http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (6): 1165-1171, 2010
ISSN 1812-5638

Survey of Anonymity and Authentication in P2P Networks

[1,2]Xiaoliang Wang, [3]Lincong Yang, [1]Xingming Sun, [4]Jinsong Han, [1]Wei Liang and [5]Lihong Huang
[1]School of Computer and Communication, Hunan University, Changsha, 410082, China
[2]College of Information and Engineering, Xiangtan University, Xiangtan, 411105, China
[3]School of Journalism and Communication, Hunan University, Changsha, 410082, China
[4]School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi, China
[5]College of Mathematics and Econometrics, Hunan University, Changsha, 410082, China

Abstract: Anonymity has received increasing attention in the literature due to the users' awareness of their privacy nowadays. While anonymity related issues have been extensively studied in peer-to-peer (P2P) systems, numerous concerns have been raised about the issue of providing authentic partners in P2P systems. In addition, the network authority requires authentication so that misbehaving entities in the network remain traceable. This study analyzes this problem and reviews related researches. Besides, we also advise some possible methods for this problem.

Key words: P2P, anonymity, authentication, traceability

INTRODUCTION

As an emerging model of communication and computation, peer-to-peer (P2P) networking has recently gained significant attention.

Numerous concerns have been raised about the issue of providing authentic partners in P2P systems. To guarantee authentic responders, some researchers have built trust models to help peers verify the validity of other entities. A number of approaches have been proposed to provide reliable authentication in the P2P systems. Some use reputations or web of trust as authentication access. Other researchers have adopted cryptography to attain security authentication (Akleylek *et al*., 2005; Lua, 2007; Narasimha *et al*., 2003).

At the same time, privacy is an important issue in current P2P systems. Taking Gnutella as an example, the identity of a requesting peer can only be hidden to further peers, but visible to all his neighbors. The identity of a peer who responds with query results is exposed to every peer in the returning path. Privacy is demanded in P2P systems. Hence, a number of methods have been proposed to provide anonymity such as P5 (Sherwood *et al*., 2002) and APFS (Scarlata *et al*., 2001) Tarzan (Freedman and Morris, 2002), MorphMix (Rennhard and Plattner, 2002) and WonGoo (Lu *et al*., 2004). Most, if not all of them, deliver messages via non-traceable paths comprised of several anonymous proxies or middle agent peers or adopt onion router technique (Syverson, 1998). However, failure to support authentication makes these approaches vulnerable to impersonation and man-in-middle attacks.

TRUST AND AUTHENTICATION

Many articles concern about providing trust and reliable authentication in the P2P systems. Wu *et al*. (2008) used the incomplete experience to get the trust rating in P2P systems and use aggregation mechanism to indirectly combine and obtain other peer's trust rating. Simulation results and analysis show that their proposed trust management model can quickly detect the misbehavior peers and limit the impacts of them in a P2P file-sharing system. EigenTrust (Kamvar *et al*., 2003) provides each peer in the network a unique global trust value based on the peer's history of uploads and thus aims to reduce the number of unauthentic files in a P2P network. NICE (Lee *et al*., 2003) provides a platform to implement distributed cooperative applications. Based on trust chains, NICE computes a user reputation in a PGP-like model. By employing an asymmetric cryptographic algorithm, it requires peers to encrypt cookies to help others compute their reputations. In addition, Akleylek *et al*. (2005), Lua (2007) and Narasimha *et al*. (2003) adopt cryptography to attain security authentication. For example (Lua (2007) proposed a hybrid security protocol by unifying the ID-based cryptography and online secret sharing

Corresponding Author: Xingming Sun, School of Computer and Communication, Hunan University, Changsha, 410082, China Tel: 86-731-8821341 Fax: 86-731-88822417

schemes. His scheme can verify the peers' identities by easily obtaining the ID-based public signature verification key of every other peer from the peer identifier in the P2P overlay networks. Takeda *et al.* (2008) proposed a new authentication method called Hash-based Distributed Authentication Method (HDAM). The HDAM realizes a decentralized efficient mutual authentication mechanism for each pair of peers in the P2P network. It performs a distributed management of public keys by using Web of Trust and Distributed Hash Table. In Chen *et al.* (2008), each participating peer dynamically maintains a trusted group to perform distributed challenge-response authentication. It is based on Byzantine fault tolerance (Lamport, 1983).

