia.2016.10.5.04

On Privacy and Anonymity in Freenet System

Tianbo Lu, Zhimin Lin, Lingling Zhao, Yang Li

School of Software Engineering, Beijing University of Posts and Telecommunications, 100876, Beijing, China
lutb@bupt.edu.cn, ttn_210@163.com

Abstract

As a typical representative of anonymous network applications, Freenet system has so many advantages in sharing, privacy, anonymity as well as uploading and downloading convenience that it adequately realizes expression freedom. So it's widely used in different fields. For Freenet system, academia and system designers have been conducting research and improvement which mainly on following points: structure, topology, routing algorithm and the Darknet mechanism which proposed by new version. The purpose of these efforts is to increase the system network utilization, enhance the reliability of transmission and improve the safety and robustness of the system. This paper reviews and summarizes the research progress of Freenet system by collating and analyzing relevant articles. We also analyze and compare the main ideas, the algorithm application as well as pros and cons of different articles surrounding different topics. In addition, we also tease out the development and the evolution trends of Freenet system in time order, and combined with current network situation, we made reasonable proposals and prospects and draw scientific conclusions.

Keywords*: Freenet , Privacy, Anonymity, Security*

1. Introduction

In the era of information technology, business and government are trying to use many methods to inhibit a variety individuals Network effects. Meanwhile, the individual is unable to know what will occur to their data, their original intention was restricted and the expression freedom cannot be obtained [1]. In the open network, we need to design a system which can make the network information encrypted and send anonymous messages, achieving expression freedom.

The proposal of Freenet system, gives a good solution to this problem. The system originally derived from an unpublished report "distributed storage and retrieval system", which is proposed by Ian Clarke [2]. Such thinking gives the foundation and directions to following researchers, in another paper, the designers presented Freenet by the thinking of distributed data storage and caching, the content of which users need to publish into distributed storage using a different computer in the system, and encrypt them [3]. However, publisher and users do not know the specific storage location. As a result, users can anonymously publish or get all sorts of information.

Freenet is a widely deployed, completely decentralized system focus on anonymity and censorship-resilience [4]. In this system, through files encryption, making users of the system (including their own) very difficult to find the storage nodes files and do not know whether the file is stored in their own nodes. Users need to provide their own nodes bandwidth and hard disk storage information to make the system to do appropriate action. The frequency of files used to choose whether to drop or update those files, and the files which rarely used would be discarded. In addition, according to related paper, we know that some sites, chat forums and search capabilities, have chosen to share this information based on the distributed data storage achieved [4].

ISSN: 2005-4262 IJGDC

The statistical data of the system site displays: the download of Freenet system been used more than two million times and widely around the world. At the same time, the idea of Freenet system has also been taken seriously in academic circles, which also triggered a debate in relevant legal and philosophical aspects. Ian Clarke, the project proponent, was selected as one of the top 100 innovators in 2003 by former MIT Technology Review magazine [4].

In recent years, Freenet system proposed a new idea: Construction of the Darknet. In this network, users can simply connect to their trusted partners, and then it can be interconnected into a global network. This idea enhances the user's anonymity and privacy. So the outside world attack can't trace back to the source of the information publisher, ensuring the security of information, it can be regard as a free small world.

Seeing relevant research, there is little in-depth study of Freenet system progress and technological development. Therefore, we collected and summarize the related theses and tease out their content and relationships. Which we hope to provide reference to other researchers. Our contributions to this work are follows:

(1) Introduce the origin and evolution of Freenet system;

(2) Summarize the main techniques used in Freenet system to achieve privacy and
(3) anonymity;
(4) A comprehensive assessment for Freenet system and reasonable advice and prospect.

2. Related Works

2.1. Edition Evolution

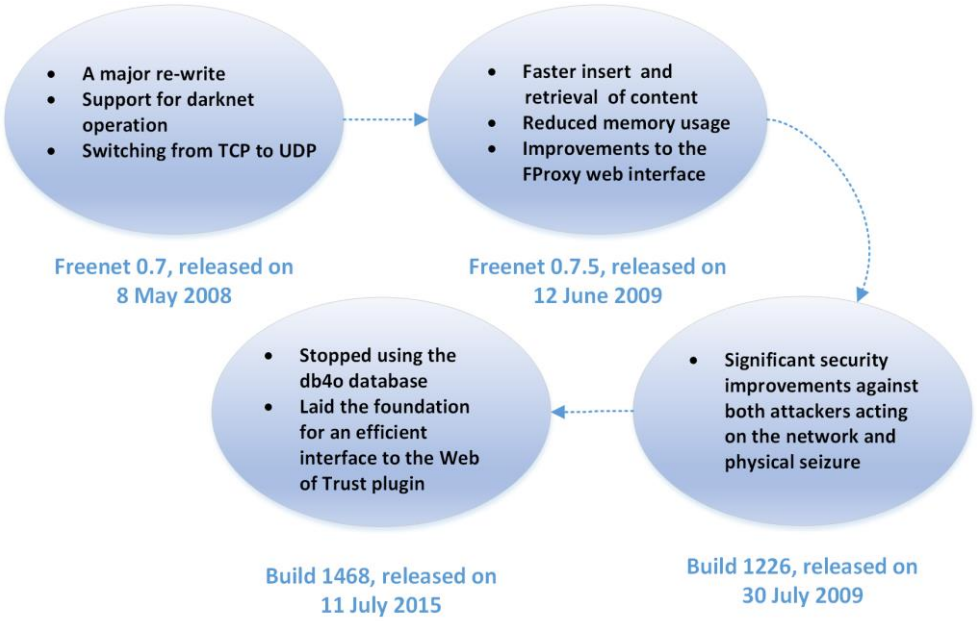

Figure 1. Edition Evolution

As illustrated in Figure 1, Freenet 0.7, released on 8 May 2008 gives a rebuild and combine to previous editions. The most fundamental change of it is that the system supports Darknet operation. Meanwhile, it adds the switching from TCP to UDP, this function speeds up the message transmission of UDP hole punching in the network [5].The next edition, Freenet 0.7.5, released on 12 June 2009, updates the 0.7.in many aspects, including retrieval of content reduced memory usage as well as faster insert. In addition, there are significant enhancements on Proxy web interface, the tool for freesites

browsing. A lot of smaller bug fixes and usability improvements are also realized. Edition 0.7.5 is also shipped with a Windows new version installer [6]. As for build 1226, released on 30 July 2009, it does security improvements against attacks both on the network and physical seizure of the computer running the node [7]. The build 1468, released on 11 July 2015, db4o database stops used for Freenet core and build a foundation-- whose efficient interface to the Web of Trust plugin used for providing spam resistance [8].

