International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.25-40
http://dx.doi.org/10.14257/ijsia.2016.10.7.03

Towards a Comprehensive Analysis of Crowds Anonymity System

Tianbo Lu[1], Xinyuan Zhang[1], Xiaofeng Du[2] and Yang Li[1]

[1]*School of Software Engineering, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
[2]*School of Computer Science, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
lutb@bupt.edu.cn, 247958455@qq.com

Abstract

There is an increasing command for anonymity in network. Crowds[1] is an popular anonymity system proposed by Michael K. Reiter and Aviel D. Rubin which main idea behind it is hiding users' identities by routing their packets randomly within a group of similar users. Crowds can provides sender anonymity and also has an advantage that the computation load of relay nodes is very small but it does not protect the identity of the receiver. This paper presents an overview on Crowds and introduces the development of Crowds from the following aspects: anonymity analysis, application especially the application in P2P and the performance. We summarize the work about anonymity analysis based on Crowds and divide them into receiver analysis, probabilistic behavior, attack and anonymity proof. Crowds is high efficient but it can't resist the global attack, therefore, to meet the needs of the different levels of anonymity, there is a vast body of anonymity literature concerned with anonymity analysis, for example, Crowds can't provide receiver anonymity but receiver anonymity is important in many cases, so many work extending the Crowds system from sender anonymity only to sender and receiver anonymity. In addition to the analysis, we also summarize the applications of Crowds. Undoubtedly, it is widely used in P2P. We also give an overlook of the performance of Crowds.

Keywords*: component; Crowds; anonymity system; receiver anonymity; p2p*

1. Introduction

Crowds protocol was proposed by Bell Laboratories in 1998 [1], which aims to protect users' privacy when they are browsing the web. It enables users to retrieve information from the web server without leaking their information to the web server or third party, such as IP addresses and domain names. The idea of Crowds is "mixed in the crowd", meaning that they conceal themselves in the population. It is a peer-to-peer network with a different path selection policy from the Mix-net [40] system where each node in the system can forward messages on behalf of other users as well as themselves. Crowds organize the users into a group called the crowd that can execute web transactions on behalf of the user. User in Crowds is a proxy representation which is installed on his computer called Jondo. When someone in Crowds browses web, his request will be forwarded by local Jondo to another Jondo or the terminal server. When a Jondo receives the request sent by another Jondo in Crowds, it has certain probability to be forwarded to any other Jondo, or forwarded to the server. Thus, Web servers, and other members of the Crowds as well as the third-party observer can't determine who initiated the request.

ISSN: 1738-9976 IJSIA

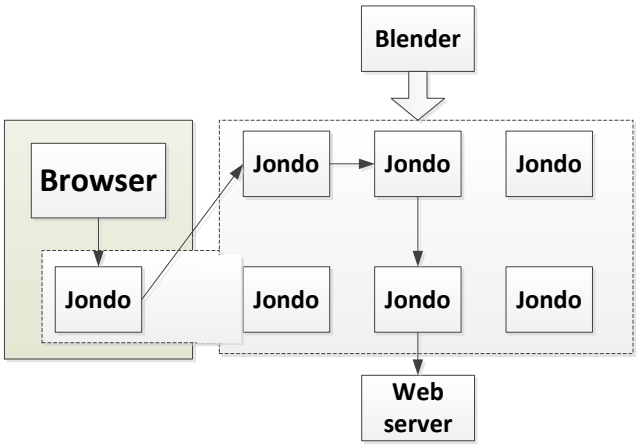


Figure 1. Structure of Crowds

Each node that forwards a packet to another node records who is the predecessor. In this way, a virtual tunnel is built, which is used for the communication between the sender and the receiver. As each node only stores information about its predecessor, it is impossible for an intermediate node to be aware of the whole path nor the sender identity. Subsequent requests initiated at the same Jondo follow the same path (except perhaps going to a different end server), and server's replies traverse the same path as the requests, following the reverse way.

In Crowds, when a user requests a web page, he selects a Jondo randomly to sends the request with encrypted, so that the attacker can't see anything. After receiving the request, the Jondo firstly decrypts it to get the destination address then it will send the request which own the probability p_f to A possible such path is shown in "Figure 2". In this figure, the path is R1 → R3 (with probability $\frac{1-p_f}{1-n}$) →server (with probability p_f).

Jondos are report and control by a server called blender, in order to use the blender server. In order to establish contact with blender, the user must first set up an account and save his name and password on the blender server. When the user starts his Jondo, Jondo and blender communicate with each other with the shared password, and then blender add the new user to a list of members of Crowds, and share the list to the new user. In addition, blender server generates a shared key and report table in which each key can be used to verify the other group members, and blender will notify other members of the new members joining in the system, so that all members of the system are informed of the new member. Each member in Crowds has its own Jondo member table, this table is initialized when the Jondo join the group.

When receive information that new member join in or someone removed by the blender, Jondo update the table. If a Jondo fails to connection someone in the table, the Jondo will remove it and update the table. The structure of Crowds look like "Figure 1".

