*International Journal of Engineering Research and Development*
***e*-ISSN: 2278-067X, *p*-ISSN: 2278-800X, www.ijerd.com**
*Volume 3, Issue 10 (September 2012), PP. 62-67*

# Tracing Misbehaving Users by Utilizing Ticket-Based Protocols by Trusted Third Party in Anonymizing Networks

Krishna L [1], Suma Latha L[2]

[1]*M.Tech 2nd year, Department of Computer Science and Engineering, University College of Engineering, JNTU Kakinada, Kakinada, Andhra Pradesh, India.*

[2]*Associate Professor, Department of Computer Science and Engineering, University College of Engineering, JNTU Kakinada, Kakinada, Andhra Pradesh, India.*

***Abstract—Anonymizing networks provides network services to users without specific identity. Network administrator cannot identify user actions in anonymizing networks. Anonymizing networks such as The Onion Routing Networks (TOR) uses a layer structured encrypted message and series of routers each with a key to decrypt and forward the message. Which hide's the client's IP address from the server. The limitation of such networks is the users who employing this anonymity for opprobrious purposes. They use their anonymity for disfiguring web sites. The common action done by web servers is IP-address blocking but it is not possible in case of anonymous networks. Hence it simply blocks entire network. Its effect is denying access to both behaving and misbehaving users. This paper illustrate a generalized approach in which users of anonymizing networks would use resources that directly reveal their identity (e.g., passports or a national PKI) or indirect resources(IP address, Email addresses). Our system thus provide unconditional anonymity for honest users and traceability of misbehaving users by utilizing ticket-based protocols generated by trusted third party.***

***Keywords—Onion Routing, pseudonym, credential, anonymity. unconditional anonymity, Unlinkable, misbehaviors.***

## I. INTRODUCTION

Now a days due to increase in popularity of internet users and awareness of anonymity of web users, website administrators cash the user needs by attracting users by providing anonymity. Anonymity in the sense, provide services without knowing user details like phone number, address and email address. For example Wikipedia provides editable requests. User can edit the text in Wikipedia without giving user details even e-mail address. Anonymity not only in the case of email address but also in case of IP-address, passport number, PAN cord number etc. Anonymity and privacy issues have gained considerable research efforts and focused on investigating anonymity in different context or application scenarios. The anonymity-related issues have been extensively elaborated in payment-based systems such as e-cash and peer-to-peer (P2P) systems and even spread to wireless mesh networks (WMNs) in recent days. While anonymous P2P systems may support the protection of unpopular speech, they may also protect illegal activities, such as fraud, libel, the exchange of illegal pornography, the unauthorized copying of copyrighted works, or the planning of criminal activities. One requirement for anonymity is to unlink a user's identity to his or her specific activities, such as the anonymity fulfilled in the untraceable e-cash systems [2], [4] and the P2P payment systems [3], [5], where the payments cannot be linked to the identity of a payer by the bank or broker. Anonymity is also required to hide the location information of a user to prevent movement tracing, as is important in mobile networks [6], [7], [8] and VANETs [25]. In this paper we consider the Onion Routing network as an anonymizing network with which the packet routs through.

## II. INTRODUCTION TO ANONYMOUS NETWORKS

Anonymity of participants is usually achieved by special routing overlay networks that hide the physical location of each node from other participants. Common reasons to use Tor are to avoid being tracked by advertising companies on the Web, reach Internet services and sites blocked by the ISP or participating in chat rooms for victims of all kinds of abuse. Most people can probably think of at least one reason to be anonymous on the net without causing anybody else any harm. Government agencies use Tor for intelligence gathering and people in China and other countries without freedom of speech use it to communicate with other freedom seekers.

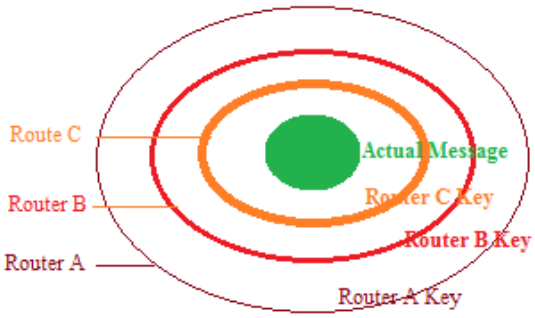


***Fig.1*** A routing onion data structure formed by encrypting a plaintext message with successive layers of encryption, each layer can be decrypted like the layer of an onion by one intermediary in a succession of intermediaries.