2.2. Related Theses

About Freenet, there are many theses discuss the system, we collected some of them and summarize it into Figure 2. As the Figure 2 shows, the related theses publish year spans from 1999 to 2014. According to these theses, we mainly outline the following aspects. The first section is about introduction and the he fundamental thesis is "Freenet White Paper". In this section, we mainly describe the requirement of anonymous system and the origin of Freenet system. According to that, we point out the basic idea and technology about Freenet system.

Then, we mainly analyze and summary around three topic. The first topic is small world, there are four theses talk about it. Hui Zhang and Ashish Goel propose an enhanced-clustering cache replacement scheme for use in place of LRH in 2002. In 2005 Sandberg published two theses. The first one gave two ideas about searching in the small world. Another one applies small world models and finds greedy path when only a graph is presented, in 2007, Vhelm Verendel found ways to speed up the routing method.

The next topic is about the Darknet mechanism. Ian Clarke proposes this new architecture, it is a new version of Freenet in 2010. He describes the simulation of the data in new conditions of Freenet system. After that, Stefanie Roos describes the small world model based on a distributed routing algorithm, which is the beginning of Darknet routing algorithm. He proposes a realistic analytical method and a novel routing algorithm with provable polylog expected routing length in 2013.

While the modifications and upgrade form application software to the underlying protocol has been one of the obstacles in the development of Freenet network, we must now review its system architecture and propose the new algorithms. In Stefanie Roo's paper, they focus on the long delays and low success rates for finding and retrieving content in Freenet, and they tried to identify the bottlenecks of existing routing algorithms, then they propose a new algorithm. Their results show that the new algorithm is better than before.

The last topic focus on privacy and anonymity, we discuss the following content. The first one is the distributed storage and trusted connection based on Clark and Sandberg's research. Then Prateek Mittal proposes decentralized protocol-Pisces in 2013. As for the Darknet, Nathan.S.Evans gives the first independent security analysis of Clark and Sandberg's routing algorithm in 2009. With the development of Freenet system, Benjamin Schillerand devises simple attacks and derives a novel embeddings model in 2012. The detail information of each topic will be introduced later.