ANONYMITY

Privacy has become an increasingly salient issue and considerable progress has been made with anonymous communications. Some articles adopt the idea of creating a hierarchical broadcast network to complete anonymous communication, such as P5 (Sherwood *et al*., 2002). Some methods adopt anonymous Mix router technique. For example, Tarzan (Freedman and Morris, 2002), MorphMix (Rennhard and Plattner, 2002) are based on Chaum's Mix method and their anonymity is better for Internet environments. In APFS (Scarlata *et al*., 2001), peers construct an anonymous path with tail peers using an onion technique, providing complete and mutual anonymity for peers. WonGoo (Lu *et al*., 2004) relies on layered encryption and random forwarding to achieve more stronger anonymity and high efficiency of communication. Some methods adopt middle agent peers to transfer message. Representative of literature is Crowds (Reiter and Rubin, 1998). Crowds hides his own in the group and enables the intermediate peers to randomly choose a successor to forward the request. Some studies are related to cryptography. Chang *et al.* (2007) proposed two protocols for hybrid P2P systems and pure P2P environments. These two protocols are based on primitive roots for three main reasons: simplicity, flexibility and efficiency. Some articles are committed to addressing some of the problems that exist in anonymous P2P system. MuON (Bansod *et al*., 2008) leverages epidemic-style data dissemination to deal with churn. While existing anonymity schemes will incur high latency, Shitrit *et al.* (2008) described a novel low-latency P2P anonymous scheme and is suitable for interactive services. GARM (Ji *et al*., 2007), REM-P2PAE (Dong *et al*., 2008) and (Hao *et al*., 2008) focus on reputation mechanism in anonymous environment. We propose SMA (Han *et al*., 2005a), SSMP (Han *et al*., 2005b) and PUZZLE (Han and Liu, 2008), which employ secret sharing scheme to allow peers to issue queries and responders to deliver requested files anonymously. Based on Random Walk, we also design an anonymous protocol called RWAP (Han *et al*., 2005c) in decentralized P2P systems. In addition, Rumor Riding (Han and Liu, 2006) utilizes a lower symmetric cryptographic algorithm to achieve anonymity. Compared with existing approaches, our proposals achieve mutual anonymity in P2P networks with a low cryptography processing and significantly reduce traffic cost and encryption overhead.

However, failure to support authentication also makes these approaches vulnerable to impersonation and man-in-middle attacks. We found this problem in our anonymity research.

SECURITY WORRIES

In addition, we must be concerned about anonymous abuse problem. That is, how to make anonymity controlled and traceable. Now anonymity abuse is severe. For example, some malicious peers use anonymity systems to send a large number of packets to a certain peer. This behavior will lead to network congestion so that the peer is single point of failure in P2P communication. Some peers send anonymously malicious messages in P2P reputation systems to slander other peers. In P2P resource share, some attacking peers can use anonymity systems to create and spread virus or polluted resource.

These three considerations lead to the conclusion that P2P systems must have some methods that can satisfy not only anonymity but also authentication and traceability. However, for one peer to authenticate and trace others, he needs to know the identity of the other peers, which affects anonymity. Thus, there exists an inherent contradiction between anonymity and trust or traceability in P2P systems.

AUTHENTICATION IN ANONYMITY

Although, this issue has not attracted extensive academic attention, there are still some articles related to this area. Next, we will introduce the relevant methods and discuss possible way to solve this problem.

We divide the area into two categories, System Control and Path Control. System Control means that systems modify, update and repair existing anonymous mechanism to attain anonymity and authentication. In System Control, main research focuses on system structure not anonymous path. On the other hand, some researches present some methods retaining anonymous

information in path to trace back. These researches main modify packet and mark some path information in it. Psychologically speaking, the former is proactive inhibition, the latter is retroactive inhibition.

System control: Most of articles about anonymity authentication mainly use secret handshakes, zero-knowledge proof, fair blind signature, group (ring) signature, K-TIMES anonymity, UCHVE (Liu *et al*., 2006) and so on to take effect.

For example, some anonymous secret handshakes (Huang and Cao, 2009; Su, 2009) are proposed so far, but they fail to completely solve the proposed problem. As handshakes are unlinkable, a client has no way to tell whether the one she is shaking hands with is the same as the one behind some earlier handshakes.