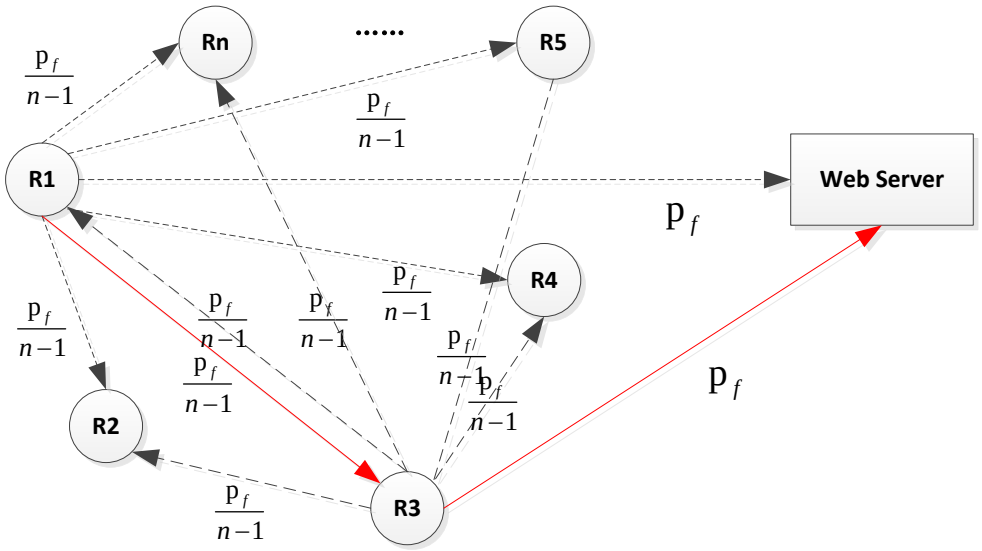


Figure 2. Example of a Path in Crowds System

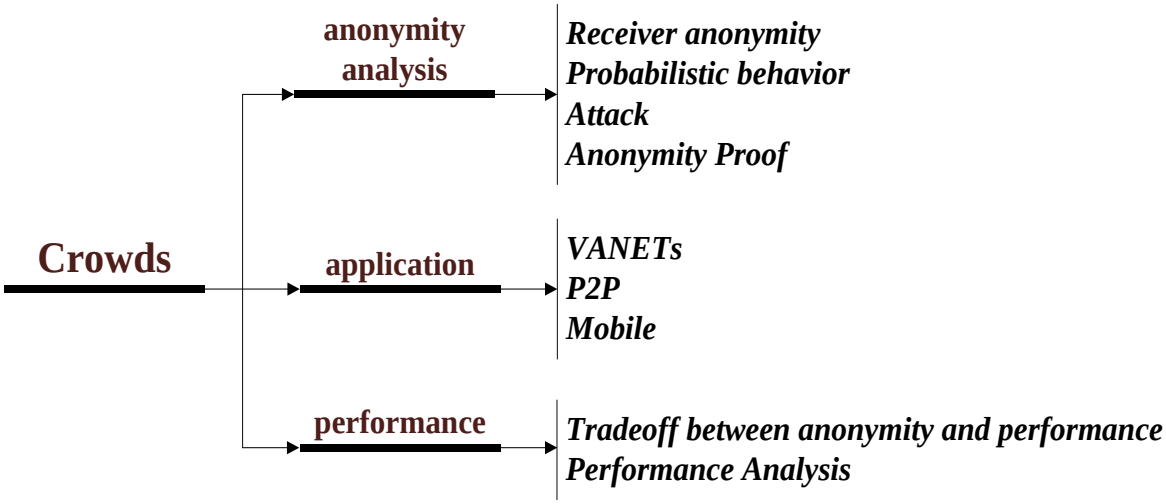


Figure 3. Development of Crowds

Because of its simple and efficient features, Crowds caused extensive discussion and quickly became a popular anonymity schema since it had been proposed. In this article, we will summarize for Crowds of the previous studies, the extension and the application of Crowds. These studies will be broadly divided into three areas as shown in "Figure 3".

2. Anonymity Analysis

There is a vast body of anonymity literature concerned with anonymity analysis. In order to compensate the defects of Crowds that can only provide sender anonymity, most of the works are associated with receiver anonymity, due to their works the need of sender anonymity and receiver anonymity can be realized. [23] and [29] combine Crowds and Mix-Nets to achieve the receiver anonymity. The paper [25] proposed a sender anonymity and receiver anonymity scheme called Crowds6, it is based on the protocol of

IPv6. In the work of [11], they propose an anonymous scheme system based on probabilistic choice of actions and multiple loopbacks solving the problem that how the identity of a proper receiver is protected without encryption. There are a lot of other work about anonymity analysis. [3] considers the participants' probabilistic behavior and provide a system named Crowds-Trust which achieves 'probable innocence' and [2], [9],[38] talk about the attack. Anonymity proof is a key concern in anonymity area, guaranty that the anonymity system is really effective is an important challenge. For this purpose, there are a lot of work to prove the correctness of anonymous communication systems. [5] and [32] verify Crowds with IOA and [24] uses the probabilistic model checker PRISM to analyze the Crowds. In addition to these traditional verification methods, there are also a lot of works advanced new method to analysis the correctness of Crowds such as [29], [34] and [27]. The structure of this part shown as "Figure 4".

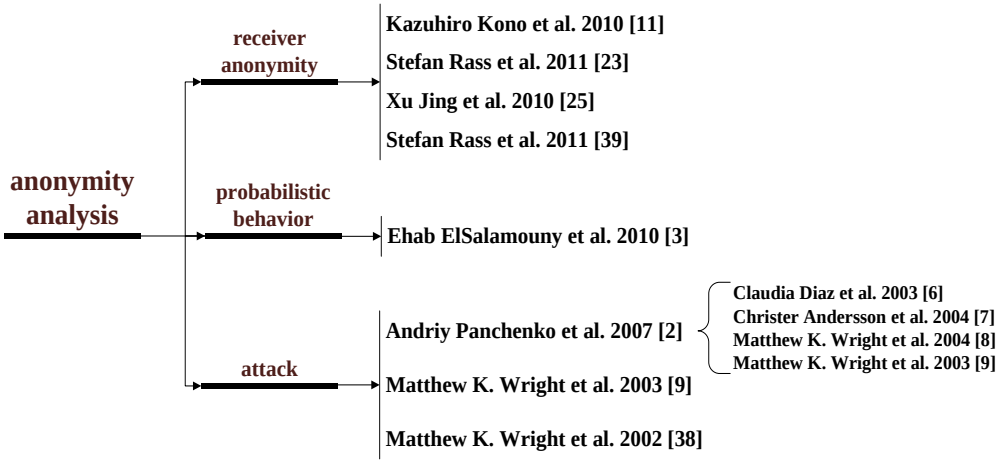


Figure 4. Anonymity Analysis

2.1. Receiver Anonymity

Crowds only provide sender anonymity, in some cases, that can't meet the needs for users. Therefore, extending the Crowds system from sender-anonymity only to both, sender and receiver anonymity becomes very meaningful. [23], [39] are about helping to implement sender and receiver anonymity of Crowds system. Their intention is improving the Crowds to protect the receiver's privacy like it protects the sender by combining Crowds with a Mix-Nets, where replaced the public key encryption by a secure transmission protocol. They prove such a system can achieve absolutely receive anonymity only when the network size towards infinity and their main contribution is demonstrate that how a certain level of anonymity is achievable in finitely large networks.