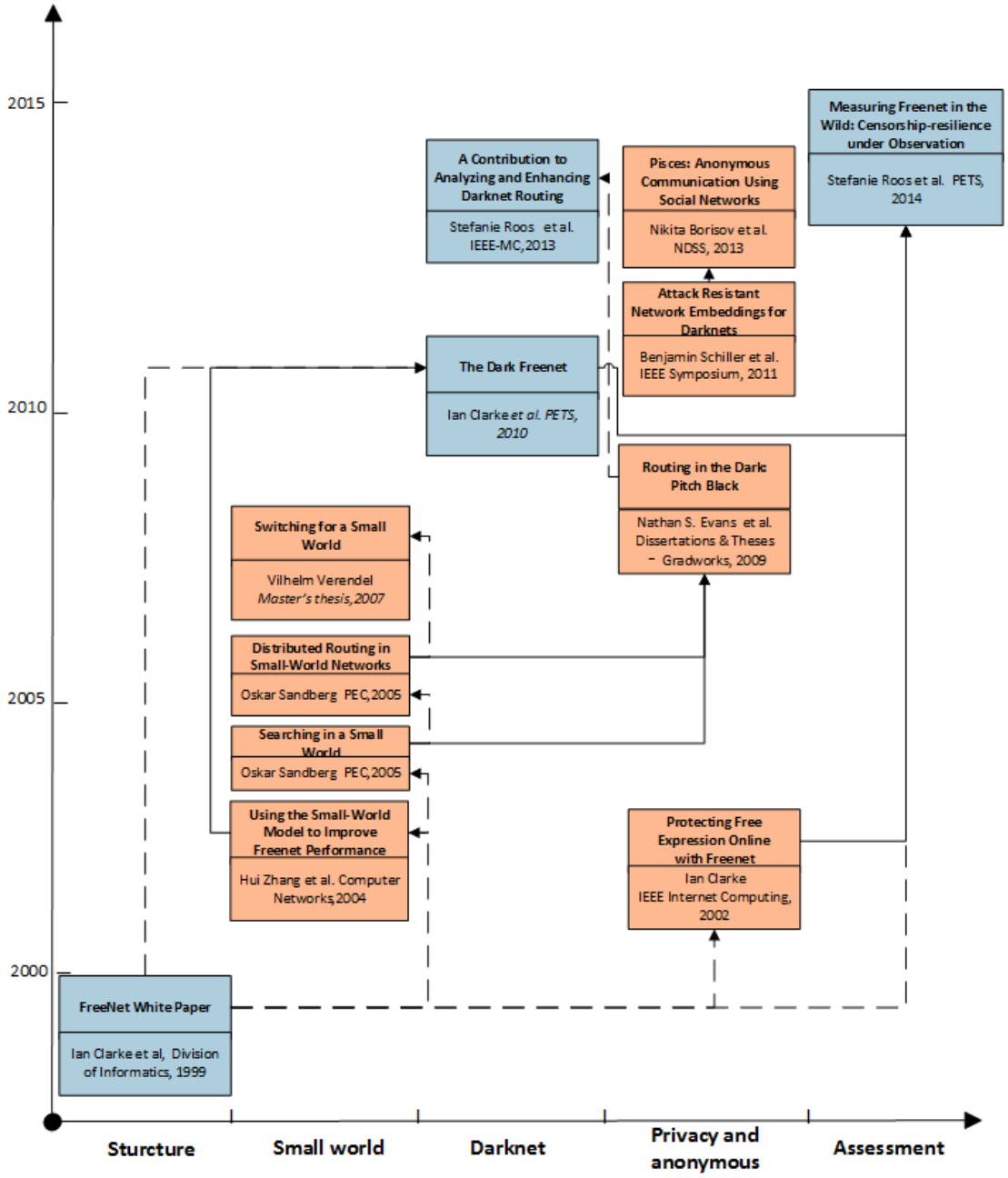

Figure 2. Main Theses of Freenet System

Finally, Figure 3 shows the current study status about Freenet from following three topics: small world, Darknet, anonymous and privacy. It includes the related institutions, researchers as well as their relationships. From the picture we can see, among the theses we reference, there are three universities related to the topic of small world, three for Darknet, seven for anonymous and privacy, which is the most. We can also see that, there exists common contains between different theses, and we find that an institution may be involved in more than one topics and a research team may also study different aspects. This reveals the fact that the research about Freenet system idea is widely around academic circles.