Some articles use zero knowledge authentication to tradeoff anonymity and authentication in P2P system (Lai-Cheng, 2008; Lu *et al*., 2008; Wierzbicki *et al*., 2005). To protect real identities, in these articles, each peer is required to generate a pseudonym. With the help of pseudonyms, some peers still can misuse anonymity. Pseudo Trust (Lu *et al*., 2008) and (Wei and He, 2009) use pseudonyms in the anonymous P2P network. Particularly, Our Pseudo Trust (Lu *et al*., 2008) proposes a scheme called Pseudo Trust (PT), where each peer, instead of using its real identity, generates an unforgeable and verifiable pseudonym using a one-way hash function. A novel authentication scheme based on Zero-Knowledge Proof is designed so peers can be authenticated without leaking any sensitive information. With the help of PT, most existing identity-based trust management schemes become applicable in mutual anonymous P2P systems. However Pseudo Trust is not perfect. If a malice peer uses PT to communicate with others, other peers can authenticate its pseudonym according with real identity by Zero-Knowledge Proof, but yet do not know his real identity. Wierzbicki *et al*. (2005) also used zero-knowledge proofs and Merkle's puzzles to describe a new protocol for authentication in Peer-to-Peer systems for controlled anonymity. But it does not solve the single fault problem.

The K-times anonymous authentication is proposed by (Nguyen and Safavi-Naini (2005) and Teranishi and Sako (2006). It includes group managers, users and victims and is based on Bilinear Pairings of mathematical curves. It ensures that group manager is able to track a user's true identity if only the number of evidence that victim provides is more than K value. Otherwise, even if victim colluding with group managers, he yet does not misuse trace power. Zhu *et al*. (2006) used this mechanism to track anonym who launches deliberate attack. K-times anonymous authentication solves the case of anonymity abuse more than K times perfectly, but not suitable for one less than K times.

Blind signature (Chaum, 1983) is a protocol for obtaining a signature from a signer where the signer's view of the protocol cannot be linked to the resulting message-signature pair. Blind signature scheme is often used in anonymous digital payment systems. Since the existing proposals of blind signature schemes provide perfect unlinkability, criminals can misuse such payment systems. So Stadler *et al*. (1995) has proposed a new type of blind signature schemes, called fair blind signature scheme. The scheme has the additional property that it is possible to link a message-signature pair with the corresponding protocol view of the signer. In FBST (Wang and Sun, 2009), we propose a security architecture to ensure anonymity and authentication for honest users and keep traceability for misbehaving users in P2P systems. We use Fair Blind Signature Trust (FBST) to resolve the conflict among anonymity, authentication and traceability. Signature that has information about identity ensures authentication. At the same time, blindness of signature and additional anonymous scheme provides anonymity. Moreover, traceability is achieved due to the fairness of fair blind signature. However, FBST only support PKI based scheme and this assumption in distributed P2P environment is actually very difficult to achieve. So in CST (Wang *et al*., 2010), we use Collaboration Signature Trust (CST) to resolve the conflicts among anonymity, authentication and traceability without PKI assumption. The tradeoff between anonymity and authentication is achieved due to the novel collaboration signature. Security analysis shows that the CST can perfectly resolve tradeoff between anonymity, authentication and traceability.

Group signature technique is also an instinctive idea to certify anonymity and authentication. The conception of group signature is introduced by Chaum and Heyst (1991). However, in most of group signature mechanisms, group manager can reveal arbitrarily the true identity of the group member, which will cause trace abuse. At the same time, this mechanism is difficult to deal with signature revocation problem of members. Ring signature (Ronald *et al*., 2001) is a signature approach similar to group signature, but without traceability like group signature. Lee *et al*. (2009) and Zhang *et al*. (2008) combined the respective advantages of group and ring signature to realize dynamic anonymity authentication mechanisms, respectively.

Another cryptography to be used to balance anonymity and authentication is the private credential framework proposed in PCS (Bangerter *et al*., 2006) and

the universal custodian-hiding verifiable encryption scheme (UCHVE) (Liu *et al*., 2006). Suriadi *et al.* (2008) used PCS to hide user's real identity and UCHVE to make PCS key transparent. Consequently the anonymous tracer must attain the key with the help of user to revoke anonymity and know the user's identity. This mechanism prevents the case of trace abuse but only for conventional networks not suitable for P2P environment.

In P2P environment, network traffic is huge. How to utilize existing cryptography technology to design lighter weight anonymous authentication is future work in this area.

