Blocking of Mischievous Users in Anonymizing Networks Using Nymble System: A Survey Study

Kamble Maheshkumar S.
M. Tech. Student
Department *of CSE*
SGGS IE&T
Nanded, India
E-mail: maheshkumar.kamble@gmail.com

Prof. Hatkar S. S.
Associate Professor
Department *of CSE*
SGGS IE&T
Nanded, India
E-mail: shubhanand.hatkar@yahoo.com

***Abstract*— A Tor network popularly known as an anonymous network provides a way to access internet services anonymously through a series of routers without revealing users identity. A user almost remains unknown in the public networks and makes use of various facilities of his interest. Networks such as "Tor (The Onion Router)","Crowds" and "I2P" gained popularity in the past several years, but success of such likewise networks however has been limited by users engaging this anonymity for harmful purposes such as spoil the appearance of popular websites. As a result of this website administrators block the entire network to which the system of malicious user is connected. Hence, because of malicious users un-malicious users have to suffer. To address this problem, we present a Nymble system in which a server can "blacklist" malicious users without affecting un-malicious users and also maintaining anonymity across the network.**

Keywords- Anonymity, revocation, pseudonym.

I. INTRODUCTION

Now a day it seems very important to most of the users operating in cyberspace environment to maintain their privacy. Over last two decades a lot of research is proposed based on anonymous communication between users and lot of protocols has been designed to achieve anonymity to maintain privacy. To make a comprehensive classification of such anonymity protocols and systems a cubic taxonomy [4] approach is proposed which describes anonymity in wired and wireless networks as shown in Fig 1. One of the popular ways to maintain privacy is the use of anonymous networks like Tor [3]. Such network delivers the best efforts to maintain user's state of anonymity by hiding user's IP address. Lot of users makes a good use of this anonymous service and ensure safe communication across the public network to which we can call as well-behaving users or un-malicious users, but some users which can fall under category of malicious users can use this service repeatedly for abusive purpose. One of the popular example is defacement of website "Wikipedia". So, a website administrator cannot block the malicious user's IP address because of services provided by anonymous network, as an effect of this, a website administrator block the entire anonymous network. Here well-behaving users have to suffer because of misbehavior of malicious users, because they cannot use anonymous services.

Some of the solutions to this problem are pseudonym credential systems [9] which uses pseudonyms to blacklist a user for misbehavior and revocable anonymous credential systems [12] in which transactions made by user are remains un-linkable because of obtained credentials from an organization. Thus, we can classify our discussion of anonymous and pseudonymous blacklisting systems into three categories: the pseudonym systems, the revocable anonymous credential systems and the Nymble-like systems.

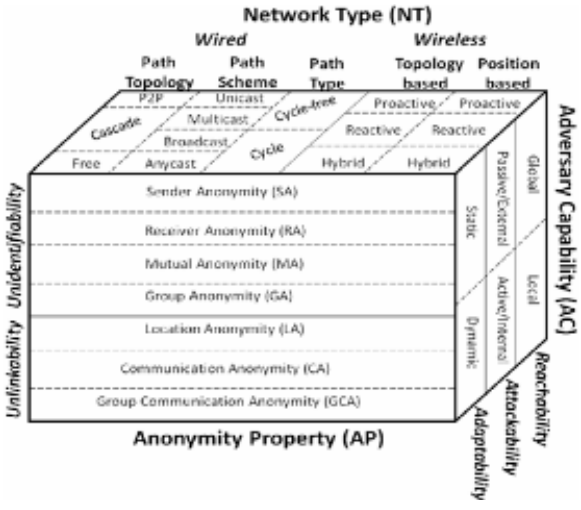

Figure 1. Cubic Taxonomy (CT) Components. [4]

A. Pseudonym Systems

As our classification, first class of blacklisting systems are the pseudonym systems. These type of systems provide user with pseudonymity on the contrary of anonymity. Here, user's identity at same or different service providers remains unlinkable to her real identity but some actions of users at a particular service provider are easily linked because a user can communicate with service provider using a persistent pseudonym. This makes revocation task very simple by adding the pseudonym to a blacklist and denying access to any user with a pseudonym on the blacklist. Existing pseudonym systems are merely based on: 1) offstage credentials 2) group signatures.

