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.

I. INTRODUCTION

Wireless mesh networking has recently become a possible solution for networking environment where it is hard to prepare for networking infrastructure. However, it is well known that packet loss increases exponentially as the size of the network grows, and thus, it is often not robust enough in practice. In WMN secrecy and privacy issues have gained considerable research efforts in the literature which have focused on investigating secrecy in different context or application scenarios. One requirement for secrecy is to unlink a user's identity to specific activities, such as the secrecy fulfilled in the untraceable banking systems and the P2P payment systems, where the payments cannot be linked to the identity of a payer by the bank or broker. ANONYMIZING networks such as Tor route traffic through independent nodes in separate administrative domains to hide a client's IP address. Secrecy is also required to hide the location information of a user to prevent movement tracing, as is important in mobile networks and VANETs. In wireless communication systems, it is easier for a global observer to mount traffic analysis attacks by following the packet forwarding path than in wired networks. Thus, routing secrecy is essential, which conceals the confidential communication relationship of two parties by building a secrecy path between them. Nevertheless, unconditional secrecy may incur insider attacks since misbehaving users are no longer traceable. Therefore, traceability is highly desirable such as in banking systems, where it is used for detecting and tracing double spenders.

II. NYMBLE SYNOPSIS

In this paper we propose a secure Nymble system, where users acquire an ordered collection of nimblest, a special type of pseudonym, to connect to Websites. Without additional information, these nymbles are computationally hard to link and hence, using the stream of nymbles simulates secrecy access to services. Web sites, however, can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user. Servers can therefore blacklist secrecy users without knowledge of their IP addresses while allowing behaving users to connect secretly. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted. Although our work applies to anonymizing networks in general, we consider Tor for purposes of exposition. In fact, any number of anonymizing networks can rely on the same Nymble system, blacklisting secrecy users regardless of their anonymizing network(s) of choice. The purpose of the Nymble project is to allow for responsible, secrecy access online. It provides a mechanism for server administrators to block misbehaving users while allowing for honest users to stay secrecy; in fact even the blocked users remain secrecy. The name "Nymble" comes from a play on the word "pseudonym" and "nimble". Instead of giving users a simple pseudonym, the Nymble system assigns users "nymbles"; that is, a pseudonym with better secrecy properties.

A. Nymble properties

1. Secrecy blacklisting: A server can block the IP address of a misbehaving user without knowing the identity of the user or his/her IP address.

2. Privacy: Honest and misbehaving users both remain secrecy.

3. Backward secrecy: The blacklisted user's previous activity remains secrecy /unlikable, and is refused future connections.

4. Blacklist-status awareness: A user can check whether he/she has been blocked before accessing services at the server.

5. Subjective judging: Since misbehaving users are blocked without compromising their privacy, servers can provide their own definition of "misbehavior".

Type	Initiator	Responder	Link
Basic	–	Authenticated	Confidential
Auth	Authenticated	Authenticated	Confidential
Anon	Anonymous	Authenticated	Confidential

Fig 1. Different types of controls exploited in Nymble

B. Anonymizing networks - tor

Tor is an anonymizing network that hides a client's identity (actually, your computer's IP address) from the servers that it accesses. Tor keeps a client's IP-address secrecy by bouncing its data packets through a random path of relays. Each relay knows only of the relay that sent it data and the next relay in the random path. As long as the entry and exit nodes do not collude, the client's connections remain secrecy. Tor provides anonymity, but some people abuse this anonymity. Since website administrators depend on blocking the IP addresses of misbehaving users, they are unable to block misbehaving users who connect through Tor; their IP address is hidden after all. Frustrated by repeated offenses through the Tor network, the usual response for websites such as Slashdot and Wikipedia is to block the entire Tor network. This is hardly an optimal solution, as honest users are denied secrecy access to these websites through Tor.