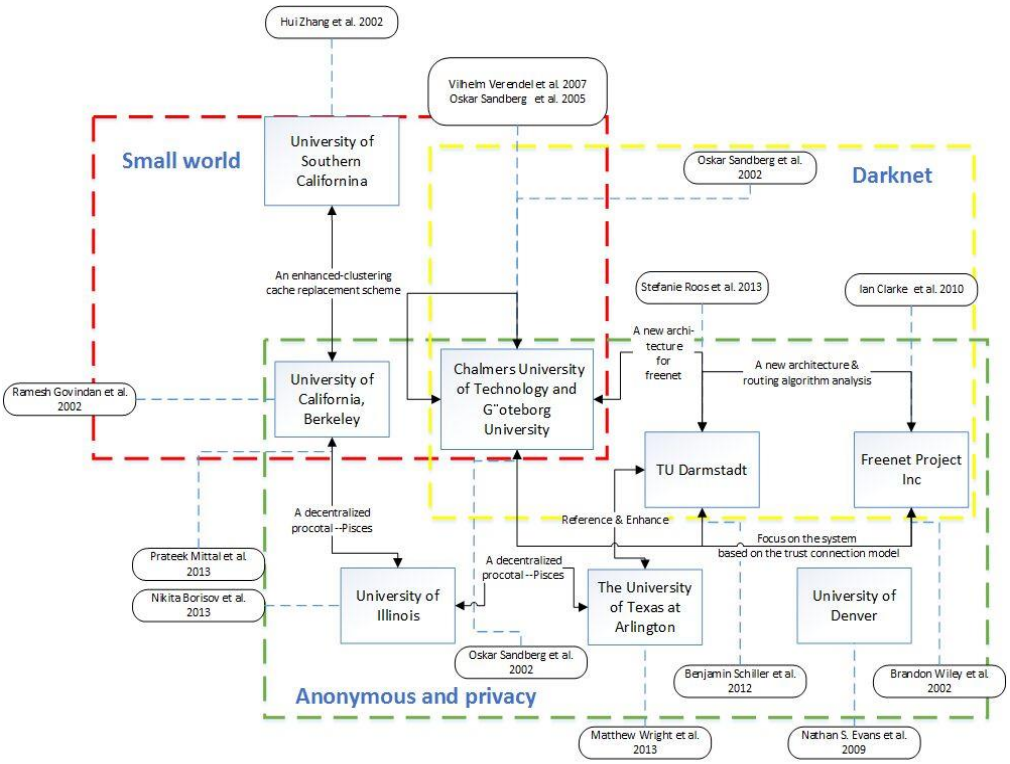

Figure 3. Study Status of Freenet System

3. Small World Networks

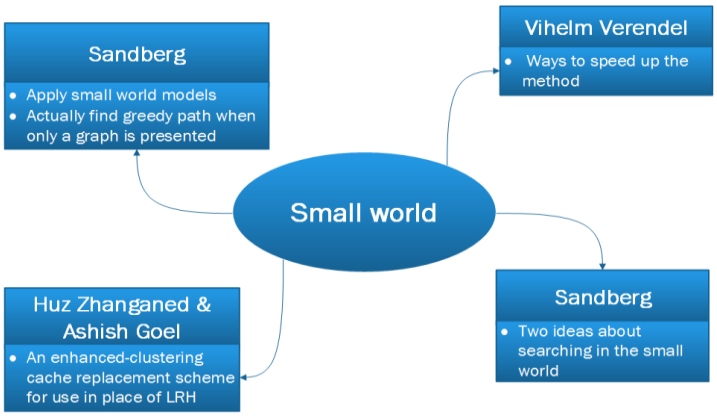

Figure 4. Studies around Small World in Freenet System

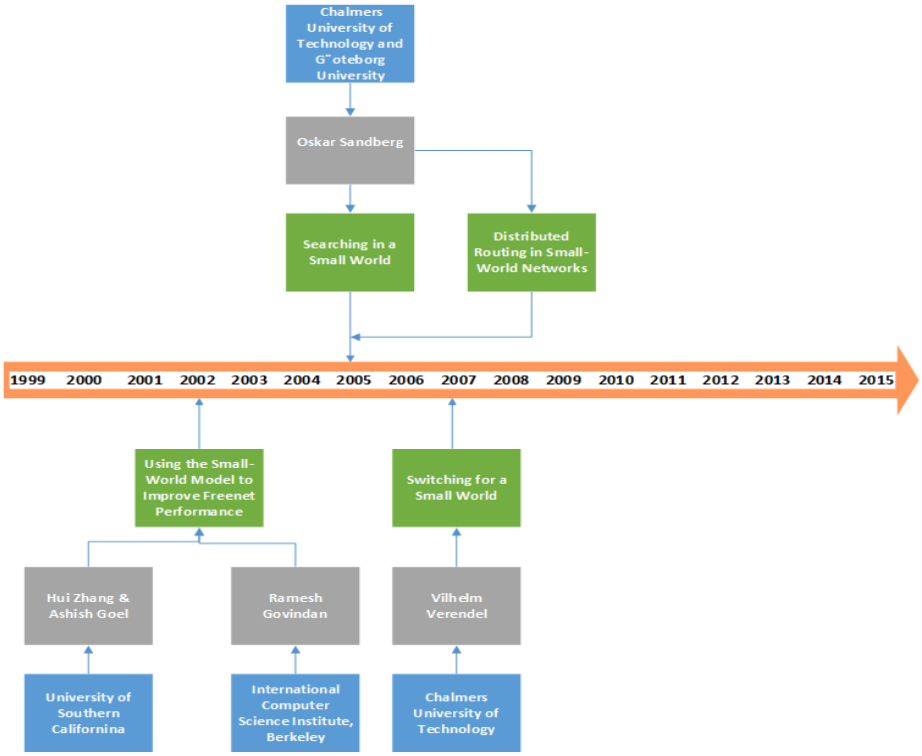

Figure 5. Time Axis for Small World Studies

The view of "Small world phenomenon" can be traced to the famous experiment proposed by Stanley Milgram in 1960 [9]. His experiment showed that people can find very effective route to the destination, even the other side of the country, this conclusion also applies to the Internet.The detail information of these theses is shown as the Figure 4 and Figure 5.

If a network has small-world topology, then its routing can work, and should be scaled with roughly O (log^2 N) (or O (log N) if nodes have O (log N) number of connections) [10].

In many such networks, empirical observations suggest that any two individuals in the network are likely to be connected through a short sequence of intermediate acquaintances [11] [12]. Freenet routing is based on the topology of the small world.

3.1. Small World Model Simulation in Freenet System

As remarked by Hui Zhang, a Freenet network can be evolved into a network with small-world characteristics. In particular, the study shows that the number of bits in a Freenet network path length can grow with the size of the network follows the log relation, drawing its clustering coefficient is high, especially in the small-world networks.

In his experiments, using a simulator to verify each change request and the number of hops which follows logarithmical general relationship. In Freenet network load low scale, through the free performance under heavy network, simulate the performance of the Freenet, achieving a single free network simulator to mimic the file generation, storage, routing, and retrieval. In practice, Freenet access on the collection of data HopsToLive. Thus, the performance of the system is assessed by the request successful rate: preferably by two in dices represent the average hop but only for each successful request. Ultimately, this study shows that the usage of random shortcuts, and enhanced clustered cache than LRU and instead of chaos shortcuts. It should be noted that this change is important that the agreement does not involve any modification of Freenet, only partially been filled when the data stores the user's behavior. Finally, based on an idealized model, with

caching alternatives analysis Freenet modify the incubation period, the model will come to the Small world, it can make peer system performance improved [10].

3.2. Searching and New Routing

In practical network, people may want to search for small-world networks. In 2005, Sandberg studied this topic and firstly proposed two different search strategies, based on Kleinberg's search algorithm [12]. He studied the demand of effective search algorithm in different types of networks, noted that the new search algorithm model might be the future direction of the network. Subsequently, he made specifically addressed in another article, proposing a new routing method, which is the searching based on a distributed approach. Before that, in Kleinberg's searching method, he proposed that the possibility of efficient routing depends on a balance between the proportions of shortcut edges indifferent lengths with respect to coordinates in the base grid [13]. In a seminal paper, Sandberg proposed a method of routing that does not depend on such knowledge, which can be implemented in a completely distributed way without any global elements. In a single paragraph in that paper, he attempted to fit it against Kleinberg's model so as to make efficient searches possible. With a good estimate for this embedding, it is possible to achieve greedy routing work without knowing the original positions of the nodes when the graph was generated [14].

Therefore, Sandberg trying to adapt Kleinberg's method, which is more effective. The authors used the Metropolis-Hastings algorithm model to achieve this routing method, and test its results. That algorithm uses the data generated by artificial control to test, whose results proved to be well, it later will also be used for real social network. In the fully distributed routing and switching experiment, the authors also proposed switch with the node at the walk terminal under idealized distribution.

The advantages of this algorithm are that the algorithm is shown to be fully distributed, which indicates an application can be directly connected to the network through their own trusted friends to realize distributed routing and enables the information exchange. However, the disadvantages are that this algorithm has not been proven whether it can also be applied in more general social networks, so the problem is still in the stage of idealized.

3.3. Switching

In 2007, Vilhelm Verendel base on the research of Sandburg's, studied how to speed up his method. The Metropolis-Hastings algorithm essentially used to fit a Kleinberg distribution by trying to embed the nodes of a graph with no position information [12]. In the diagram of the scene generated as the ideal Kleinberg model, without any prior assigned positions, this method is showed to be performed well.

The key of this work is to speed up the algorithm by adding modifications to traditional selection methods. To compare the efficiency of different selection methods later, he simulates two stop criteria and then he proposes three different selection methods to improve the speed the algorithm effects, he call this method as local selection because they relate to the positions that graph neighbors take in the lattice. Finally, he tried to use a different approach: not select switching peers deliberately, instead by including more partners with each step of the Markov chain to step [15].

To his conclusion, the three local selection methods speed up the rate of the stop standard than selecting nodes consistent random. There are also some improvements of doing this if one considers steps of the chain when involved more nodes, but compare with that, a directed switch gives more improvement [15].