1) Offstage Credentials

Pseudonym systems are used to control the transfer of information between a user and various organizations. In this scheme user first has to establish a pseudonym with an organization with which she wishes to communicate. Then, user obtains a credential over a pseudonym to transfer information about herself to organization.

2) Group Signatures

In 1991, Chaum and van Heyst proposed group signatures [11], wherein each member of a group can sign any message on behalf of the group. Anyone can verify a group signature using the group's public key but a special entity known as Revocation Manager can only verify a particular group signature of a group member. Misbehavior of any user within group, link the users past and future activities and thus anonymity of that user get revoked.

Thus we conclude that pseudonym systems provide users with pseudonymity instead of full anonymity. Therefore, even under normal operation, users (misbehaving or otherwise) are subject to a loss of privacy as compared to using an anonymous communications network without a pseudonym system. So the remaining classes such as revocable anonymous credentials and Nymble-like systems improves pseudonym systems by adding a crucial term known as unlinkability which leads a user to full anonymity.

B. Revocable Anonymous Credential Systems

The second class of blacklisting systems is revocable anonymous credential systems. Many blacklisting systems rely on Trusted Third Party (TTP) for authentication like our Nymble system but some of the systems do not rely on these TTP for the purpose of authentication. Revocable anonymous credential systems completely replace the use of TTP with zero-knowledge proofs. Unfortunately, the high computational overhead associated with them means that they are often of theoretical interest only.

C. Nymble-like Systems

The third class of anonymous blacklisting systems are the Nymble-like systems. P. P. Tsang proposed Nymble [1] as a solution to the problem of allowing service providers across Internet to revoke the activity of individual misbehaving user of anonymous networks. Nymble uses a novel construction to build mutually unlinkable and verifiable authentication tokens for users of anonymous networks, while empowering service providers with access revocation capabilities comparable to what they have with non-anonymous users. In particular, this scheme implements a privacy-preserving IP address blocking for users who communicates through anonymous networks.

"Nymble System" provides properties such as:

- Anonymous authentication.
- Backward unlinkability.
- Subjective blacklisting.
- Fast authentication speed.
- Rate-limited anonymous connections.
- Revocation auditability.
- Anti-Sybil attack.

In Nymble system, a user acquire collection of nymbles, a special type of pseudonym to connect to websites. Websites can blacklist user by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user by making the nymbles which were used before complaints remain unlinkable.

Hence, server can blacklist the anonymous user without knowledge of their IP addresses while allowing well behaving users to connect anonymously. In this system, user should be aware of her blacklist status before she communicate with Nymble system and disconnect immediately if blacklisted.

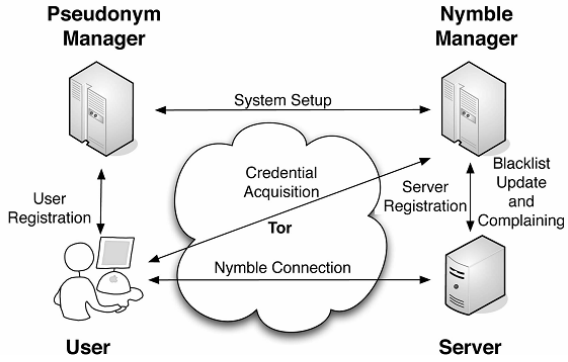

Figure 2. The Nymble system architecture [1]

Above (Fig.2) is the Nymble system architecture with various modes of interaction in anonymous networks. This system overcome from many drawbacks which arise at previously proposed systems including the speed, computation work, security etc.

1) Working of Nymble:

Nymbles are generated by the "Nymble Manager" based upon pseudonym and server ID. Websites can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user. One important thing which can be observed in our proposed system is that even though the future nymbles of the abusive user are linked,

the nymbles that are used before complaint remain unlinkable. Hence, Nymble system guarantees backward unlinkability.