Tor (The Onion Router) is a system intended to enable online anonymity. "Onion Routing" refers to the layered nature of the encryption service as in fig. 1: The original data are encrypted and re-encrypted multiple times, then sent through successive Tor relays, each one of which decrypts a "layer" of encryption before passing the data on to the next relay and, ultimately, its destination. This reduces the possibility of the original data being unscrambled or understood in transit. The message with the original plaintext only being viewable by at most: the sender, the last intermediary (the exit node) and the recipient. If there is end-to-end encryption between the sender and the recipient, then not even the last intermediary can view the original message; this is similar to a game of 'pass the parcel'. us An intermediary is traditionally called a node or router.

## III. RELATED WORKS

There are several solutions for this system each with considerable effort. As follows

**A. Pseudonymous Credential Systems [14], [17], [15]:** Users log into Web sites using pseudonyms an assumed name, which can be added to a blacklist if a user misbehaves. It won't make different as all the users indirectly giving their details to web servers and reduces privacy.

**B. Anonymous Credential Systems [14], [15]:** User login to group manager. Server complains to group manager if any user in the group misbehaves. Server has to query the group manager for every authentication, and thus, lacks scalability.

**C. Traceable Signatures [16]:** Allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced. In this approach user actions before complaint also known by the server and lacks the backward unlinkability.

**D. Subjective Blacklisting:** Servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In this approach users are unaware of their whether their behaviors will be judged fairly. dynamic accumulators [17], [18], a revocation operation results in a new accumulator and public parameters for the group, and all other existing users' credentials must be updated, making it impractical.

**E. Verifier-local Revocation (VLR) [19], [20], [21]:** fixes this shortcoming by requiring the server ("verifier") to perform only local updates during revocation. It increases lots of computations on server side and hence reduces performance.

**F. Nymble [9]:** users acquire an ordered collection of nymbles, a special type of pseudonym, to connect to websites. Without additional information, these nymbles are computationally hard to link,4 and hence, using the stream of nymbles simulates anonymous 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—those used before the complaint remains unlinkable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously.

## IV. EXISTING SYSTEM

Let us have a close look at nymble [9] system based on which we implemented our solution. The user first contacts the pseudonym manager and obtains a pseudonym. The pseudonym is valid for a particular linkability window (about 20 hours or 1 day). The pseudonym is submitted to nymble manager and asks control over a website. The nymble manager generates a nymble ticket which is unique to a user-serve pair, pseudonym and a time period (probably 10 minutes). The all future nymbles of user are generated by a seed. The user submit's the nymble ticket at the web server and use the services of web server. If user misbehaves server complains to nymble manager by submitting nymble ticket of user. The nymble manager issues the seed to server with which the web-server can predict the future nymbles of user and can stop service according to servers wish. All the future connections of that particular linkbility window become linkable.

***Limitations of Existing System:*** Nymble system provides most of the features like anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted). There are minor consequences with this system.

- There are two trusted third parties, pseudonym manager and nymble manager. If one of two trusted parties compromise or compromised by any malicious node the entire system will collapse. Which causes lack of security and increases trust assumption, that is user and web-server has to believe both nymble manager and pseudonym manager.
- The only reason that nymble manager and pseudonym manager operating separately is to direct connect from user to pseudonym manager for the purpose of knowing actual IP address. The system is completely specific to IP-address blocking employed by Internet services.
- The system does not support varying linkability windows, but does support varying time periods for different servers. There are some inherent limitations for using IP addresses as the scarce resource. If a user can obtain multiple addresses, he can evade both nymble-based and regular IP-address blocking.

## V. PRAPOSED SYSTEM

Our solution is an enhancement to the nymble [] system. Users of anonymizing networks can also use resources like passport, e-cash and national PKI as identity. We can also use the email addresses as identity which could provide more privacy, but provide weak blacklistability guarantees because users can easily create new email addresses. In thais case there is no need of pseudonym manager. In our system we use a single trusted third party that is nymble manager. That is we include only the nymble manager. The user connects to the nymble manager through anonymous network. Our system provides support to vary time period (T) and linkability window (L) for different servers.