4. The new Darknet Routing Mechanism

Darknet, a friend-to-friend network, whose every node only can communicate with the peers he trusts. Therefore, in this situation, his identity just can be showed to trust peers. The detail information of related thesis is shown as follows:

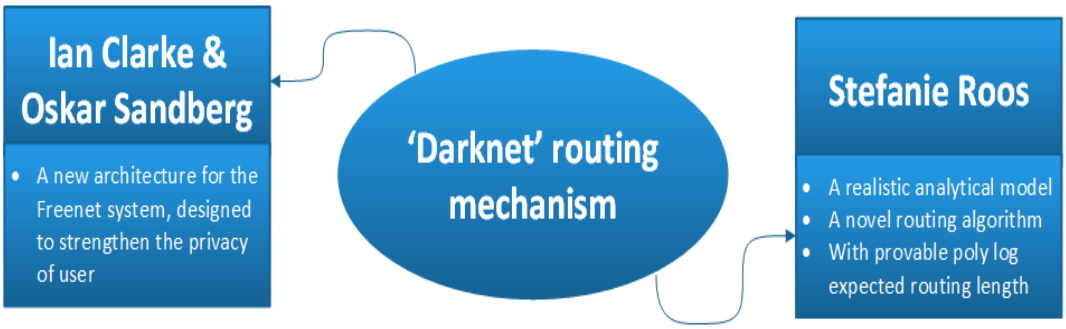

Figure 6. Studies around Darknet Mechanism in Freenet System

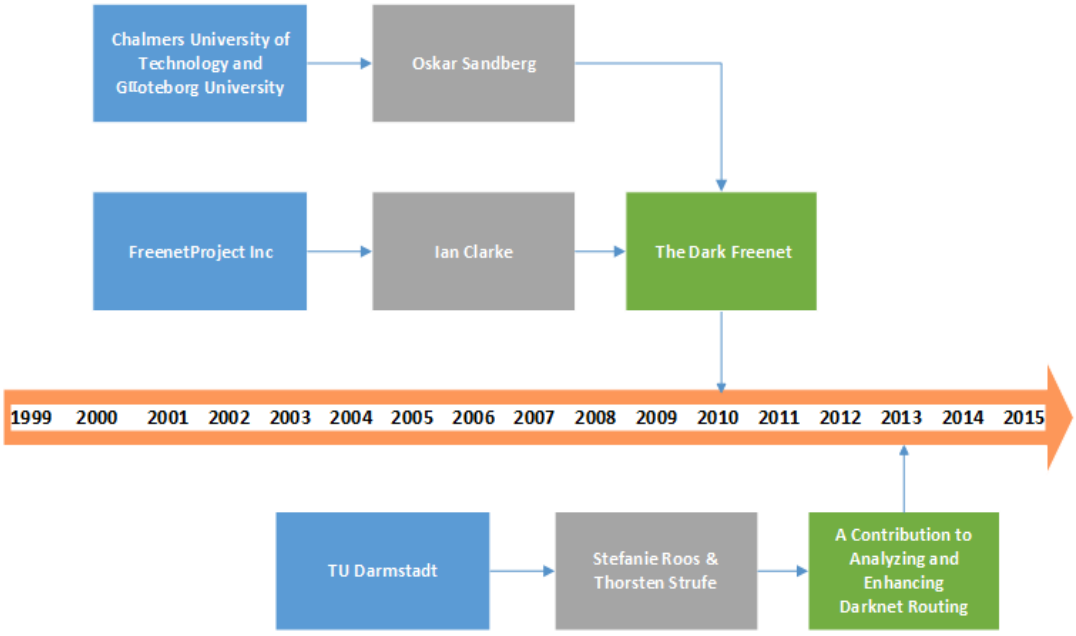

Figure 7. Time Axis for Darknet Studies

4.1. Darknet Mechanism

In a seminal paper Ian Clarke proposed this new architecture; it is a new version of Freenet. In his paper, he remarked on the trusted connection model and simulated the data in the new conditions from Freenet system. According to the model he proposed, the data and the actual deployment of trust partner communications. And did simulations in social network with real data to assess whether this model can provide credible connection, which is expected. In addition, the hybrid model simulation, joins an open network, it can study whether these nodes can coexist on the same network [16].

About the simulation, the first two simulations are based on pure underground network. The third simulation used a small portion of the open network connected to the partner. During the simulation, we can obtain the following results: in the first experiment, which

studies the effect of redundancy on the network load and availability. By simulating a week, based on pure underground network, then it evaluated the success rate and steps to complete the request more than one day.

According to the simulation, the performance of the network depends on the results of the popular file distribution requests. They found that when the storage load in the network increases, this ratio will be larger. This is also due to the large popularity of certain documents, it may cause network load increases. Furthermore, this is the issues which the network has not yet been able to fully resolve.

In the second experiment, they studied the network capacity performance of the amount of churn when a single node removed from the network even loses their data forever. When a node leaves and joins the network, the probability of permanent decreases by changing them. When a node leaves, all the files are lost, it can be reconnect later, but as a "fresh" node has no data. Here, it needs to study node requests and the method of the cached data can compensate the different rates when the node with data leave network. As a result, once there are some documents stored in the network, its last Networks request often will make up for the loss of a particular copy. Meanwhile, this is a mobility Network, when some key value remove, the strategy to avoid the loss may be a problem.

In the final experiment, it access to fixed open network connection by letting some of the trust nodes and dynamic optimization dark network connected to stranger, they studied the open network capabilities, which base on these choices random. Then, it showed that the network can perform well when it cooperates with the Darknet and Opened nodes [16]. Furthermore, they found that both of two connections can rarely influence the load or the availability for the network.

4.2. Topology

The second chapter describes the small world model based on a distributed routing algorithm, which is the beginning of Darknet routing algorithm. Sandberg proposed a new routing implementation. However, this algorithm still has many limitations, it does not achieve the expected length of Freenet routing compared with polylog routing, some ideal design is also difficult to be implemented and have higher maintenance costs. After considering these issues, Stefanie Roos and Thorsten Strafe gave a simplified model and a class of Darknet routing algorithms [17]. Then, they propose a new routing algorithm---NextBestOnce, it can calculate the expected routing length. They did a series of calculations and experiments, and analyze the performance of D^2-*DFS*, which is given by Darknet using a deterministic routing algorithm, and adjusted the node identifiers to the fixed topology [16]. In addition, they point out two drawbacks about D^2-*DFS*. On the one hand, there exists excess message, for the node must be contacted to check whether the message has been passed. On the other hand, nodes are always contacting the news that has not yet been seen, which is a difficult problem to be solved.