Path control: At present, no article concentrates on anonymity authentication in P2P systems from the perspective of path control. But there are still many scholars have proposed some methods in general anonymous network. Introduction of these methods will help us to further consider how to authenticate and trace the dishonest in anonymous environment. As we said earlier, Path Control is a retroactive inhibition approach. Some studies have indicated that many intruders are deterred once they perceive risks involved. One of the intruders' greatest fears is losing their anonymity.Consequently,if in a certain condition we can track anonymous path and authenticate those machines in path, attack action would be reduced dramatically (Li *et al*., 2004) which indirectly achieves the target of restricting and authenticating anonym. The aim of trace is to track packet sources. In conventional IP networks, a lot of trace schemes are widely proposed. Common trace methods include Logging (Snoeren *et ai*., 2001), Link Testing (Burch and Cheswick, 2000), ICMP Trace, Centertrack, (Stone, 2000) Packet Marking (Song and Perrig, 2001; Park and Lee, 2001; Savage *et al*., 2000).

Among them, the most method maybe used in P2P system is Packet Marking, which is based on packet marking technology. The main idea of packet marking is to let routers mark packets with partial path information probabilistically (Song and Perrig, 2001; Park and Lee, 2001; Savage *et al*., 2000) or determinately (Belenky and Ansari, 2003). Because of huge number of nodes in P2P networks, it is impossible to mark every node. So Probabilistic Packet Marking seems more suitable for P2P environment. The principle of Probabilistic Packet Marking is that packets are probabilistically marked with partial path information as they are forwarded by routers. Having received enough information from path,the victim could reconstruct the full paths along which attack flows travel. Stronger evidence shows this technique can be applied to P2P environment is that there are some articles (Cheng *et al*., 2008; Jin *et al*., 2006; Ye *et al*., 2007) for WSN and ad-hoc network environments, which is similar to P2P systems. Ye *et al.* (2007) uses probabilistic packet marking method to locate anonymous attack on the node, but it assumes that any data can be written to the header data. That is to say, if node decides to mark a certain packet, it will mark the data added into the header. Therefore, the packet may be getting longer and longer and eventually had to be sliced to deal with, which is extremely difficult to be implemented. So it only has theoretical significance. On the other hand, (Gong and Sarac, 2005) points out, the basic packet marking method in a multi-attack path reconstruction bring on high false alarm rate and a high degree of computational complexity. Besides, due to limited space in the packet, conventional PPM always requires large flow of packets to collect the complete path information which will incur a large number of loads. These shortcomings have become obstacles in practical application. In P2P anonymous system, a certain cryptonym path is formed by a small number of anonymous packets.

How to mark path information in a small number of packets?

In future, one possible approach is to use the idea of Code Division Multiple Access (CDMA) technology to mark more information in sole packet by superposition mode. In this area, we have already done some preliminary investigation work. Besides, future researches should integrate all kinds of information theory and signal processing technology, such as watermarking, digital fingerprint to complete anonymous authentication in P2P system. As our mentioned (Li *et al*., 2008), there are a large number of redundant fields in P2P protocols. Those fields can be used to mark path information anonymously.

CONCLUSION

In this study, we analyze the tradeoff between anonymity and authentication in P2P network environment and introduce related researches. Besides, we propose some possible advices for this problem. From this article, we can be aware that harmonizing contradiction between anonymity and authentication in P2P system is not only a hot spot but also hard work.

ACKNOWLEDGMENTS

The research was supported by National Natural Science Foundation of China (60736016, 60873198, 60973128 and 60973113) and National Basic Research Program of China (2006CB303000, 2009CB326202, 2010CB334706), 973 pre-special project (2009CB326202, 2010CB334706) and China Postdoctoral Science Foundation funded project (20090461298).

REFERENCES

Akleylek, S., L. Emmungil and U. Nuriyev, 2005. A modified algorithm for peer-to-peer security. Proceedings of the System and Control Theory Workshop, (SCTW'05), Azerbaijan National Acad. Science, Gebze, Turkey, pp: 258-264.

Bangerter, E., J. Camenisch, A. Lysyanskaya, M. Blaze and B. Crispo *et al.*, 2006. A Cryptographic Framework for the Controlled Release of Certified Data. Springer Verlag, Cambridge, UK., pp: 20-50.