Crowds does not solve the key distribution problem on the routing paths between the sender of the request and the last node due to its implementation mechanism, so the message content and recipient addresses are forwarded in clear text and all members can see them on the routing path. In this context, Crowds system can't achieve the receiver anonymity. In the work of [25], receiver anonymity is achievable by solving the problem of sharing the key between the sender and last-hop on the routing path. The scheme proposed by [25] named Crowds6 which based on the protocol of IPv6. The main idea of Crowds6 is selecting the last-hop which called keynode in Crowds6 of all jondos on the routing path by the sender randomly and using the keynode's public key to encrypt symmetry key which is used to decode the message content .The only work of other jondos is forwarding the message to the keynode. After receiving the packet, the keynode uses its private key decrypt the message to get the symmetric key and get the address of the receiver further. "Figure 5" shows the structure of the message.

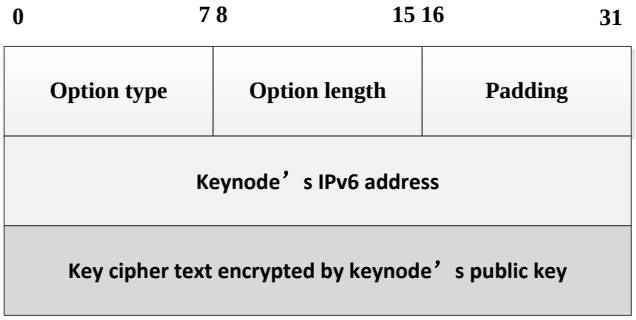


Figure 5. Example of a message in Crowds6

In the paper [11], they propose an anonymous scheme system based on probabilistic choice of actions and multiple loopbacks solving the problem that how the identity of a proper receiver is protected without encryption, in which it is able to avoid the weak point in Crowds system that the destination of the message indicates the receiver of the message. Their scheme has three communication modes, respectively S-Mode, R-Mode and L-Mode. S-Mode represents Straight Mode, it means that a node in the system will send the message to its destination directly. R-Mode is called Relay Mode, in this mode, the received message will be transmitted to another node instead of the destination node. The last mode L-Mode is called Loopback Mode, when a node chooses this mode, it changes the destination of the message to itself so that it will forward the message to itself and thus the node will perform the action of "loop back". Owing to the existence of the L-Mode, the nodes in the routing path can't distinguish whether the destination of the message is the destination of the receiver or not. So the system can achieve the receiver anonymity. "Figure 6" shows the action of a node in the system.

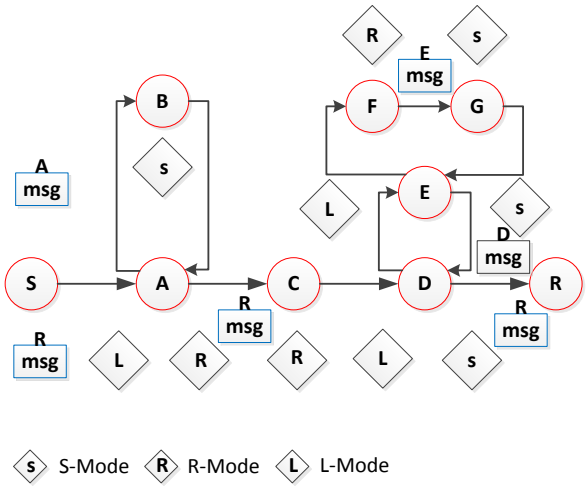


Figure 6. Example of Nodes Action in the System

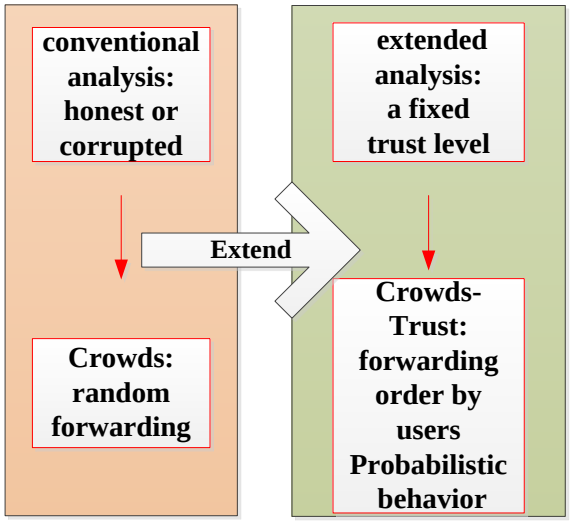


Figure 7. Expansion of Crowds-Trust

2.2. Probabilistic Behavior

The existing work on the analysis of Crowds anonymity most simply divide the users for honest or corruption, and the authors of [3] think that is not practical and trust plays a major role in deciding the forwarder. With this work the paper aims to make the next step in the security analysis of Crowds. They want to extend conventional analytical methods which participants is just honest or corrupted so that they use a fixed trust level t∈[0, 1] to determine the probability whether a node is honest. The paper assess to the impact on the Crowds security of its participants' probabilistic behavior. Therefore they provide the following program to this topic: First they assign a fixed trust level ti (values in [0, 1]) for each participant on behalf of its robustness to resist corruption, and a fixed performance level qi. Then extend the protocol to change the forwarding policy which no longer forwarding randomly but according qi to choose to the forwarding nodes. According to this model ("Figure 7"), the authors formulate the necessary conditions to achieve 'probable innocence'. These conditions can then be used to propose a new protocol named Crowds-Trust which uses trust information to achieve 'probable innocence' for principals exhibiting probabilistic behavior. They also derive expressions for different level of anonymity required.

