Computers and Electrical Engineering 000 (2017) 1–17

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Enhancing Rumor Riding protocol in P2P network with Cryptographic puzzle through challenge question method☆

Mary Subaja Christo[a,*], S. Meenakshi[b]

[a] Research Scholar, Sathyabama University, India
[b] HOD Department of IT, Jeppiaar SRR Engineering College, India

ARTICLE INFO

Article history:
Received 16 October 2016
Revised 14 February 2017
Accepted 15 February 2017
Available online xxx

Keywords:
Peer-to-Peer
Security
Challenge question
Reliable rumor riding protocol
Cryptographic puzzle
Malicious node

ABSTRACT

This research seeks is to investigate the Peer to Peer network topology and its custom behavior. The habitual effect of Peer to Peer network includes considering all the connected nodes as peers and these peers head-on with other peers to effectuate the tasks assigned to each one of them. The entire embrace of this network topology clings on to the heterogeneous sphere. Due to its comprehensive network topology and penchant features, the network is vulnerable to many castigating attacks. Furthermore, the possession attributed to the security traits of the network is comparatively tiny. Thus, this network topology is subjected to copious attacks. Rumor Riding (RR) is an anonymous and non-path based protocol. In this protocol, three nodes (including the Initiator, Intermediate, and Responder) are involved in sharing the information or searching the file. In some cases, the named three nodes may act as attackers leading to initiator attacks, intermediate attacks and responder attacks. The reason behind the argument is that RR protocol is based on an anonymous method that tends to hide the information from source to destination without authentication. Hence, the network performance gradually becomes ineffective. The main intent of this paper is to explore the ways and means to prevent all the stated onslaughts. To achieve this, we have developed an attack prevention protocol. The protocol involves the Reliable Rumor Riding Protocol in P2P Network through the Cryptographic Puzzle attributed to the Challenge Question Method. Furthermore, we have augmented the performance and measured. Hence, in this quintessential way, the network operation is proved to be secured and authenticated.

1. Introduction

In the discipline of Peer-to-Peer (P2P) network, P2P computing refers to the distribution of resources among computers. Some of the resources that are shared include knowledge, processing power, information emanating from distributed databases and disk storage. It should be noted that within a P2P system, it is probable for computers to act as both the servers and clients. As such, their duties in specific undertaking are defined based on the system requirements at a particular period. For instance, a file transfer request that is sent from computer A to computer B. In the process of sending the file, computer B turns out to act as the server while computer A becomes the Client. Such role will be reversed when

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. R. Varatharajan.

* Corresponding author.
E-mail address: marysubaja@gmail.com (M.S. Christo).

http://dx.doi.org/10.1016/j.compeleceng.2017.02.008
0045-7906/

the request end changes. This method minimizes the work of the servers while enhancing the general performance of the network.

The file sharing application is very popular as it is currently being used in P2P systems. Predominantly, file sharing refers to the distribution of resources using P2P technology which is utilized in the networking process. The P2P file sharing enables users to identify media files like music, books, games and movies via its software program. The role of the software program is to hunt for other computers that are connected through P2P network in an attempt to locate the required content. The peers or nodes of such networks are end-user computer systems that are unified through the Internet. In the recent past, P2P file sharing technology has advanced through various design phases away from the primary networks. For instance, Napster, which has proliferated the technology and other recent models that include the Bit Torrent protocol. Numerous factors led to the broad acceptance and facilitation of P2P file sharing [1]. These factors include the increasing internet bandwidth, the extensive physical media digitization, and the growing proficiencies of residential individual computers. Hence, users could easily transfer at least one file among computers through the internet. The sharing of files occurs through certain file-sharing networks and various file transfer systems. Specific PC owners or participants have to trust the search entity before downloading the specific programs absolutely. Accordingly, when P2P programs are sanctioned to run on one's computer, it significantly increases susceptibility to security breaches [2]. Examples of such breaches include a) erasing directories or files located on the computer; b) writing on or reading from the files on your computer, and c) producing new directories or files on your computer. It is worth noting that it is quite problematic to secure P2P applications against the above breaches.

An anonymous P2P protocol is generally referred to as a Rumor Riding (RR), and it is non-path based. As such, the initiator directs cipher texts and key messages to multiple neighbors. The ciphertexts and key messages assume random walks disjointedly within the system. Each walk is termed as a rumor. It is through the random walk that the rumor established the anonymous path. Neither the responder nor the initiator needs to be troubled by the path maintainers and structure. RR protocol only pays attention to the anonymous downloading and searching in P2P systems [3,4]. Due to the anonymity, the doors are opened to probable abuses and misuses, that results in the exploitation of the P2P network. The network is abused by spreading destructive resources such as; viruses, Trojan Horses, and spams. In RR, the initiator acts as a malicious node which may direct false request texts to the responder. If the responder is malevolent also, the man in middle attack may happen and might utilize different IP address. To mitigate this challenge, it is proposed to use an initiator, to be authenticated by a responder, and the responder authenticated by the initiator. In this way, the authentication becomes necessary and helpful in P2P networks.

To ensure data security during its broadcast from the source node to the endpoint, the authentication system offers verification of the identity or other attributes to a network usage. In this study, we have used Challenge Question based on the Puzzle hacking method. Thus, the Cryptographic Puzzles are used to authenticate the Intermediate nodes in a P2P network. When the node acts as an Intermediate node, they answer the Challenge Question or Puzzle which becomes necessary for it. An Intermediate node can decrypt the message only if the answer is correct. When the answer is right, the node forwards it to the other nodes in the network to find the Responder node. Otherwise, the intermediate node may fail to decrypt the initial message. Likewise, it authenticates the intermediate node.

The other sections of this paper are organized as follows;

Section 2 introduces the related work. Section 3 deliberates on Reliable Rumor Riding Protocol that ensures security during the data transmission from source to destination. Section 4 discusses the many metrics used to assess the performance of the suggested algorithm. Further, the segment provides the simulation outcomes. Section 5 encompasses a conclusion this work.

2. Related works

2.1. Anonymous search in P2P network

Xiaoliang et al. explained the importance of authentication in P2P networks [5]. These authors stated that anonymity searching allows attackers into P2P networks. To eliminate these attackers, the network requires trust and reliable authentication. Stefan Kraxberger et al. proposed trust transaction for the online service provision [6,7]. The provision stipulates that before making a purchase decision, the buyer should check the trust value of the product from third parties, based on the feed back of their trust value. Alternatively, the buyer can purchase the item with the help of a reputation system. Jia Zhang proposed the establishment of trust based P2P network [8]. Accordingly, Jia highlighted that P2P anonymous communication needs the trust method. This is because the anonymous tunneling may not provide higher anonymity, but may provide lower performance. Takeda et al. proposed HDAM authentication method [9]. Currently, P2P network suffers more from authentication, and it is for this reason that she has used HDAM method to increase reliability in P2P networks. Cheng et al. elucidated that, in the P2P framework, the service provider should authenticate the requested node based on the communication history. Cheng et al. also noted that the service provider should evaluate the trust value and finally establish if the node is trustworthy or not [10].

Gupta et al. developed a Reputation Aggregation method based on different gossip algorithms [11]. This technique is used to authenticate every node in the P2P network. The authentication is done with the help of reputation value obtained from every node. Lu et al. explained that a Zero Knowledge-based authentication in P2P system identifies the fake trust (FT) [12].

Please cite this article as: M.S. Christo, S. Meenakshi, Enhancing Rumor Riding protocol in P2P network with Cryptographic puzzle through challenge question method, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.02.008