Bansod, N., A. Malgi, B.K. Choi and J. Mayo, 2008. MuON: Epidemic based mutual anonymity in unstructured P2P networks. Comput. Networks, 52: 915-934.

Belenky, A. and N. Ansari, 2003. IP traceback with deterministic packet marking. Commun. Lett. IEEE, 7: 162-164.

Burch, H. and B. Cheswick, 2000. Tracing anonymous packets to their approximate source. Proceedings of the 14th Systems Administration Conference (USENIX LISA 2000), Dec. 3-8, New Orleans, Louisiana, USA., pp: 319-327.

Chang, C.C., C.Y. Lin and K.C. Lin, 2007. Simple efficient mutual anonymity protocols for peer-to-peer network based on primitive roots. J. Network Comput. Appl., 30: 662-676.

Chaum, D. and E.V. Heyst, 1991. Group Signatures. In: Advances in Cryptology-EUROCRYPT '91, Davies, D.W. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-54620-7, pp: 257-265.

Chaum, D., 1983. Blind Signatures for Untraceable Payments, Advances in Cryptology-Crypto '82. Springer-Verlag, Santa Barbara, CA, USA., pp: 199-203.

Chen, R., W. Guo, L. Tang, J. Hu and Z. Chen, 2008. Scalable byzantine fault tolerant public key authentication for peer-to-peer networks. Proceedings of the 14th International Euro-Par Conference on Parallel Processing Las Palmas de Gran Canaria, Spain, Aug. 26-29, Springer-Verlag, Berlin, Heidelberg, pp: 601-610.

Cheng, B.C., H. Chen and G.T. Liao, 2008. FBT: An efficient traceback scheme in hierarchical wireless sensor network. Security Commun. Networks, 2: 133-144.

Dong, J., C. Tan and Y. Zhang, 2008. A Reputation Evaluation Method in P2P Anonymous Environment. Institute of Electrical and Electronics Engineers Computer Society, Zhangjiajie, Hunan, China, pp: 1516-1521.

Freedman, M.J. and R. Morris, 2002. Tarzan: A peer-to-peer anonymizing network layer. Proceedings of the 9th ACM Conference on Computer and Communications Security, Nov. 18-22, Association for Computing Machinery, Washington, DC, USA., pp: 193-206.

Gong, C. and K.I.P. Sarac, 2005. Traceback Based on Packet Marking and Logging. Institute of Electrical and Electronics Engineers Inc., Seoul, Korea, pp: 1043-1047.

Han, J. and Y. Liu, 2006. Rumor Riding: Anonymizing Unstructured Peer-to-Peer Systems. IEEE Computer Society, Santa Barbara, CA, United States, pp: 22-31.

Han, J. and Y. Liu, 2008. Mutual anonymity for mobile P2P systems. IEEE Trans. Parallel Distributed Syst., 19: 1009-1019.

Han, J., Y. Liu, L. Lu, L. Hu and A. Patil, 2005. A Random Walk Based Anonymous Peer-to-Peer Protocol Design. In: Networking and Mobile Computing, Lu, X. and W. Ahao (Eds.). LNCS., 3619, Springer-Verlag, Berlin, Heidelberg, ISBN-13: 978-3-540-28102-3, pp: 143-152.

Han, J., Y. Liu, L. Xiao, R. Xiao and L. M. Ni, 2005. A mutual anonymous peer-to-peer protocol design. Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, April 04-08, IEEE Computer Society, Denver, Colorado, USA., pp: 68-77.

Han, J., Z. Yanmin, L. Yunhao, C. Jianfeng and H.J. Lei, 2005. Provide privacy for mobile P2P systems. Proceedings of the 1st International Workshop on Mobility in Peer-to-Peer Systems. June 6-10, IEEE Computer Society, Ohio, USA., pp: 829-834.

Hao, L.M., S.T. Yang, S.N. Lu and G.L. Chen, 2008. Trusted computing-based reputation scheme with anonymity in P2P systems. Shanghai Jiaotong Daxue Xuebao/J. Shanghai Jiaotong Univ., 42: 165-168.

Huang, H. and Z. Cao, 2009. A novel and efficient unlinkable secret handshakes scheme. IEEE Commun. Lett., 13: 363-365.

Ji, W., S. Yang, D. Wei and W. Lu, 2007. GARM: A Group-Anonymity Reputation Model in Peer-to-Peer System. Institute of Electronic and Electronic Engineering Computer Society, Urumchi, Xinjiang, China, pp: 481-488.