2.3. Attack

The paper [2] analyses the anonymity of Crowds by calculating how many observations the colluding members have to make in a Crowds system to determine the frequency a node communication with a server within arbitrary precision shown as "Figure 8". The calculation results show that the crowds system can't provide good security because the number of rounds required by collusion attacker to determine the frequency of Crowds nodes communicate with the server is quite small, but the precision is very high. The paper propose the corresponding solution by introducing "an adaptive behavior of the honest system members" .In this scheme, each honest node observes the network like the attacker dose, but these observations are limited to their own and the nodes don't sharing the observation result with each other. According to the traffic analysis made by the honest node, it can estimate the sending rate of other nodes and calculate the maximum frequency it can communicate with server without being detected by the attacker.

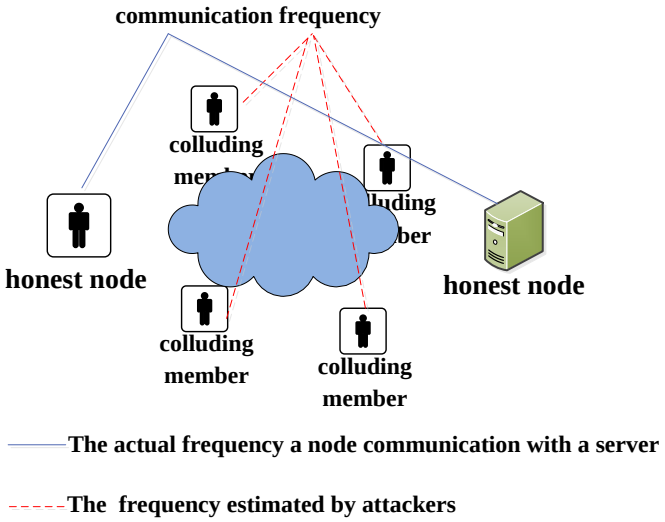


Figure 8. Example of a Node Communication with Server

2.4. Anonymity Proof

The formal method has already been applied to analyze distributed systems and it can also be used to study the anonymous communication systems, such as [12] and [14], the method used in [14] is Mull Krakow chain and the method in [12] considers theorem-proving.

The main idea behind [5] is formalizing and verifying Crowds with IOA by using computer-assisted tools. They demonstrate the anonymity of the Crowds communication system based on the method introduced by [12]. In their work, they acquire the specification of Crowds system with an I/O-automaton-based formal specification language and get the first-order logic by putting the specification to a formal verification tool. Consequently, the simulation results prove the anonymous of Crowds system and they also prove the anonymous of other system based on Crowds [11].

3. Application

Since the Crowds anonymity protocol has been proposed, it has been widely used due to the simple and efficient characteristics. Crowds is ideally suited for P2P environment for its nature so that much study expand Crowds and used it in P2P network to provide anonymity. [17] proposes BitBlender which designed for BitTorrent protocol and [15] is

for file sharing system. Dual-Path [19] is also proposed for providing anonymity of P2P network. [18] and [20] discuss the problem about the nodes join and leave the network frequently. All of these scheme are based on Crowds and designed for P2P network. Crowds is also used in other fields like VANETs[16] and mobile[7][21]. The structure of this part shown as “Figure 9”

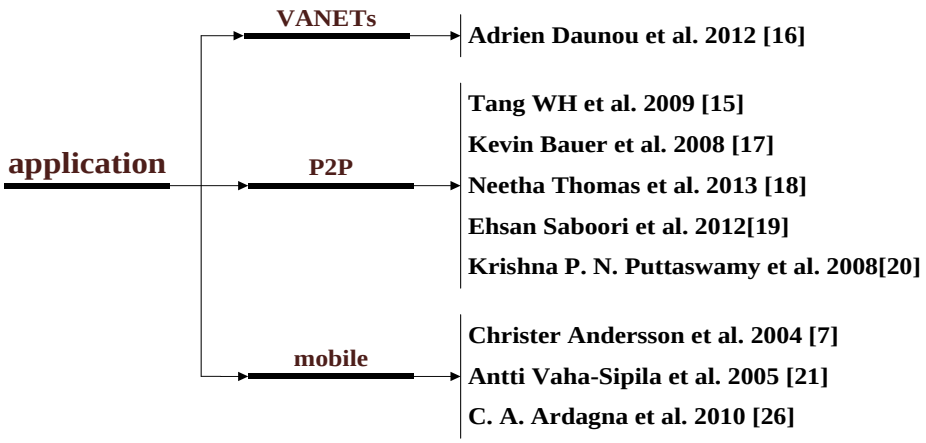


Figure 9. Application

3.1. VANETs

People pay more and more attention on traffic safety, so the Vehicular Ad hoc NETworks (VANETs) have emerged. VANETs can support intelligent inter-vehicle communication and provide information on road traffic conditions to improve car safety. The anonymity is a very important factor in VANETs, [16] implement an anonymity solution based on Crowds protocol used in VANET environment. “Figure 10” illustrates the structure of the network.

3.2. P2P

P2P is a dynamic, scalable network that can be used to share files, telephony, discussion forms, and streaming media. The node in P2P can freely join and leave. Each node can be connected to any other nodes and can send or receive data from each other. Crowds is a P2P anonymity protocol and very suitable for P2P network, so that there are much work based on Crowds to provide anonymity for p2p network.