Therefore, they present NextBestOnce, which idea is that when one wants to forward message to the neighbor closest to the destination, it can be expected polylog route length [18].With the presentation of this model, they simulated by comparing NextBestOnce and the existed network routing to prove its effectiveness. As the simulation results shows, in the network size between 1000 and 100,000, the deviation is obvious and the difference between these two algorithms also exists, the NextBestOnce is better in general. But the probability in such a small number of runs situation happen at the dark network sizes is low. Thus, if there needs to ensure the length of polylog route, NextBestOnce is a better algorithm. What's more, they also find that the model prove that it's hard to realize the Freenet route in practical, but its will have a positive impact on the future of routing protocols and topologies.

5. Privacy and Anonymity

In this section, we analysis several security approaches to focus on the properties and relations about privacy and anonymous in the most noteworthy and innovative ways. In order to improve its performance, an in-depth understanding of the deployed Freenet system is required.

The detail information of these theses is shown as follows:

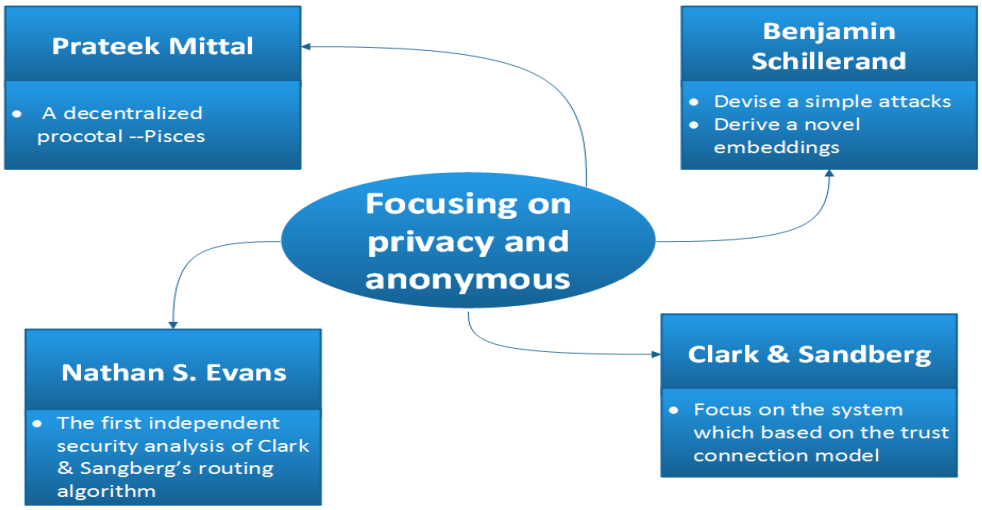

Figure 8. Studies around Privacy and Anonymity in Freenet System

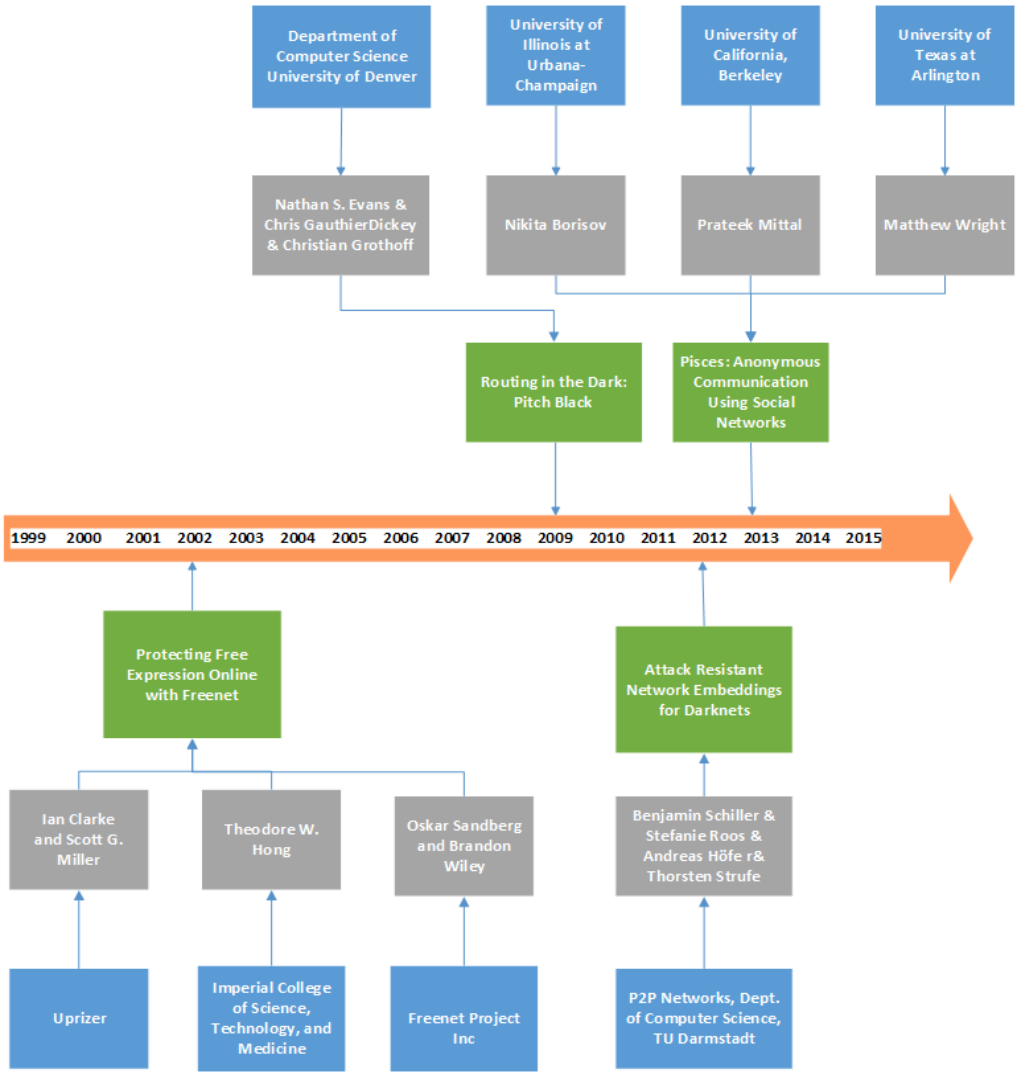

Figure 9. Time Axis for Privacy and Anonymity Studies

5.1. Distributed storage

In order to realize distributed storage, the node typically assigns each node operators a certain amount of disk space to store data. Freenet files are divided into a number of small blocks and create repeat blocks to provide redundancy. Each block is processed independently, which means that a single file may have a number of different components stored in different nodes [16].

The advantage of this storage files is it can spread over different nodes anonymously, the nodes themselves do not know the data storage condition in present node, other nodes cannot trace back to the location of the file, which ensures system anonymity and high design reliability. While,if the data is not used for a long time, it will be discarded by Freenet to ensure the disk space being updated and utilized [2] [3].

5.2. Trusted Connection

Previous generations of Freenet system provide some anonymous queries and data separation, but it is vulnerable to outside attacks. To solve these problems, Ian Clarke R & D team proposed to change the past ideas. In the new design, the nodes can be restricted to only connect the partner nodes they trusted, in the process of establishing; they dynamically generated direct network operations [16]. This model

makes the outside world cannot trace the message node, so it is difficult to attack, which fundamentally improves the anonymity and security of the communication process.

The advantage of the trusted-connection model is that it can keep network away from the Sybil attack [19]. However, the present implement have not performed mix nodes but it may still be a question to avoid attacks to affect the routing.

5.3. Protocols

Prateek Mittal proposes decentralized protocol-Pisces. In the devise process, to avoid the less nodes dominated the create process, that protocol tries to apply a random walk method.

In this paper, they propose to construct circuits by using social networks because they are more likely to compromise than any previous practice dispersed anonymity system .They get the fact that when to be protected from the random walk in social networking, topologies are likely to continue to the honest users. So they have the idea which tries to conFigure to select a random walk on the social network topology in this way that cannot be manipulated by a Byzantine adversary. To prevent the adversary from biasing the random walk by manipulating their routing tables, they propose the reciprocal neighbor policy: the honest nodes can use a tit-for-tat if malicious nodes try to exclude honest nodes during peer discovery [20].