C. Blacklisting secrecy users

By providing a mechanism for server administrators to block secrecy misbehaving users, we hope to make the use of anonymizing networks such as Tor more acceptable for server administrators everywhere. All users remain secrecy — misbehaving users can be blocked without deanonymization

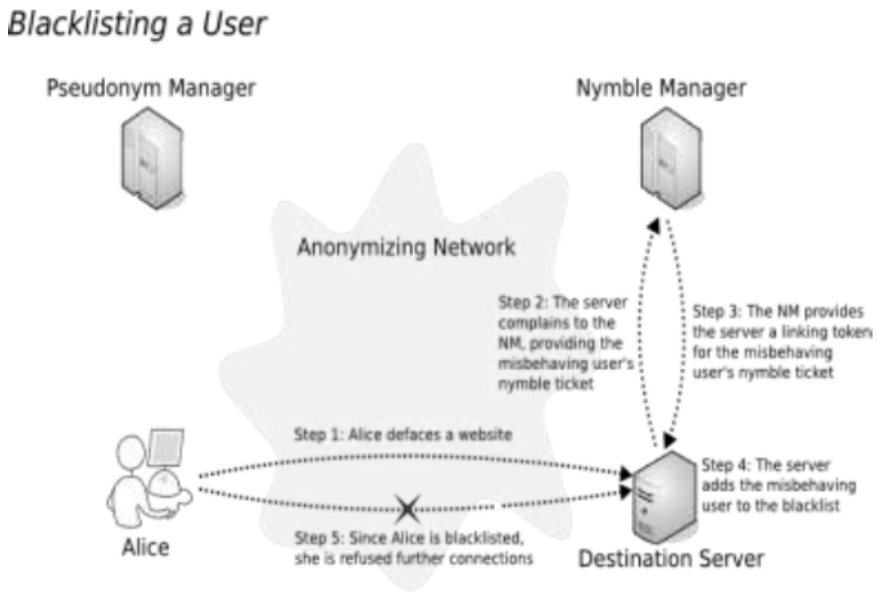


Fig: 2 Black Listing Users

.

III. MODULES OF PROPOSED SYSTEM

A. Pseudonym manager

The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM directly (i.e., not through a known anonym zing network), ensuring that the same pseudonym is always issued for the same resource.

B. Nymble Manager

Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted. Although our work applies to anonym zing networks in general, we consider Tor for purposes of exposition. In fact, any number of anonym zing networks can rely on the same Nymble system, blacklisting anonymous users regardless of their anonym zing network(s) of choice.

C. Nymble-authenticated connection

Blacklist ability assures that any honest server can indeed block misbehaving users. Specifically, if an honest server complains about a user that misbehaved in the current likability window, the complaint will be successful and the user will not be able to "nymble-connect," i.e., establish a Nymble-authenticated connection, to the server successfully in subsequent time periods (following the time of complaint) of that likability window.

Rate-limiting assures any honest server that no user can successfully nymble-connect to it more than once within any single time period. Non-frame ability guarantees that any honest user who is legitimate according to an honest server cans nymble-connect to that server. This prevents an attacker from framing a legitimate honest user, e.g., by getting the user blacklisted for someone else's misbehavior. This property assumes each user has a single unique identity.

When IP addresses are used as the identity, it is possible for a user to "frame" an honest user who later obtains the same IP address. Non-frame ability holds true only against attackers with different identities (IP addresses). A user is legitimate according to a server if she has not been blacklisted by the server, and has not exceeded the rate limit of establishing Nymble-connections. Honest servers must be able to differentiate between legitimate and illegitimate users.

Anonymity protects the anonymity of honest users, regardless of their legitimacy according to the (possibly corrupt) server; the server cannot learn any more information beyond whether the user behind (an attempt to make) a nymble-connection is legitimate or illegitimate.

