Optik - International Journal for Light and Electron Optics 273 (2023) 170345

Contents lists available at ScienceDirect

Optik

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

A resilient group session key authentication methodology for secured peer to peer networks using zero knowledge protocol

P.Lalitha Surya Kumari [a,*], C.H.Sarada devi [b], S. Thivaharan [c], K. Srinivas [d], Avula Damodaram [e]

[a] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad 500075, India
[b] Department of C.S.E., Meenakshi College of Engineering, Chennai 600078, India
[c] Department of C.S.E., P.S.G. Institute of Technology and Applied Research, Coimbatore 641062, India
[d] Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology, Cheeryal, Village, Keesara Mandal, Medchal District, Telangana, India
[e] Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Kukatpally, Hyderabad, Telangana 500085, India

ARTICLE INFO

Keywords:
Zero knowledge protocol
Authentication
Confidentiality
Lagrange Interpolation
Pseudo trust
Peer to Peer network
NS-2

ABSTRACT

This novel methodology develops a Pseudo Trust in Peer-to-Peer networks using Lagrange Interpolation and Zero-Knowledge Protocol and creates a non-forgeable pseudonym. Authentication of a peer can be done without disclosing any sensitive information by using Zero-Knowledge Protocol. Each node in a peer maintains a unique I.D. It is not necessary to reveal the credential information at the time of verification. The implementation of distributed trust model is done incrementally in P2P networks. This proposed methodology generates different polynomials at the source and destination, respectively. After creating polynomials, authentication is performed using a challenge-based system (Zero-Knowledge Protocol) by exchanging pseudo-random numbers. Source and destination generate the same polynomial without exchanging any secret information. This polynomial can be used for encryption and decryption. The proposed algorithm is analysed by considering three parameters of network Throughput, the number of packets dropped and the number of packets delivered. These results measure the performance of the proposed algorithm applied in Peer-to-Peer networks over public networks.

1. Introduction

1.1. Peer to Peer networks

Every computer in P2P networks is recognised through a unique name. Peer to Peer network (P2P) is huge, openly available and will increase in magnitude for the specified technology [1]. Peer-to-peer (P2P) constructions are usually considered “file-swapping” networks to distribute resources among their nodes [2].

In general, all the nodes in the P2P community structure distribute resources like files, printers, and community access. P2P networks are decentralised networks. Given this, the primary server, the main server, or a controller isn’t always required. A peer-to-

* Corresponding author.
E-mail addresses: vlalithanagesh@gmail.com (P.LalithaS. Kumari), saradhadevi6@gmail.com (C.H.Sarada devi), thivahar@psgitech.ac.in (S. Thivaharan), katkamsrinu@gmail.com (K. Srinivas), damodarama@gmail.com (A. Damodaram).

https://doi.org/10.1016/j.ijleo.2022.170345
Received 22 September 2022; Received in revised form 19 November 2022; Accepted 2 December 2022
Available online 6 December 2022