According to above, they designed Pisces, a decentralized anonymity system that uses random walks on the networks (such as Darknet) to take advantages of the trust relationships without being exposed to the circuit operation. They also concluded that its application works well and have strong resilience to active attacks. At last, they showed that Pisces provides significantly higher anonymity than existing approaches using real world social network topologies, and it provides up to six bits higher entropy in a single communication round compared with decentralized approaches that do not leverage social networks [20].

5.4. Data Formats and Encryption

There are mainly two types of the key. The first key, which used for large static pieces of data, is called Content Hash Key (CHK). Since it's generated from the data, it cannot be generated in advance and estimated by somebody without data. However, such keys are still effective in the case that a document needs to provide a link to a copy of a particular static document. The second key, which allows several documents that holds a similar key-pair to be published, is called Signed Subspace Key (SSK). As the name called, the holder of the key-pair has a secret subspace to publish signed documents in the method. This key is used for updating by including a version or a date of publication.

Searching documents in Freenet needs the publishers, so there is no proper method for keyword to search. And the size of documents in Freenet is fixed - 32kB for CHKs, and 1kB for SSKs as a basic measure against data collection and traffic analysis. About the data encryption, Freenet system uses symmetric encryption. The parts are spread around the entire network which allows downloading in a valid way, for inserted base on different keys. Splitting also provides an additional layer of redundancy to make clients use erasure codes to ensure that he doesn't need to use all nodes to recreate the document [16].

5.5. Security Analysis

As an open system, Freenet inevitably has some malicious nodes. Although the system designers have taken measures to prevent them, but Freenet is still faced with many security problems.

Evans, Dickey and Grothoff analysis the security of the Clarke and Sandberg's routing algorithm which is more effective in the Freenet. They try to attack on the Freenet tested

to test the safety performance of the distributed routing algorithms. In this process, they mainly simulate attack test in two ways, destroying the position of the initial random distribution node. The first one attacks the internal node, causing the loss of storage capacity nodes and the network load imbalance, resulting in data loss. The second mode is the reason of location unbalance in a condition without any opponent.

In each experiment, the secret key of the data has random distribution, and the storage space for each node is the same. When iteration start, a particular node is switched to attack mode, which is also randomly selected. If a node in the network does not have enough storage space, the data will be discarded, the key to assess the experiment performance is to find the average route length of the node-specific key [21]. For the purpose of clustering the position of the nodes, an attacker can use the switching technology, which can lead the mismatch of nodes and its responsible key space. In addition, carrying out the experiment in a different topology, they obtained similar results. The experimental results show that when change the way the nodes participates, its performance will be severely degraded, resulting in increased cost routing, and it will make massive data loss in a short period of time [21].

According to the result, some suggestions are proposed to improve the security of the system. The first way authors suggest is to regularly re-initialization of the node random position, increasing the time required to exchange positions. The second method what they proposed is detecting the position of malicious nodes may distribution by estimating the size of the network. In practice, the size of the network is difficult to estimate, but may be judged according to the particular topology.