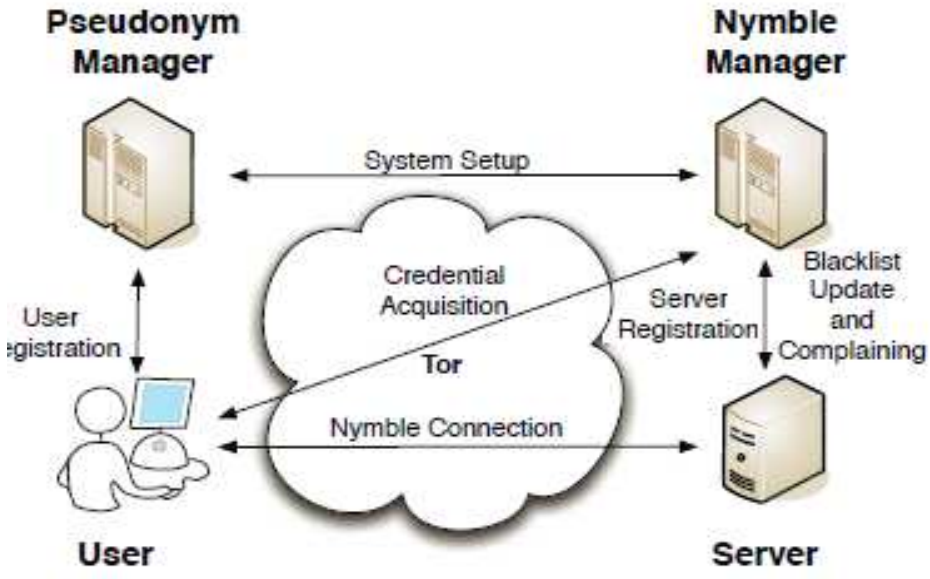
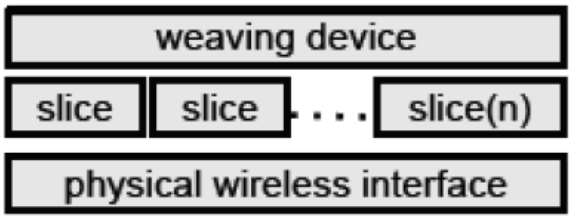


Fig: 3 Connection Authentications

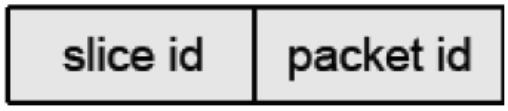
.

IV. DESIGN OF MESH SLICE

A slice device –It is identified by a slice id, is a logical unit for packet transmission.
A weave device – It is a controller-like device that controls the whole process of mesh Slice



4(a).mesh slice devise



4(b). Mesh slice label

Slice id - (used for physical interface multiplexing)
Packet id (used for eliminating duplicate packets)

A. Container Flow in Mesh Slice

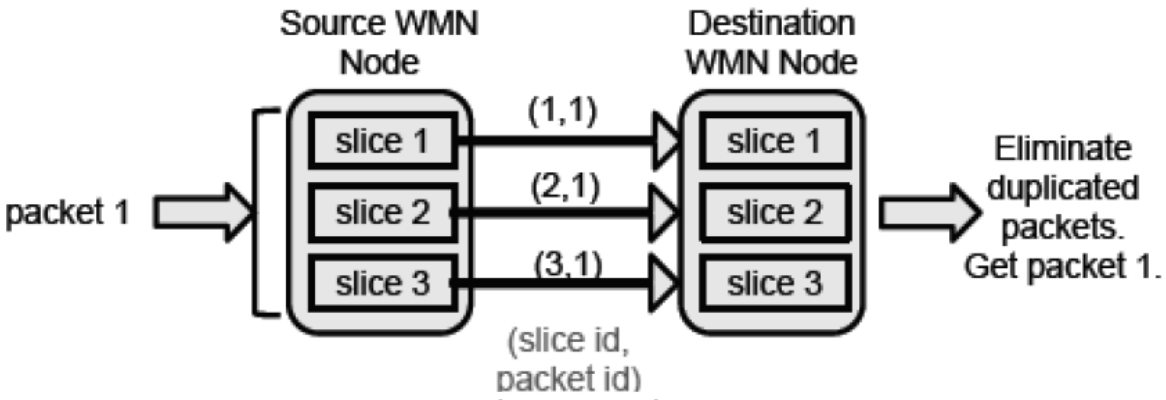


Fig 5: Packet Container Flow

At sender side

1. Weave device adds header to the packet, then assigns packet id, and duplicates it onto each of the slicing devices.
2. Each slicing device assigns its own slice id to the packet and sends it out.