BitBlender is introduced by [17], it is designed for the p2p protocol, BitTorrent, to provide the user privacy which is not considered in the BitTorrent. The main purpose of BitBlender is to provide a low-overhead anonymity layer for BitTorrent to achieve deniability. BitBlender provide deniability by introducing a special node called "relay peers" shown as “Figure 11”, it can on behalf of active nodes to transmit data. When a node requests for a document, the node can’t be determined that these data is coming from the normal node or relay peers. Thus, the anonymity provided by the system is dependent on the proportion of normal nodes and relay peers involved in the file transfer. However, the expected cost is also dependent on the amount of relay peers involved in the transmission.

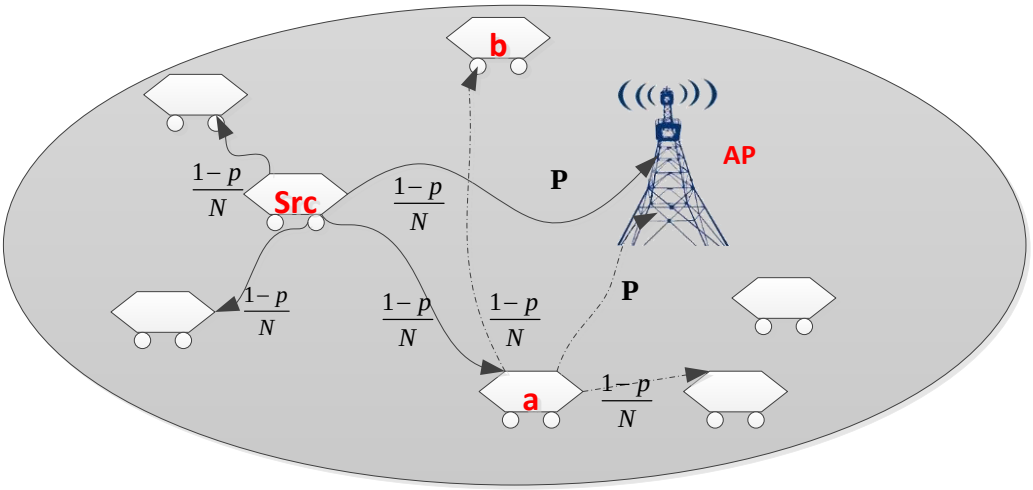


Figure 10. Structure of VANETs based on Crowds

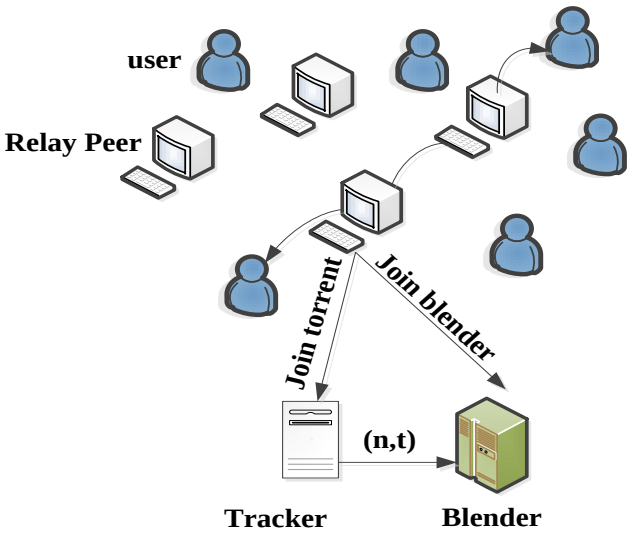


Figure 11 Relay nodes

Dual-Path [19] is an approach to provide anonymity for P2P network. This approach provides anonymity with a trusted server "suppernode". By this approach, the receiver can't identify who is the requester and any other nodes can't determine the two communicating parties. The requester has established two paths to transmit data. These two paths are called Request path and Response path. Request path is for sending a request and the Response path is for transmitting the requested data to the requester. Response path is embedded in Request path, the receiver only knows the first peer on the Response path. "Figure 12" shows them. To this end, the message must be encrypted as onion routing like "Figure 13" and "Figure 14".

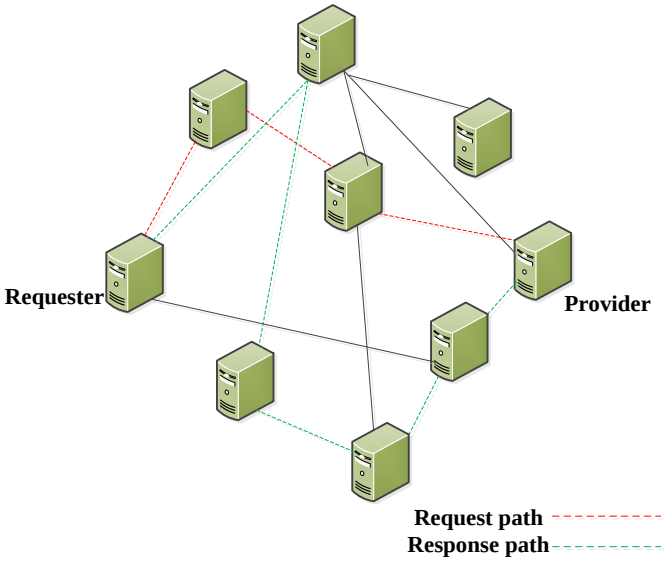


Figure 12. Request Path and Response Path

A major challenge to realize anonymity communication in p2p environment is the node dynamically join or leave the network leading the anonymous routing paths frequently reconstruction. Dynamically join and leave will reduce efficiency, and also lead to disclosure of information due to logging attacks, such as the predecessor attack especially when the path is long. [18] and [20] discuss on this aspect.