The server registers with nymble manager ones per linkability window. Each server will be with its own linkability window. User submits its identity to nymble manager. Nymble manager generates a nymble unique to user-server pair, time period and also linkability window specific to the server. These nymbles will be encapsulated with HMAC algorithm and forms nymble tickets. The user now submits nymble ticket to web-server. If user misbehaves server will complaints to nymble manager by submitting the nymble ticket and obtains seed. Web sites can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user—those used before the complaint remains unlinkable. Servers can therefore blacklist anonymous users without knowledge of their identity while allowing behaving users to connect anonymously.

**System Structure:**

The user first contacts to nymble manager by submitting self generating pseudonym and asks for control over a server by submitting user identity and server url. Server login to nymble manager by directly connecting (not anonymous connection) to NM. Server can register at NM ones per likability window. Nymble manager holds user server mapping. Using the mapping NM creates nymble. To provide the requisite cryptographic protection and security properties, the NM encapsulates nymbles within nymble tickets. User then submits nymble tickets to server and uses service provided by web server. If user misbehaves, server obtains seed from NM to identify future nymbles of that particular user. Our system ensures that users are aware of their blacklist status before they present a nymble and disconnect immediately if they are blacklisted. This feature strengthens anonymity of user.

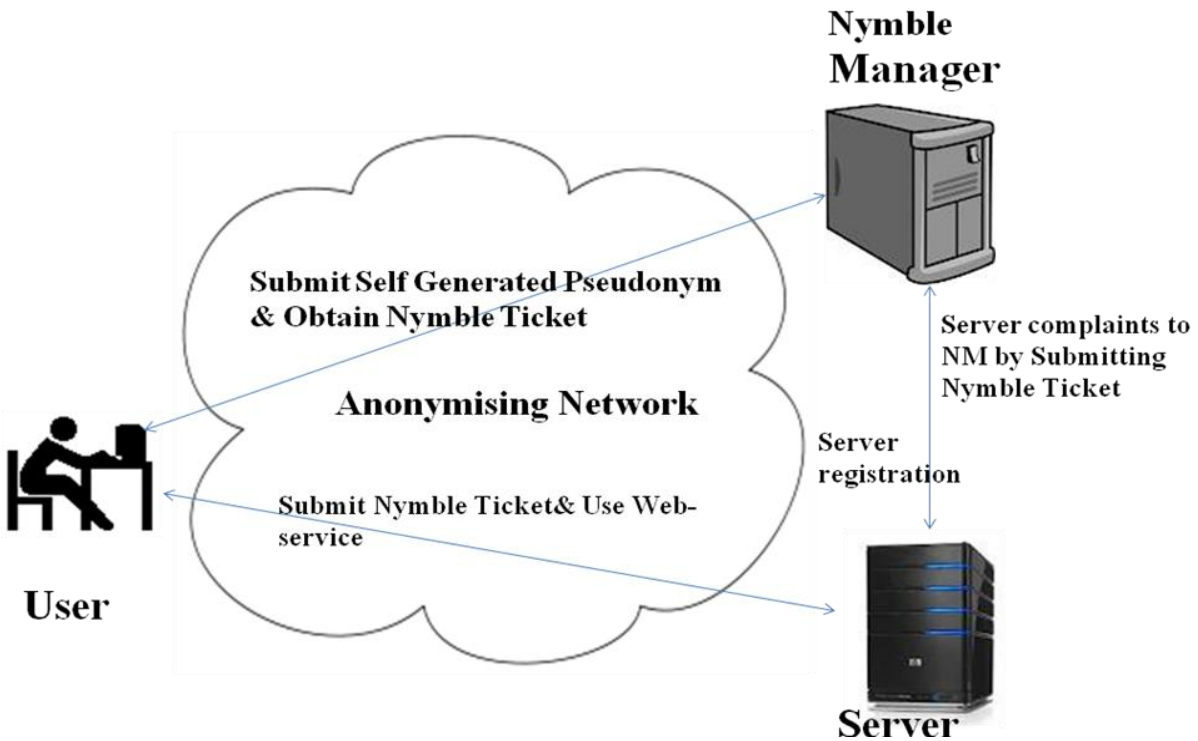


***Fig.2*** The system architecture showing the various modes of interaction. Note that users interact with the NM and servers though the anonymizing network.