There are basically two modules in Nymble system. They are:

a) Pseudonym Manager: User need to contact the pseudonym manager and demonstrate control over a particular resource in order to get its IP-address blocked. The user is required to connect to the PM directly i.e. not through a known anonymizing network. Pseudonym Manager has the knowledge about Tor routers and hence it won't accept it if a user tries to connect with it with anonymizing network.

The basic idea behind connecting directly with Pseudonym Manager is that, it can identify the IP-address of the user. Pseudonyms are chosen based upon the controlled resource ensuring that the same pseudonym is always issued for the same resource. Pseudonym Manager only knows the IP address-pseudonym pair and hence it does not know the server to which the user wants to connect. User contacts the Pseudonym manager only once per linkability window (e.g. Once a day).

b) *Nymble Manager:* After getting the pseudonym from the pseudonym manager, the user connects to the Nymble Manager through anonymizing network and requests nymbles for access to a particular server.

Nymbles are generated using the user's pseudonym and the server's identity. Nymble Manager doesn't know anything about the user's identity. It knows only the pseudonym-server pair. Nymble Manager encapsulates nymbles within "Nymble tickets" in order to provide cryptographic protection and security properties.

Nymble tickets are bound to specific time periods. In Nymble system, time is divided into linkability windows of duration W and each w is split into L time periods of duration T, i.e. W=L*T.

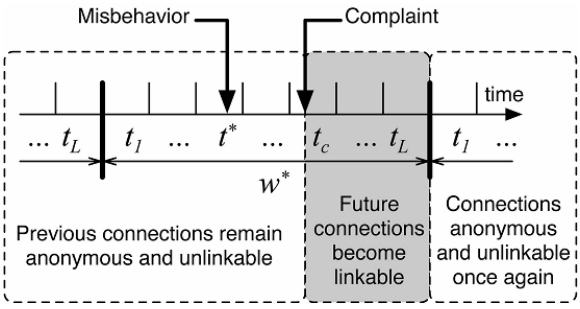

Figure 3. The life cycle of a misbehaving user. [1]

From the above Fig.3, we can illustrate that future connections will become linkable for a particular current window from which the complaint is registered and after that window the connections will be anonymous and unlinkable once again. This shows the backward unlinkable nature of this system.

2) Goals of Nymble System:

Nymble system aims for four security goals. They are:

a) Blacklistability: Blacklistability assures that any honest server can indeed block misbehaving users. Specifically, if an honest server complains about a user that misbehaved in the current linkability 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 linkability window.

b) Rate-limiting: Rate-limiting assures any honest server that no user can successfully nymble-connect to it more than once within any single time period.

c) Anonymity: Anonymity protects the anonymous nature of honest users, regardless of their legitimacy according to the server.

d) Non-frameability: It 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.

II. NYMBLE IN WIRELESS NETWORKS

This system also used in wireless sensor networks as a part of a K-Anonymity privacy preserving location monitoring system [6] which allows users to access services privately by hiding its own IP address. This wireless anonymous network is developed for the purpose of monitoring personal locations which must not carried out by an untrusted server as it my poses threat to the privacy of a monitored individual.

To enable the system to provide high quality location monitoring services two location anonymizing algorithms are considered namely resource and quality aware algorithms and are depends on k-anonymity privacy agenda. In this procedure a person is indistinguishable among k persons, to enable trusted sensor nodes to provide the aggregate location information of monitored persons. Each aggregate location is in a form of a monitored area A along with the number of monitored persons residing in A, where A contains at least k persons.

The Resource aware algorithm reduces the communicational and computational cost, on the other hand the quality-aware algorithm increase the accuracy of the aggregate locations by reducing their monitored areas.

In this anonymity preservation technique Nymble architecture have an additional model called as privacy model. In this model sensor nodes over a trusted zone and server can communicate with each other anonymously to avoid the attacks from a malicious user in the network. To get k-anonymous aggregate locations sensor node execute the location anonymization algorithm. Here, resource aware algorithm helps to minimize communication and computational cost whereas quality aware algorithm helps in minimize size of clocked areas.

Thus this algorithm provides high-quality location monitoring services, while preserving the monitored object's location privacy with the help of Nymble system.