Many anonymity protocol like Mix, Tor have to construct the path before starting a request. One disadvantage of this is that if a node leaves the P2P network, the initiator has to reconstruct the path again. We call these approaches as path-based approaches. [18] proposes a new strategy, Rumor Riding(RR), to solve this problem. In contrast with Tor, Rumor Riding is a non-path-based anonymity approach for decentralized P2P systems. RR using symmetric encryption instead of using asymmetric encryption, therefore Rumor Riding is lightweight. In RR, an initiator encrypts the message with a symmetric key, and then send the key and the cipher text to different neighbors. The key and the cipher texts take random walks separately in the system, where each walk is a rumor. The key rumor and a cipher rumor meet at some peer, the peer is able to recover the original query message and act as an agent to issue the request for the initiator.

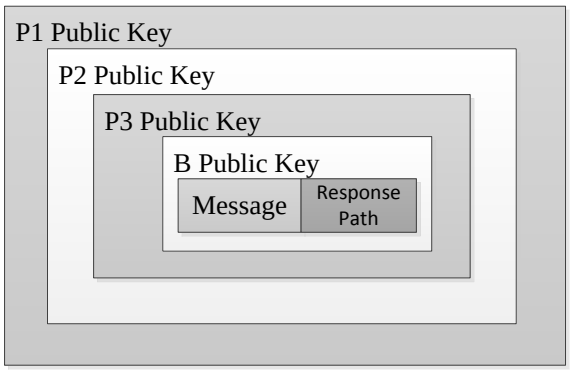


Figure 13. Request Message

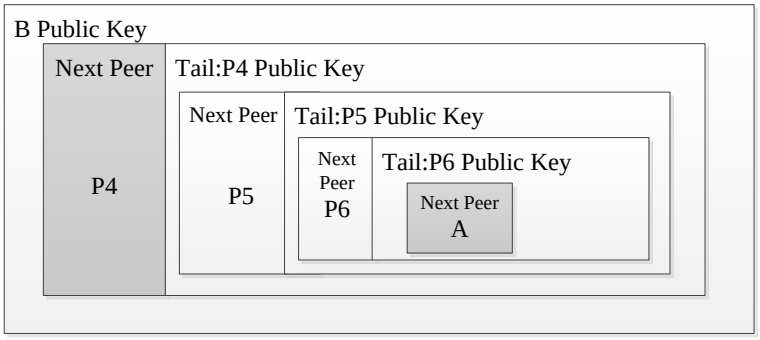


Figure 14. Response Message

3.3. Mobile

In today's rapid development of mobile Internet, mobile applications anonymous communication has become a hot topic. [7], [21] and [26] are talk about it.

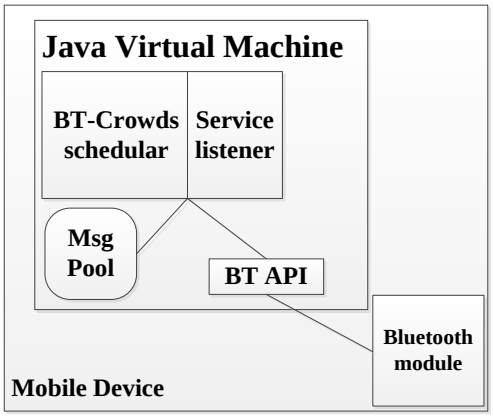


Figure 15. Internal Organization of a BT-Crowds Jondo

BT-Crowds[7] describes a store and forward Crowds which uses the Bluetooth protocol stack and provides enhanced privacy protection. The internal organization of a BT-Crowds jondo is shown in "Figure 15", each jondo include Bluetooth protocol stack, Bluetooth API and BT-Crowds applications. A BT-Crowds jondo like an HTTP server, they receive OBEX PUT request. On the other hand, BT-Crowds jondo likes an HTTP client, it sends the OBEX PUT request to the other jondos. There is a message pool between the server and the client which is used to transmit the message. The message pool is persistent, that is, it is always alive when user using it. Message in the message pool is sent after a period of time.

In BT-Crowds, there are three jondos: normal jondos, gateway jondos and kiosks. normal jondos like jondos in Crowds, they forward the message to other jondos. Gateway jondos forwards the message to the final recipient, a properly configured phone can serve as a gateway jondos. Kiosks are specially configured jondos, which is located in physically crowded places. Kiosks can be installed in crowded places through rational urban planning, through them people can freely communicate anonymously by phone in the street.

4. Performance

Crowds is more effective than many anonymity schema but in some case, it is not effective enough. So there are many study about how to tradeoff between anonymity and

performance such as [22], [28], [30], [35]. There are also much work to prove the performance about Corwds such as [4]. The structure of this part is shown as “Figure 16”

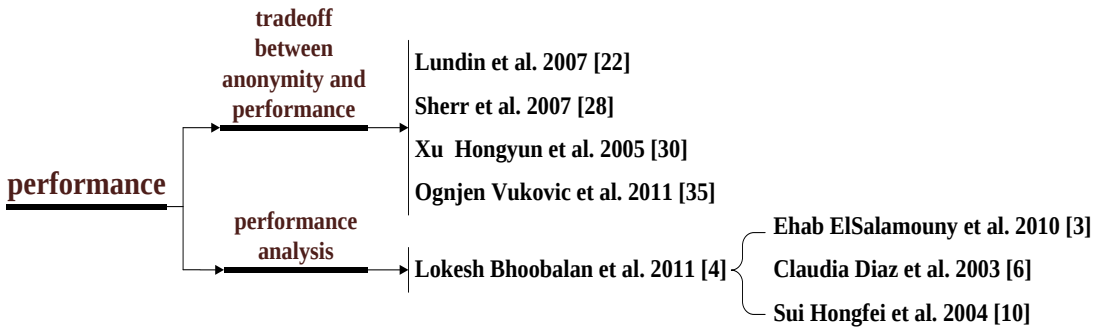


Figure 16 Performance

4.1. Tradeoff between Anonymity and Performance

Not only many applications want to be able to choose the route, but also want to adjust the performance and anonymity in order to meet their specific needs. For example, the anonymous video conferencing systems require high bandwidth and low latency, but it is willing to endure the anonymity of only innocence. In contrast, an anonymous e-mail system may require very strong anonymous (for example, beyond suspicion), without any restriction of bandwidth or latency.