The communication among Server and NM is direct communication.

**Reduced Trust model:**

The trust assumption has been reduced due to reduction in number of trusted parties. If server believes the nymble manager as honest, blacklistability and rate-limiting can be achieved. If user believes nymble manager as honest, non-framability, Anonymity and non-identity can be achieved. One more assumption for the system to work as we expected is the user should not others identity. That means the user must be legitimate.

***Table I:*** **Who Trust Whom to Be How for What Guarantee.**

| Who | Whom | How | What |
|---|---|---|---|
| **Servers** | NM | Honest | Blacklistability &Rate Limiting |
| **Users** | NM | Honest | Non-framability, Anonymity &Non-identity |

## VI. MPLEMENTATION DETAILS

Our system implemented with four major modules, Pseudonym Generation and Revocation, Nymble Manager, Blacklisting a User and Nymble-authenticated connection

**A. Pseudonym Generation and Revocation:**

- This section copes with the pseudonym generation technique and the related revocation issue. The pseudonym is used to replace the real ID in the authentication, which is necessary for both anonymous network access and location privacy.
- In the intradomain authentication in our system, the client generates his own pseudonym by selecting a secret number and computing the pseudonym. The corresponding private key can be derived, in a similar way to that of [23]. Compared to [1], [24], [6] where a batch of pseudonyms are assigned to each client by the TA, the self-generation method vastly reduces the communication overhead in the system.
- Moreover, the client is able to frequently update his pseudonyms (with tickets) to enhance anonymity by using this inexpensive method.

**B. Nymble Manager:**

- It acts as trustet third party between user and server
- After generating a pseudonym, the user connects to the Nymble Manager (NM) through the anonymizing network, and requests nymbles for access to a particular server.
- A user's requests to the NM are therefore pseudonymous, and nymbles are generated using the user's pseudonym and the server's identity. These nymbles are thus specific to a particular user-server pair.

**C. Blacklisting a User:**

- Let a user connects and misbehaves at a server the server later detects this misbehavior and complains to the NM.
- As part of the complaint, the server presents the nymble ticket of the misbehaving user and obtains the corresponding seed from the NM.
- The user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

**D. Nymble-authenticated connection:**

- It consists of cryptographic primitives like message authentication (MA), symmetric-key encryption (Enc), digital signatures (Sig).
- Assures that any honest server can indeed block misbehaving users and any honest user who is legitimate according to an honest server can nymble-connects to that server
- Rate-limiting assures any honest server that no user can successfully nymble-connect to it more than once within any single time period.

We evaluated our system as on Intel Core i3-370M with 3GB DDR3 memory and 500GB HDD, with packages Java RMI, SWING, J2ME as front end, Ms-Access07 as backend, Apache-tomcat-6.0.18 is the web server to deploy the web server application, My Eclipse 3.0 IDE is used as development tool run on Windows07.

## VII. ACHIEVEMENTS

The security requirements that our system can achieve are as follows

**A. Security primitives:** The security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely digital signature, message authentication code (MAC), and encryption, in our system.

**B. Privacy:** We provide identity privacy and protects the anonymity of honest user provided that user trust NM as honest.

**C. Backward unlinkability:** all the actions done by the user before the connection are unlinkable (i.e., including those since the misbehavior and until the time of complaint). Server can able to link only the future connections of that particular day (for example the linkability window is one day).

**D. Limited connections:** The user can obtain nymble ticket once per time period. The server has to login to NM once per linkability window. This limits the number of connections acquired for user for a given period of time.

**E. User aware of blacklist status:** Users who make use of anonymizing networks expect their connections to be anonymous. If a server obtains a seed for that user, however, it can link that user's subsequent connections. It is of utmost importance then that users be notified of their blacklist status before they present a nymble ticket to a server. In our system, the user can download the server's blacklist and verify his/her status. If blacklisted, the user disconnects immediately. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted.

**F. Nonframeability:** As we use MAC to check validity of nymble ticket, server cannot frame her own nymble tickets of a user to complaint to NM. Also user cannot generate nymble tickets to connect to server. This guarantees that any honest user who is legitimate according to an honest server can 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.

**G. Blacklistability:** Only a honest server can complaint about a user as the nymble ticket is generated by HMAC. The server cannot generate its own nymbles of any user due to HMAC. An honest server can always contact an honest NM with a valid ticket and the NM will successfully terminate during the blacklist update.

