DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5534

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

TECHNICAL NOTE

Available Online at www.ijarcs.info

SECURE KEY ISSUING SCHEME IN BIT-TORRENT NETWORK

Ratnadeep Nath
Department of Computer Science and Engineering
Dibrugarh University
Dibrugarh-786004, India

Aminullah Laskar
Department of Computer Science and Engineering
Dibrugarh University
Dibrugarh-786004, India

Bishal Saha
Department of Computer Science and Engineering
Dibrugarh University
Dibrugarh-786004, India

Sudipta Majumder
Department of Computer Science and Engineering
Dibrugarh University
Dibrugarh-786004, India

Abstract: Bittorrent Protocol was introduced as a means of transferring large files efficiently. But, with progressing time, security issues are consuming the Bittorrent traffic like parasites. In this paper, we propose a secured key issuing scheme for Bittorrent to remove these security threats. We will combine both Identity Based Cryptography (IBC) and SKIP to generate secured keys for the peer in order to isolate the malicious ones and hence, secure the network.

Keywords: Peer-to-Peer, Bittorrent Protocol, Secured Key Issuing, Identity Based Cryptography, KGC, KPAs. Shamir's Secret Sharing Scheme

I. INTRODUCTION

In a world where internet is at the peak of almost everything, transfer of information has always been one of the top priority of the netizens. Of all the existing network models, the peer-to-peer network became the closest one to the ideal World Wide Web. Bit-torrent, which is the most popular peer-to-peer based network, has now emerged as the primary means of transfer of large files due to its consumption of less bandwidth. It is one of the leading protocols with approximately 35% of internet traffic credited to it alone. But with growing popularity, its security threat issue has also become a question of the century. It is vulnerable to cyber attacks due to the insufficient number of certification and authentication services which is responsible for peer's identity verification and corroboration purpose respectively [1]. To illustrate it more, consider a network with three peers. To secure the network, a security key is issued and is circulated among all the peers. But, what will happen if one of them is a notorious peer and wants to disrupt the network? As he knows the security key, he can infuse any malware with the file to be transferred. Through this paper, we will show how to bypass this type of flagrant peer and transfer files securely in a Bittorrent Network.

II. BACKGROUND

To set the scene for the paper, we begin with a brief overview of the Bittorrent Protocol with its concerning security issues. Suppose, there are some peers in a Bittorrent Network, and they want to transfer a large file like a movie or a game. So, they will have to start sending their respective chunk of the file. But, before doing that, they thought of securing the network and hence, provided a security key like a password, to each other. Afterwards, they start sending the file. But, there lies the biggest blunder of all. What if one of the peer is a malicious entity which is pretending to be a good seeder. It will contaminate the whole network with malwares and ransom-wares; and eventually agitate the whole swarm.

III. PROPOSAL

In this paper, we propose an IBC established Secure Key Partitioning technique for the Bittorrent Network to transfer large files. We expect the technique to be more reliable, efficient and secure among peers of the network. It comprises a setup of IBC infrastructure where a peer authentication protocol is introduced. The protocol can register peers by implementing Shamir's Secret Sharing technique. The technique also includes a secure key distribution protocol which circulates private keys securely. Lastly, by implementing BFT protocol to Key Privacy Authorities (KPAs), the malicious KPAs are removed and are replaced with new KPAs.

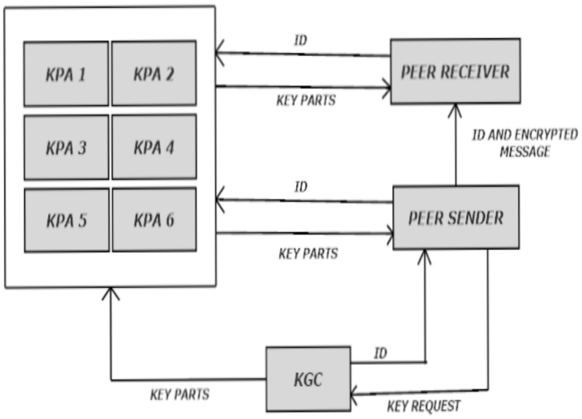

Figure 1. Architecture of the network system

Shamir's Secret Sharing Scheme: In the aforementioned example, the Secure Key falling into the hands of malicious peers, remained the unsolved problem. To protect the secure key, Shamir's Secret Sharing Scheme is applied where the key is divided into various parts, giving each peer its own unique part. So, even if some of the secret key have been contaminated, the master key can be recovered by combining at least the threshold number of secret keys.