5.6. Attack Resistant

Network embedding is a procedure which the IDs in the Darknet are assigned. In order to improve the security of the Darknet system, Schiller and other researchers propose a new embedding algorithm and analysis the result of the emulation. The new embedding algorithm uses ASK and TURN which base on a Local Markov Chain (LMC). Then, according to the new algorithm, they take the test.

Under GTNA attack, they analysis and assess the algorithm [22]. The first step is the emulation settings, they simulate a structure, use the communication diagram they established which is built on mutual trust relationship between participants. Next, from more than 500 nodes, they randomly selected the specific malicious nodes and start the iterative process, which completes the simulated attack. In the second step, they made two assumptions and verified. The first is to verify whether the exchange algorithm which Sandberg proposed, satisfied the embedded standard. The result is in the case of where there is no attack, using embedded standard can significantly optimized routing and switching. The second is that in case of attack, verify whether the exchange algorithm is susceptible. Finally, the data showed that attacks will lead to decline in the quality of routing and switching.

On this basis, they assume that the three attacks described in the article may not appear in the LMC. By creating related simulation scene, they found LMC has better quality standards, for it is not vulnerable to such attacks. In conclusion, this new algorithm improves the safety performance of the system as well as the security of user ID [23].

6. Conclusion

In current Freenet routing algorithm, the only way to assess the performance of nodes is attempted. In the next routing, some researchers provide an efficiency unit of measure which can simply compare the node performance. If the algorithm correction makes the results closer to the estimated value, this correction proved to be effective, and the mechanism can dynamically optimize the speed of routing [24].

In this paper, we sort by time of the publication, tease out the development of Freenet system, and provide a brief assessment about the system. Then, we introduce and summarize the main ideas about the small world and the Darknet mechanism. Moreover, we discuss and compare the anonymity and privacy in Freenet system from different aspects. We also analyze the application of relevant algorithm, including the advantages and disadvantages of each strategy, and give further comparisons and prospects.

Acknowledgements

This work is supported by the following programs: the National Natural Science Found ation of China under Grant No.61170273; 2010 Information Security Program of China N ational Development and Reform Commission with the title “Testing Usability and Securi ty of Network Service Software”.

References

[1] https://Freenetproject.org/about.html#why anonymity , last accessed 2015-11-10
[2] I. Clarke. “A distributed decentralised information storage and retrieval system.Unpublished report”, Division of Informatics, University of Edinburgh, **(1999)**.
[3] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong. “Freenet: A Distributed Anonymous Information Storage and Retrieval System”, In: Proceedings of the International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability. New York, NY: Springer-Verlag, **(2001)**, p. 46-66.
[4] https://Freenetproject.org/about.html#introduction , last accessed 2015-11-10
[5] Ihlenfeld, Jens (2006-04-04). "Freenet 0.7 soll globales Darknet schaffen", Golem. Retrieved 28 October 2015. http://www.golem.de/0604/44448.html, **(2006)**.
[6] https://Freenetproject.org/news.html#Freenet-0-7-5-released , last accessed 2015-10-30
[7] https://Freenetproject.org/news.html#build1226 , last accessed 2015-10-30
[8] https://Freenetproject.org/news.html#20150711-1468-release , last accessed 2015-10-30
[9] Milgram, Stanley. "The small world problem", Psychology today 2.1, **(1967)**, pp. 60-67.
[10] Z. Hui, A. Goel, and R. Govindan, "Using the small-world model to improve Freenet performance", INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. Vol. 3. IEEE, **(2002)**.
[11] D. J.Watts, “Small worlds: the dynamics of networks between order and randomness”, Princeton university press, **(1999)**.
[12] J. Kleinberg, "The small-world phenomenon: An algorithmic perspective", Proceedings of the thirty-second annual ACM symposium on Theory of computing, ACM, (**2000)**.
[13] O. Sandberg, “Searching in a small world”,” Diss. Chalmers tekniska högskola, **(2006)**.
[14] O. Sandberg, "Distributed Routing in Small-World Networks", ALENEX, **(2006).**
[15] V. Vilhelm, “Switching for a small world”, Diss. Master’s thesis, Chalmers University of Technology, G öteborg, Sweden, **(2007).**
[16] I. Clarke, "Private communication through a network of trusted connections: The dark Freenet", Network , http://Freenetproject.org/papers.html **(2010)**.
[17] S. Roos, and S. Thorsten, "Provable polylog routing for Darknets", Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on. IEEE, **(2012)**.
[18] S. Roos, and S. Thorsten, "A contribution to analyzing and enhancing Darknet routing", INFOCOM, 2013 Proceedings IEEE. IEEE, **(2013)**.
[19] J. R. Douceur, "The sybil attack", Peer-to-peer Systems. Springer Berlin Heidelberg, **(2002)**, pp. 251-260.
[20] P. Mittal, W. Matthew, and B. Nikita, "Pisces: Anonymous communication using social networks", arXiv preprint arXiv:1208.6326, **(2012)**.
[21] N. S. Evans, C. G. Dickey, and C. Grothoff, "Routing in the dark: Pitch black", Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual. IEEE, **(2007)**.
[22] B. Schiller, "GTNA: a framework for the graph-theoretic network analysis", Proceedings of the 2010 Spring Simulation Multiconference. Society for Computer Simulation International, **(2010)**.
[23] B. Schiller, "Attack resistant network embeddings for Darknets", Reliable Distributed Systems Workshops (SRDSW), 2011 30th IEEE Symposium on. IEEE, **(2011)**.
[24] S. Roos, "Measuring Freenet in the wild: Censorship-resilience under observation", Privacy Enhancing Technologies. Springer International Publishing, **(2014)**.

Authors

Tian-Bo Lu was born in Guizhou Province, China, 1977. He is an Associate professor in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer network.

Zhi-Min Lin was born in Shanxi Province, China, 1993. She is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her technical interests include information and network security, anonymous communication.

Ling-Ling Zhao is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her technical interests include Cyber-Physical System and P2P network.

Yang Li was born in Hunan Province, China, 1978. He is a PhD and his technical interests include information security, distributed computing and P2P network.