On the basis of Trusted Third Party (TTP) we can again classify our anonymous blacklisting systems into two broad categories: 1) Anonymous blacklisting systems with TTP (e.g., Nymble). 2) Anonymous blacklisting systems without TTP (e.g., PEREA, BLAC).

As we have explained Nymble system in section 1.3 as first category of our classification with TTPs. Now we move towards the second category of classification without TTPs and discuss about PEREA [] as an example of this classification.

III. PEREA

It is the second category of the system based on our classification over TTPs. This system popularly known as PEREA [5] which is a practical TTP-free revocation of repeatedly misbehaving anonymous users. Need behind proposing such a system is same as need behind proposing Nymble system. As user knows the fact that she can remain fully anonymous through anonymous networks like TOR [3], this fact leads to misbehavior of a user. So, here to defend such type of activities user have to authenticate itself to Service Providers. In Nymble system, as a part of revocation of such users TTPs can take action against misbehaving users. Authentication made by TTPs depends on possession of pseudonyms which are encrypted with TTP's key. If any user misbehaves, Service Provider handover escrowed identity of that user to TTP which is most important step while making complaint. But, action of handover of such an information of user to TTPs never guaranteed anonymity of their connections. The only drawback with the TTPs is Service Provider must have to trust TTPs which seems unfair to users like Whistleblowers etc.

Eliminating TTPs: BLAC [8] is a very firstly proposed scheme that can eliminate involvement of TTPs in revocation of anonymous users. In this scheme Service Providers can add an entry from an anonymous user's authentication transcript to a blacklist, on the basis of which the user is revoked and cannot authenticate. This eliminates the involvement of TTPs in revocation procedure. Here, blacklist with thousands of entries leads to a severe bottleneck at Service Provider because the amount of computation at Service Provider required for authentication is linear in the size of the blacklist, i.e., O (L) where L is the number of entries in the blacklist. With BLAC "more efficient blacklist checking" is a problem and hence PEREA is designed to address this problem.

In PEREA the complexity of authentication at Service Provider is independent of size of blacklist. To explain this P. P. Tsang gives the following example [5]

Example: If K= 7, then the SP (Service Provider) must blacklist a user's misbehavior before that user has made 7 subsequent authentications. Note that a blacklisted user is not revoked if he or she has already made K subsequent authentications, and therefore we differentiate between the action of blacklisting and the end result of whether the user is actually revoked. Since the SP may take some time to recognize misbehaviors (e.g., malicious edits on Wikipedia may not be detected immediately), these K authentications can be rate limited to K authentications every T minutes. Combined with rate limiting, SPs have enough time (T) to recognize misbehaviors, and honest users can authenticate anonymously at an acceptable rate (one authentication every T/K minutes on average). For example, for K= 7, T = 70, SPs must judge misbehaviors within 70 minutes, and users can authenticate once every 10 minutes on average. In many cases where users are not expected to authenticate more than a few times a day, K= 10, T = 2880 would allow SPs 2 days to catch misbehaviors and allow 5 authentications per day on average. In practice, SPs would want to keep K low to rate limit anonymous authentications.

IV. SUMMARY

Throughout this survey we have explain and discuss anonymous blacklisting systems like PEREA, BLAC which introduce a concept like revocation window size in parallel with Nymble system which introduces use of TTPs in anonymous credential blacklisting systems. Comparison of various blacklisting systems on the basis of different

As we have compare and discussed different kinds of blacklisting systems like Nymble, PEREA, BLAC etc. There are more such systems like Nymbler, BNymble etc. which are Nymble-like systems are compared by R. Henry on the basis of their properties with the help of following Table I.

