Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 3, March 2013, pg.67 – 73

RESEARCH ARTICLE

Mesh Technique for Nymble Architecture Sustaining - Secrecy and Security in Anonymizing Networks

J.praveen kumar[1], B.shyam kumar[2]

[1]Assistant Professor, Department of Information Technology, Teegala Krishna Reddy Engineering College Hyderabad, Andhra Pradesh, India

[2]Assistant Professor, Department of Information Technology, Teegala Krishna Reddy Engineering College Hyderabad, Andhra Pradesh, India

[1]Praveenkmr914@gmail.com, [2]shyamtkrec@gmail.com

Abstract— Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited by users employing this secrecy for abusive purposes such as defacing popular websites. Website administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying secrecy access to misbehaving and behaving users alike. To address this problem, present Nymble, a system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. Our system is thus agnostic to different servers' definitions of misbehavior servers can blacklist user's .by using of Mesh technique. Which has been completely blocked by several services because of users who abuse their secrecy and providing security with MD5 algorithm?

Key Terms: - secrecy, anonymous, privacy, pseudonym. Blacklisting.

Full Text: http://www.ijcsmc.com/docs/papers/March2013/V2I3201312.pdf