At receiver side

1. The physical wireless device first demultiplexes it to the corresponding slicing device by examining slice ID, and finally to the weaving device.
2. For each flow of packets, the weaving device maintains a data structure.
3. By checking this data structure, weaving device eliminates duplicate packets.

V. SAFETY MEASURES

Md5 algorithm

MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. According to RFC 1321, MD5 message-digest algorithm takes a message of arbitrary length as input and produces output as a 128-bit fingerprint or message digest of the input. The MD5 algorithm is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted with a private key under a public-key cryptosystem such as RSA. Fig 6 shows the MD5 algorithm structure. MD5 is simple to implement. It provides a fingerprint or message digest of a message of arbitrary length. It performs very fast on 32-bit machine.

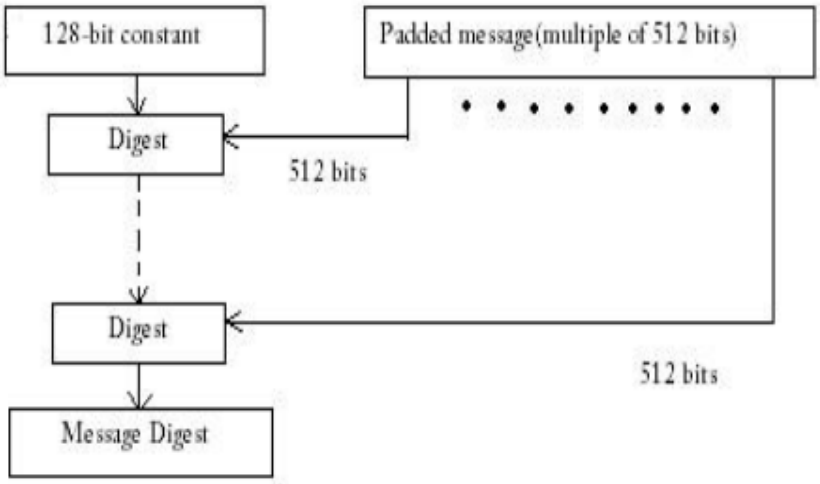


Fig 6: MD 5 Algorithm Structure

Performance steps in md5

Step 1: Append padding bits.
Step 2: Append length.
Step 3: Initialize MD buffer.
Step 4: Process the message in 16 word blocks.
Step 5: Output (message digest).

The advantages of MD5 algorithm are the generation of a digest is very fast and the digest itself is very small and can easily be encrypted and transmitted over the internet. It is very easy and fast to check some data for validity. The algorithms are well known and implemented in most major programming languages, so they can be used in almost all environments.

Performance evaluation

The Dijkstra's Algorithm is implemented and the results are simulated. The Algorithm proves to find the shortest path from source to destination to transmit the packets. The start time is noted when the algorithm starts to execute. The end time is also noted when the packets reach the destination. The time difference is calculated based on the start time and end time. The graph is plotted with time against algorithm types. Thus the comparison is made with the key based routing and the Dijkstra's algorithm and is shown in the fig.2