IV. RELATED WORK

IBC uses the user's identity as the public key. The private keys of the users are issued by a Key Generate Center (KGC) once confirming the user's credentials. IBC was introduced in 1984 by Shamir [2]; but, the first practical encryption scheme (IBE) was not available till 2001 which was developed by Boneh and Franklin [3]. Although IBC overcomes the issues of the traditional PKI, it suffers from some inherent issues, one of which is the secure channel requirement: key issuing needs the secure channel to avoid eavesdropping. In 2001, Boneh and Franklin [3] addressed secure key issuing problem using multiple key authorities. After that, several key issuing protocols [4], [5], [6] without secure channels were proposed.

So far, many studies are centered on introducing IBC into P2P security applications. Lu et al. in [7] combined distributed hash tables (DHTs [8]) and identity-based encryption (IBE) to defend against man-in-the-middle attacks, however, the scheme assumed that each noble had a pre-assigned distinctive identifier, and has obtained the corresponding nonpublic key through a secure offline channel. This is often costly and troublesome to attain on a large scale P2P overlay network. In [9], Lua projected a hybrid security protocol based on IBC to resist the Sybil attacks, Ryu et al. in [10] proposed ID assignment protocols based on IBC to allow to acquisition of node IDs to be tightly regulated so as to mitigate the Sybil attacks, however these two schemes still suffered from the attack against key issuing phase. Likir [11] conferred by Aiello et al. signs messages with IBS in Kademlia-based P2P networks, however, the authors supposed every system user had already obtained a private key and did not think about the key issuing problem.

V. CONCLUSION

With emerging networks, there is a dire need of robust and stable security. In this paper, we have proposed a secured key issuing partition for the Bittorrent network to transfer files. We combined the concepts of Identity Based Cryptography (IBC) using Shamir's Secret Sharing Scheme and Secure Key Issuing Scheme using KGC, KPAs to issue private keys for peers in the network.

VI. REFERENCES

[1] Anantha D. N., Bhimashankar, Girisha A. V., Mahalakshmi M. C., Asha G. R., Key Issuing Scheme for Communication in Peer to Peer Networks in International Journal for Research in Applied Science & Engineering Technology (IJRASET). April 2015.

[2] A. Shamir, Identity-based cryptosystems and signature schemes in CRYPTO, 1984.

[3] D. Boneh and M. K. Franklin, Identity-based encryption from the weil pairing in CRYPTO, 2001.

[4] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, Secure key issuing in id-based cryptography in ACSW Frontiers, 2004.

[5] R. Gangishetti, M. C. Gorantla, M. L. Das, A. Saxena, and V. P. Gulati, An efficient secure key issuing protocol in id-based cryptosystems in ITCC (1), 2005.

[6] A. Saxena, Threshold ski protocol for id-based cryptosystems in IAS, 2007.

[7] Z.-L. Lu, G.-H.; Zhang, Wheel of trust: A secure framework for overlay-based services ICC.

[8] I. Stoica, R. Morris, D. R. Karger, M. F. Kaashoek, and H. Balakrishnan, Chord: A scalable peer-to-peer lookup service for internet applications in SIGCOMM, 2001.

[9] E. K. Lua, Securing peer-to-peer overlay networks from sybil attack in ISCIT'07, Sydney, Australia, 2007.

[10] S. Ryu, K. R. B. Butler, P. Traynor, and P. D. McDaniel, Leveraging identity-based cryptography for node id assignment in structured p2p systems in AINA Workshops (1), 2007.

[11] L. M. Aiello, M. Milanesio, G. Ruffo, and R. Schifanella, Tempering kademlia with a robust identity based system in Peer-to-Peer Computing, 2008.