Jin, X., Y. Zhang, Y. Pan and Y. Zhou, 2006. ZSBT: A novel algorithm for tracing DoS attackers in MANETs. Eurasip J. Wireless Commun. Network., 2006: 9-9.

Kamvar, S.D., M. T. Schlosser and H. Garcia-Molina, 2003. The eigentrust algorithm for reputation management in p2p networks. Proceedings of the 12th International Conference on World Wide Web, Budapest, Hungary, May 20-24, ACM, New York, USA., pp: 640-651.

Lai-Cheng, C., 2008. Heightening security of P2P networks by neighborhood key method. Proceedings of the 1st International Conference on Intelligent Networks and Intelligent Systems, Nov. 1-3, Institute of Electrical and Electronics Engineering Computer Society, Wuhan, China, pp: 201-204.

Lamport, L., 1983. Weak byzantine generals problem. J. ACM, 30: 668-676.

Lee, S., R. Sherwood and B. Bhattacharjee, 2003. Cooperative peer groups in NICE. Proceedings of IEEE INFOCOM, April, 2003, Institute of Electrical and Electronics Engineers Inc., San Francisco, CA, USA., pp: 1272-1282.

Lee, Y.K., S.W. Han, S.J. Lee, B.H. Chung and D.G. Lee, 2009. Anonymous Authentication System using Group Signature. IEEE Computer Society, Fukuoka, Japan, pp: 1235-1239.

Li, D.Q., P.R. Su and D.G. Feng, 2004. Notes on packet marking for IP traceback. Ruan Jian Xue Bao/J. Software, 15: 250-258.

Li, Z., X. Sun, B. Wang and X. Wang, 2008. A steganography scheme in P2P network. Proceedings of the 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Aug. 15-17, Harbin, China, pp: 20-24.

Liu, J.K., P.P. Tsang, D.S. Wong and R.W. Zhu, 2006. Universal Custodian-Hiding Verifiable Encryption for Discrete Logarithms. Springer Verlag, Seoul, Korea, pp: 389-409.

Lu, L., J. Han, Y. Liu, L. Hu, J.P. Huai, L. Ni and J. Ma, 2008. Pseudo trust: Zero-knowledge authentication in anonymous P2Ps. IEEE Trans. Parallel Distributed Syst., 19: 1325-1337.

Lu, T., B. Fang, Y. Sun and X. Cheng, 2004. WonGoo: A peer-to-peer protocol for anonymous communication. Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, June 21-24, CSREA Press, Las Vegas, NV, United States, pp: 1102-1106.

Lua, E.K., 2007. Securing peer-to-peer overlay networks from Sybil attack. Proceedings of International Symposium on Communication and Information Technology, Oct. 17-19, IEEE, Sydney, Australia, pp: 1213-1218.

Narasimha, M., G. Tsudik and J.H. Yi, 2003. On the utility of distributed cryptography in P2P and MANETs: The case of membership control. Proceedings of 11th IEEE International Conference on Network Protocols, Nov. 04-07, IEEE Computer Society Washington, DC, USA., pp: 336-345.

Nguyen, L. and R. Safavi-Naini, 2005. Dynamic K-Times Anonymous Authentication. Springer Verlag, New York, United States, pp: 318-333.

Park, K. and H. Lee, 2001. On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack. Institute of Electrical and Electronics Engineers Inc., Anchorage, AK, United States, pp: 338-347.

Reiter, M.K. and A.D. Rubin, 1998. Crowds: Anonymity for Web transaction. ACM TISSEC, 1: 66-92.

Rennhard, M. and B. Plattner, 2002. Introducing MorphMix: Peer-to-peer based anonymous internet usage with collusion detection. Proceedings of the ACM Conference on Computer and Communications Security, Nov. 21, Association for Computing Machinery, Washington, DC, USA., pp: 91-102.

Ronald, L. R., S. Adi and T. Yael, 2001. How to leak a secret. Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, (ICTACISAC'01), Springer-Verlag, pp: 552-565.

Savage, S., D. Wetherall, A. Karlin and T. Anderson, 2000. Practical network support for IP traceback. Comput. Commun. Rev., 30: 295-306.