A^3 [28] is designed to meet specific performance and security for applications. Its designers believe that the existing anonymity scheme in order to pursue anonymity expense to much performance. A^3 proposes a routing algorithm that takes into account performance and anonymity. By adjusting the parameters, users can choose a suitable path to meet their need.

Anonymity systems typically use re-routing to increase the robustness of the system. However, a very long path will lead to a larger re-routing overhead and reduce the quality of service (QoS). Scalar Anonymity System (SAS) provides a compromise between anonymity and costs in order to meet the different requirements of different user's specific need [30]. SAS provides the user adjust anonymity. On the basis of an application's requirements on QoS, the user can adjust the desired degree of anonymity. Scalar Anonymity System works as “Figure 17”. The requester Alice select a forwarding probability and the message has a probability to be sent to next node on the path and has a probability 1- to be sent to the receiver Bob. Other nodes on the pass have a weight which is much bigger, the probability that it is selected is higher. If a node on the pass receives the message, it does the same thing that Alice did. Users can choose different forwarding probabilities, and so select a desired level of anonymity.

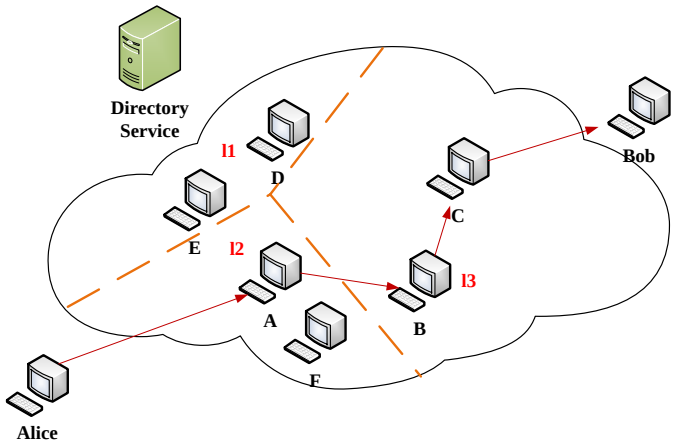


Figure 17. ScalarAnonymity System

4.2. Performance Analysis

[4] provides several experimental results to validate the operation of a crowd anonymity network. They prove that the increase of hop count is very slow and the delay is more for huge increase in the member count, this is beneficial for community adopting this service and cannot be adopted for systems that require faster response. The results also show when the probability is less than 0.85, the hop count increase slowly even for the large number of nodes. So Crowds provides efficient service.

5. Conclusion

In this paper we summarize the previous work of Crowds. We divide them into three parts namely anonymity analysis, application and the performance. We talk about receiver anonymity, probabilistic behavior, attack and anonymity proof and share the application of Crowds in VANETs, P2P environment and mobile. Final we summarize the study about performance of Crowds. We introduced the main idea of some schema, and for other schema not covered, if you're interested, you can check out by yourself based on the references.

In the future, our work is to propose a scheme based on Crowds working in p2p environment which providing sender anonymity and receiver anonymity, and having the ability to tradeoff between anonymity and performance.

Acknowledgements

This work is supported by the following programs: the National Natural Science Foun dation of China under Grant No.61170273; 2010 Information Security Program of China National Development and Reform Commission with the title “Testing Usability and Sec urity of Network Service Software”.