Table I [2]

Scheme	Misauthentication resistance	Unlinkability	Backward anonymity	Revocability	Revocation auditability	Non-frameability	ZK-verifym	ZK-pseudonym	Objective vs. subjective	Rate-limiting	Blacklist transferability	Retroactive revocation	User efficient	Verifier efficient
UST [41]	✔	✔	✔	✔	✔	✔	∞[3]	✔	S	✔			✔	✔
Nymble [30]	✔	✔	✔	✔	✔	✔			S[1]	✔		✔	✔	✔
Nymbler [26]	✔	✔	✔	✔	✔	✔	k[4]	✔	S[1]	✔	✘[2]	✔	✔	✔
BNymble [34]	✔	✔	✔	✔	✔	✔	∞[3]		S[1]	✔		✔	✔	✔
Jack [32]	✔	✔	✔	✔	✔	✔	∞[3]	✔	S/O		✘[2]	✔		✔

On the other hand R. Henry compares various revocable anonymous credential systems like BLAC, PEREA etc. with the help of Table II

Table II [2]

Scheme	Misauthentication resistance	Unlinkability	Backward anonymity	Revocability	Revocation auditability	Non-frameability	Objective vs. subjective	Rate-limiting	Blacklist transferability	Retroactive revocation	User efficient	Verifier efficient
CL [11]	✔	✔	✔	✔	✔	✔	S			✔		
BDD [7]	✔	✔	✔	✔	✔	✔	S		✔	✔		
BLAC [46]	✔	✔	✔	✔	✔	✔	S		✔	✔		
EPID [8]	✔	✔	✔	✔	✔	✔	S		✔	✔		
PEREA [49]	✔	✔	✔	✔	✔	✔	S			✔[1]		✔

.

properties like unlinkability, revocability etc. is helpful in judging these systems in real time scenario.

V. CONCLUSION

While looking at the comparison of different kind of anonymous blacklisting systems Nymble system provide most secure way to maintain anonymity and privacy of a user (malicious or any other). Nymble System eliminated nearly all weaknesses and drawbacks in the previously developed systems to make use of anonymizing networks which was blocked by many service providers. Even though there are still some issues related to backward unlinkability, this system provides enormous security properties and provide an added advantage in terms of blacklistability and non-frameability.

REFERENCES

[1] Patrick P. Tsang, Apu Kapadia,"Nymble: Blocking Misbehaving Users in Anonymizing Networks," IEEE Transactions on Dependable and Secure Computing vol. 8, No. 2, March-April 2011.

[2] R. Henry and I. Goldberg, "Formalizing Anonymous Blacklisting Systems (Extended Version)." Centre for Applied Cryptographic Research, UWaterloo, Technical Report CACR 2010-24, 2010.

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

[4] Douglas Kelly, Richard Raines, Rusty Baldwin, Michael Grimaila, and Barry Mullins, "Exploring Extant and Emerging Issues in Anonymous Networks: A Taxonomy and Survey of Protocols and Metrics," IEEE Communications Surveys and Tutorials, vol. 14, No. 2, Second Quarter 2012.

[5] P.P. Tsang, M.H. Au, A. Kapadia, and S.W. Smith, "PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication," Proc. ACM Conf. Computer and Comm. Security, pp. 333-

[6] Gayathri M., Bharathi M.," K-Anonymity Privacy-Preserving Location Monitoring System for Wireless Sensor Networks with Nymble Secure System," International Journal of Computer & Organization Trends –Vol.2 Issue 2- 2012.

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

[8] P. P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith, "Blacklistable anonymous credentials: Blocking misbehaving users without TTPs," In ACM CCS, pages 72–81. ACM, 2007.

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

[10] 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.

[11] M. Bellare, H. Shi, and C. Zhang, "Foundations of Group Signatures: The Case of Dynamic Groups," Proc. Cryptographer's Track at RSA Conf. (CT-RSA), Springer, pp. 136-153, 2005.

AUTHORS PROFILE

1. Prof. Hatkar S. S.

B.E. (Computer Science & Engg.), M.E. Electronics (Specialization in Computer) having 17 years of experience in Academic. Currently he is the Associate Professor at Shri Guru Gobind Singhji Institute of Engineering and Technology, at Nanded. His areas of specialization are Information Security and Theory of Computer Science.

2. Kamble Maheshkumar S.

Persuing M.Tech. (Computer Networks & Information Security) at Shri Guru Gobind Singhji Institute of Engineering and Technology, at Nanded. His area of interest are Computer Networking and Cryptography.