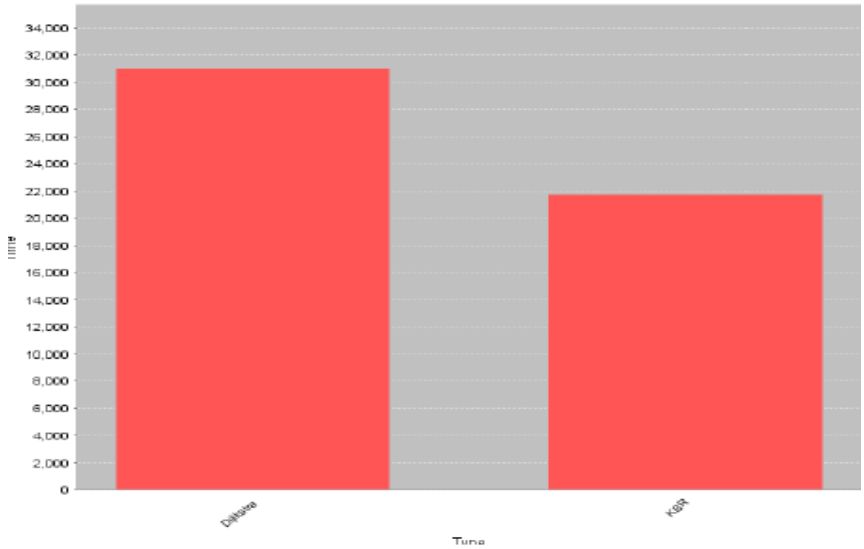


Fig.7 Comparison of time difference between Dijkstra's Algorithm and KBR Algorithm

VI. CONCLUSION

The major issues in anonymizing networks are misbehaving user access and blacklisting the misbehaving users without knowing their IP addresses. The paper proposes a more secure system which can be used to add a layer of accountability to any known anonymizing network. This system allows websites to selectively block users of anonymizing networks such as Tor. Servers can blacklist misbehaving users while maintaining their privacy and these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services. This work will increase the mainstream acceptance of anonymizing networks such as Tor, which has been completely blocked by several services because of users who abuse their anonymity. For the proposed Nymble -based anonymity system, effective anonymous routing protocols were to be used to construct anonymous communication paths and guarantee unlinks ability. Unlink ability is a requirement for preserving user privacy in addition to anonymity.

REFERENCES

[1] Camenisch.J and Lysyanskaya.A, *"Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials,"* Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, 2002..

[2] J. Kong and X. Hong, *"ANODR: Anonymous on demand routing with untraceable routes for mobile adhoc networks,"* in Proc. ofMobiHoc, 2003.

[3]Dingledine.R, Mathewson.N, and Syverson.P, *"Tor: The Second- Generation Onion Router,"* Proc. Usenix Security Symp, pp. 303- 320, Aug. 2004.

[4] Holt.J.E and Seamons.K.E, *"Nym: Practical Pseudonymity for Anonymous Networks,"* Internet Security Research Lab Technical Report 2006-4, Brigham Young Univ., June 2006.

[5] Johnson.P.C, Kapadia.A, Tsang.P.P, and Smith.S.W, *"Nymble: Anonymous IP-Address Blocking,"* Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, 2007.

[6] Lysyanskaya.A, Rivest.R.L, Sahai.A, and Wolf.S, *"Pseudonym Systems,"* Proc. Conf. Selected Areas in Cryptography, Springer,

[7] Lysyanskaya.A, Rivest.R.L, Sahai.A, and Wolf.S, *"Pseudonym Systems,"* Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, 1999.

[8] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, *"Nymble: Blocking Misbehaving Users in Anonymizing*

Networks," Technical Report TR2008-637, Dartmouth College, Computer Science,Dec. 2008
[9] Perrig, J. Stankovic, and D. Wagner, *"Security in Wireless Sensor Networks,"* Comm. ACM, vol. 47, no. 6, pp. 53-57, 2004.
[10] D. Chaum and E. van Heyst, *"Group Signatures,"* Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.
[11] J. Sun, C. Zhang, and Y. Fang, *"A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks,"* Proc. IEEE INFOCOM, pp. 1687-1695, Apr. 2008.

Authors Bibliographies

J. PRAVEEN KUMAR, working as Assistant Professor in the Department of Information Technology and having 2 years of teaching experience. He has done B.TECH in Information Technology.

B. SHYAM KUMAR, Working as Assistant Professor in the Department of Information Technology. He has done M.Tech in Software Engineering having 5 years of teaching and 2 years of Industry experience.