Scarlata, V., B.N. Levine and C. Shields, 2001. Responder anonymity and anonymous peer-to-peer file sharing. Proceedings of the 9th International Conference on Network Protocols, Nov. 11-14, Riverside, CA, United states, Institute of Electrical and Electronics Engineers Computer Society, pp: 272-280.

Sherwood, R., B. Bhattacharjee and A. Srinivasan, 2002. P5: A protocol for scalable anonymous communication. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, (CSSRSP'02), Berkeley, CA, United States, Institute of Electrical and Electronics Engineers Inc., pp: 58-70.

Shitrit, S., E. Felstaine, N. Gilboa and O. Hermoni, 2008. Anonymity Scheme for Interactive P2P Services. Institute of Electronic and Electronic Engineering Computer Society, Lyon, France, pp: 33-40.

Snoeren, A.C., C. Partridge and L.A. Sanchez, 2001. Hash-based IP traceback. Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, Aug. 27-31, San Diego, California, USA., pp: 3-14.

Song, D.X.D. and A. Perrig, 2001. Advanced and authenticated marking schemes for IP traceback. Proceedings of the 20th Annual Joint Conference on IEEE Computer and Communications Societies, April 22-26, Anchorage, Alaska, USA., pp: 878-886.

Stadler, M., J.M. Piveteau and J. Camenisch, 1995. Fair blind signatures. Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, 1995, Saint-Malo, France, Springer-Verlag GmbH and Company KG, pp: 209-219.

Stone, R., 2000. Centertrack: An IP overlay network for tracking DoS floods. Proceedings of the 9th USENIX Security Symposium, Aug. 14-17, Denver, Colorado, USA., pp: 107-118.

Su, R., 2009. On the security of a novel and efficient unlinkable secret handshakes scheme. IEEE Commun. Lett., 13: 712-713.

Suriadi, S., E. Foo and J. Smith, 2008. A User-Centric Protocol for Conditional Anonymity Revocation. Springer Verlag, Turin, Italy, pp: 185-194.

Syverson, P.F., 1998. Anonymous connections and onion routing. IEEE J. Selected Areas Commun., 16: 482-494.

Takeda, A., D. Chakraborty, G. Kitagata, K. Hashimoto and N. Shiratori, 2008. A new scalable distributed authentication for P2P network and its performance evaluation. WSEAS Trans. Comput., 7: 1628-1637.

Teranishi, I. and K. Sako, 2006. K-Times Anonymous Authentication with a Constant Proving Cost. United States, Springer Verlag, New York, pp: 525-542.

Wang, X. and X. Sun, 2009. Fair blind signature based authentication for super peer P2P network. Inform. Technol. J., 8: 887-894.

Wang, X., X. Sun, G. Sun and L. Dond, 2010. CST: P2P anonymous authentication system based on collaboration signature. Proceedings of the 5th International Conference on Future Information Technology, May 21-23, IEEE Computer Society, Busan, Korea, pp: 1-7.

Wei, Y. and Y. He, 2009. A Pseudonym Changing-Based Anonymity Protocol for P2P Reputation Systems. Institute of Electrical and Electronics Engineers Computer Society, Wuhan, Hubei, China, pp: 975-980.

Wierzbicki, A., A. Zwierko and Z. Kotulski, 2005. Authentication with Controlled Anonymity in P2P Systems. In: Parallel and Distributed Computing, Applications and Technologies. Dalian, China, 2005. Institute of Electrical and Electronics Engineers Computer Society, Washington, DC, USA., ISBN:0-7695-2405-2, pp: 871-875.

Wu, H., C. Shi, H. Chen and C. Gao, 2008. A Trust Management Model for P2P File Sharing Systems. Institute of Electronic and Electronic Engineering Computer Society, Busan, Korea, pp: 41-44.

Ye, F., H. Yang and Z. Liu, 2007. Catching Moles in Sensor Networks. Institute of Electrical and Electronics Engineers Inc., Toronto, ON, Canada.

Zhang, M.W., B. Yang, S.L. Zhu and W.Z. Zhang, 2008. Efficient secret authenticatable anonymous signcryption scheme with identity privacy. Proceedings of the Pacific Asian Workshop on Intelligence and Security Informatics, June 17, Taipei, Taiwan, Springer-Verlag, Berlin, pp: 126-137.

Zhu, B., S. Setia and S. Jajodia, 2006. Providing Witness Anonymity in Peer-to-Peer Systems. Association for Computing Machinery, Alexandria, VA, United States, pp: 6-16.