References

[1] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for web transactions", ACM Transactions on Information and System Security (TISSEC) 1.1, **(1998)**, pp. 66-92.
[2] A. Panchenko and L. Pimenidis, "Crowds revisited: Practically effective predecessor attack", Proceedings of the 12th Nordic Workshop on Secure IT-Systems (NordSec 2007), **(2007)**.
[3] V. Sassone, E. ElSalamouny and S. Hamadou, "Trust in Crowds: probabilistic behaviour in anonymity protocols", Trustworthly Global Computing. Springer Berlin Heidelberg, **(2010)**, pp. 88-102.
[4] L. Bhoobalan and P. Harsh, "An Experimental Study and Analysis of Crowds based Anonymity", The 2011 International Conference on Internet Computing, **(2011)**.
[5] Y. Kawabe, "Formalizing and Verifying Anonymity of Crowds-based Communication Protocols with IOA", INTERNET 2012, The Fourth International Conference on Evolving Internet, **(2012)**.
[6] C. Diaz, "Towards measuring anonymity", Privacy Enhancing Technologies, Springer Berlin Heidelberg, **(2003)**.
[7] C. Andersson, R. Lundin and S. Fischer-Hübner, "Privacy Enhanced Wap Browsing With Mcrowds Anonymity Properties And Performance Evaluation Of The Mcrowds System", ISSA, **(2004)**.
[8] M. K. Wright, "The predecessor attack: An analysis of a threat to anonymous communications systems", ACM Transactions on Information and System Security (TISSEC), vol. 7, no. 4, **(2004)**, pp. 489-522.
[9] M. Wright, "Defending anonymous communications against passive logging attacks", Security and Privacy, 2003. Proceedings. 2003 Symposium on. IEEE, **(2003)**.
[10] H. Sui, "The cost of becoming anonymous: on the participant payload in crowds", Information processing letters 90.2, **(2004)**, pp. 81-86.
[11] K. Kono, Y. Ito and N. Babaguchi, "Anonymous communication system using probabilistic choice of actions and multiple loopbacks", Information Assurance and Security (IAS), 2010 Sixth International Conference on. IEEE, **(2010)**.
[12] Y. Kawabe, "Theorem-proving anonymity of infinite-state systems", Information Processing Letters 101.1, **(2007)**, pp. 46-51.
[13] I. Hasuo and Y. Kawabe, "Probabilistic anonymity via coalgebraic simulations", Programming Languages and Systems. Springer Berlin Heidelberg, **(2007)**, pp. 379-394.
[14] S. Schneider and A. Sidiropoulos, "CSP and Anonymity", Computer Security—ESORICS 96. Springer Berlin Heidelberg, **(1996)**.
[15] W. H. Tang and H. W. Chan, "MIX-Crowds, an Anonymity Scheme for File Retrieval Systems", INFOCOM 2009, IEEE, vol., no., **(2009)** April 19-25, pp. 1170,1178,
[16] A. Daunou, "Design of a privacy-aware routing protocol for vehicular ad hoc networks", **(2012)**.
[17] K. Bauer, "BitBlender: Light-weight anonymity for BitTorrent", Proceedings of the workshop on Applications of private and anonymous communications, ACM, **(2008)**.
[18] N. Thomas, "A Protocol for Peer-Peer System to Provide Anonymity", International Journal of Scientific and Research Publications: 179.
[19] E. Saboori, M. Rafigh and A. Nooriyan, "Analyzing the Dual-Path Peer-to-Peer Anonymous Approach", arXiv preprint arXiv:1208.3022, **(2012)**.
[20] Puttaswamy K. P. N., Sala A. and Wilson C., "Protecting anonymity in dynamic peer-to-peer networks[C]", //Network Protocols. ICNP 2008. IEEE International Conference on, pp. 104-113.
[21] A. Vaha-Sipila and T. Virtanen, "BT-Crowds: Crowds-Style Anonymity with Bluetooth and Java", System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on , vol., no., **(2005)** Jan. 03-06, pp. 320a,320a.
[22] R. Lundin, S. Lindskog and A. Brunstrom, "Analysis of Anonymity Services from a Tunable Perspective", The Future of Identity in the Information Society: Proceedings of the Third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on The Future of Identity in the Information Society, Karlstad University, Sweden. IFIP, **(2007)**.
[23] S. Rass, R. Wigoutschnigg and P. Schartner, "Doubly-anonymous crowds: Using secret-sharing to achieve sender-and receiver-anonymity", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 7.4, **(2011)**, pp. 25-39.
[24] V. Shmatikov, "Probabilistic Model Checking of an Anonymity System", Journal of Computer Security 12, **(2003)** 2004.
[25] X. Jing, "Recipient Anonymity: An Improved Crowds Protocol Based on Key Sharing", Information Engineering (ICIE), 2010 WASE International Conference on, vol. 4. IEEE, **(2010)**.
[26] C. A. Ardagna, "Providing mobile users' anonymity in hybrid networks", Computer Security–ESORICS 2010. Springer Berlin Heidelberg, **(2010)**, pp. 540-557.
[27] G. Danezis and E. Käsper, "The dangers of composing anonymous channels", Information Hiding. Springer Berlin Heidelberg, **(2013)**.
[28] M. Sherr, B. T. Loo and M. Blaze, "Towards Application-Aware Anonymous Routing", HotSec, **(2007)**.
[29] N. Jaggi, U. MarappaReddy and R. Bagai, "A three-dimensional approach towards measuring sender anonymity", Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. IEEE, **(2011)**.

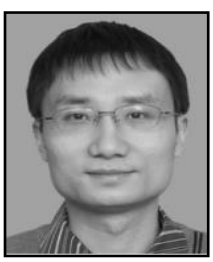
[30] H. Xu, "SAS: A scalar anonymous communication system", Networking and Mobile Computing. Springer Berlin Heidelberg, **(2005)**, pp. 452-461.
[31] J.-Q. Shi, B.-X. Fang and B. Li, "Towards an analysis of source-rewriting anonymous systems in a lossy environment", Parallel and Distributed Computing: Applications and Technologies. Springer Berlin Heidelberg, **(2005)**, pp. 613-618.
[32] Y. Kawabe and H. Sakurada, "A formal approach to designing anonymous software", Software Engineering Research, Management & Applications, 2007. SERA 2007. 5th ACIS International Conference on. IEEE, **(2007)**.
[33] J. P. Munoz-Gea, "A low-variance random-walk procedure to provide anonymity in overlay networks", Computer Security-ESORICS 2008. Springer Berlin Heidelberg, **(2008)**, pp. 238-250.
[34] L. Bhoobalan and P. Harsh, "An Experimental Study and Analysis of Crowds based Anonymity", The 2011 International Conference on Internet Computing, **(2011)**.
[35] O. Vukovic, "On the Trade-off between Relationship Anonymity and Communication Overhead in Anonymity Networks", IEEE International Conference on Communications 57.4, (2011), pp. 1-6. Danezis, George, "The wisdom of Crowds: attacks and optimal constructions", Computer Security–ESORICS 2009. Springer Berlin Heidelberg, **(2009)**, pp. 406-423.
[36] R. Wigoutschnigg, P. Schartner and S. Rass, "Shared Crowds: A Token-Ring Approach to Hide the Receiver", Availability, Reliability and Security (ARES), 2013 Eighth International Conference on. IEEE, **(2013)**.
[37] M. Wright, "An Analysis of the Degradation of Anonymous Protocols", NDSS, vol. 2, **(2002)**.
[38] S. Rass, R. Wigoutschnigg and P. Schartner, "Crowds based on secret-sharing", Availability, Reliability and Security (ARES), Sixth International Conference on. IEEE, **(2011)**.
[39] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM 24.2, **(1981)**, pp. 84-90.

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.

Xin-Yuan Zhang, was born in Liaoning Province, China, 1990. 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.

Xiao-feng Du was born in Shaanxi Province, China, 1973.He is a Lecturer in School of Computer, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer 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.