**H. Generalized Resource Form of Identity:** User can register with any form of identity like passport number, PAN cord number and even e-mail if servers allow user, more privacy. Also user can use IP-address resource of identity.

**I. Server-specific linkability windows:** our system does support varying linkability windows, and also support varying time periods for different servers as server login at NM.

## VIII. CONCLUSION

This paper mainly concentrates two issues apart from the existing system (nymble [9]). One is to provide server specific linkability window. The other is to reduce the trust assumption by reducing number of trusted parties. There are some limitations for this system. It reduces blacklistability if the user can able to get more identities with inconsiderable effort. Users of anonymizing networks would be unwilling to use resources that directly reveal their identity like passport number as it reduces privacy. Also there is a chance to forge others identity. But it is user's responsibility to make their identity secure or not forge. The system is best suited for client puzzles [22] and e-cash like systems, where users are required to perform a certain amount of computation or pay money to acquire a credential. These approaches would limit the number of credentials obtained by a single individual by raising the cost of acquiring credentials. An enhancement would be to provide protect against side-channel attacks.

## REFERENCES

[1]. M. Raya and J-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, special issue on security of ad hoc and sensor networks, vol. 15, no. 1, pp. 39-68, 2007.

[2]. S. Brands, "Untraceable Off-Line Cash in Wallets with Observers," Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cyptology (CRYPTO '93), pp. 302-318, Aug. 1993.

[3]. K. Wei, Y.R. Chen, A.J. Smith, and B. Vo, "Whopay: A Scalable and Anonymous Payment System for Peer-to-Peer Environments," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), July 2006.

[4]. D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash," Proc. Conf. Advances in Cryptology (CRYPTO '88), 2002.

[5]. D. Figueiredo, J. Shapiro, and D. Towsley, "Incentives to Promote Availability in Peer-to-Peer Anonymity Systems," Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 110-121, Nov. 2005.

[6]. G. Ateniese, A. Herzberg, H. Krawczyk, and G. Tsudik, "Untraceable Mobility or How to Travel Incognito," Computer Networks, vol. 31, no. 8, pp. 871-884, Apr. 1999.

[7]. Q. He, D. Wu, and P. Khosla, "Quest for Personal Control over Mobile Location Privacy," IEEE Comm. Magazine, vol. 42, no. 5, pp. 130-136, May 2004.

[8]. A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55, Jan.-Mar. 2003.

[9]. Patrick P. Tsang, Apu Kapadia, Cory Cornelius, and Sean W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks" IEEE transactions on dependable and secure computing, vol. 8, no. 2, march-april 2011.

[10]. D. Chaum, "Showing Credentials without Identification Transfering Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-264, 1990.
[11]. I. Damga°rd, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988.
[12]. J.E. Holt and K.E. Seamons, "Nym: Practical Pseudonymity for Anonymous Networks," Internet Security Research Lab Technical Report 2006-4, Brigham Young Univ., June 2006.
[13]. A. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems," Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, 1999.
[14]. J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, 2001.
[15]. J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.
[16]. A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 571-589, 2004.
[17]. J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, 2002.
[18]. L. Nguyen, "Accumulators from Bilinear Pairings and Applications," Proc. Cryptographer's Track at RSA Conf. (CT-RSA), Springer, pp. 275-292, 2005.
[19]. G. Ateniese, D.X. Song, and G. Tsudik, "Quasi-Efficient Revocation in Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2002.
[20]. D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, 2004.
[21]. E. Bresson and J. Stern, "Efficient Revocation in Group Signatures," Proc. Conf. Public Key Cryptography, Springer, pp. 190-206, 2001.
[22]. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairings," Advances in Cryptology-Asiacrypt 2001, pp. 514-532, Springer-Verlag, 2001.
[23]. S.M.M. Rahman, A. Inomata, T. Okamoto, M. Mambo, and E. Okamoto, "Anonymous Secure Communication in Wireless Mobile Ad-Hoc Networks," Proc. First Int'l Conf. Ubiquitous Convergence Technology, pp. 131-140, Dec. 2006.
[24]. Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 386-399, Oct. 2006.
[25]. European Telecomm. Standards Inst. (ETSI), "GSM 2.09: Security Aspects," June 1993.