RESEARCH ARTICLE OPEN ACCESS

Nymble Counter Measures for Failure Tolerant Anonymzing Networks

Reshma Balanagu[1], **Dr A Jayalakshmi[2],**
[1]STUDENT, D V R & Dr H S MIC College Of Technology, Kanchikacherla, Krishna (Dt).
[2]PROFESSOR, D V R & Dr H S MIC College Of Technology, Kanchikacherla, Krishna (Dt).

Abstract
Tor is a form of Anonymzing networks comprised of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. Individuals use Tor to keep websites from tracking them. Anonymzing networks provide users with anonymous browsing capabilities over the web using a series of routers to hide the client's IP address. Under the cover of anonymity, certain users have repeatedly launched deface/dos attacks over popular web sites such as Wikipedia. Since web site administrators cannot blacklist individual adversaries' IP addresses, they end up blacklisting the entire Anonymzing network resulting in loss of service to genuine users thus effecting entire Anonymzing network services. Previously to counter these issues Nymble System was proposed and implemented which is essentially a combination of Anonymization Network along with Pseudo Manager for nymble token operations, ip hiding activities and Nymble Manager for encountering and acting on adversaries, interfacing the clients with anonymizing network. Although Nymble System was effective in syncing target servers with the system for an efficient reporting and countering mechanisms, it has a huge computation overhead. So we propose to tweak Nymble System to allow users to access Internet services privately by using a series of mix servers and proxy repositories to hide the client's IP address from the target servers instead of the multiple routers based ip hiding approach of prior systems. These methods ensure that the number of algorithms to sync target servers with Nymble system is not beyond 10 thus reducing the computation overhead. An implementation validates the claim of the proposed system's ability to offer and preserve anonymization services yet effectively handling adversaries of the network.

Index Terms: *Anonymzing Networks, Nymble, Pseudonym Manager, Nymble Manager.*

I. INTRODUCTION

Anonymizing networks such as Crowds and Tor route traffic through independent nodes in separate administrative domains to hide the originating IP address. Anonymizing networks allows users to access Internet services privately by using a series of routers to hide the client's IP address from the server. Success of such networks seen an exponential rise, however, challenges presented by certain adversaries(users employing this anonymity for abusive purposes such as defacing popular Web sites or launching DoS attacks etc) hamper their reputation. Under the cover of anonymity, users have repeatedly defaced popular Web sites such as Wikipedia. In existing network, Web site administrators cannot blacklist individual malicious users' IP addresses, they blacklist the entire anonymizing network resulting in loss of service to genuine users. Such counter measures eliminate malicious activity through anonymizing networks at the cost of denying anonymous access to behaving users. This has happened repeatedly with Tor. So, a better system is required that can offer and preserve anonymization service yet effectively identifying the adversaries in the network.

Later, another system was proposed to use anonymizing networks such as Nymble System[1] instead of Tor. Nymble System allows users to access Internet services privately by using a series of routers to hide the client's IP address from the target servers. Nymble System is essentially a combination of Anonymization Network along with Pseudo Manager for nymble token operations, ip hiding activities and Nymble Manager for encountering and acting on adversaries, interfacing the clients with anonymizing network etc. Nymble system provides all the following properties that are vital features for successful flow of anonymization services: anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and addresses the Sybil DoS attack to demonstrate misbehaving (to make its deployment practical). Nymble system offers and preserves anonymization services yet effectively handling adversaries of the network.

In proposed system, we still use Anonymizing networks such as Nymble System. But, usage of 16 algorithms to sync target servers with Nymble system for an efficient reporting and countering mechanisms is a huge computation overhead. Here, we propose to tweak Nymble System to allow users to access Internet services privately by using a series of mix servers and proxy repositories to hide the client's IP address from the target servers instead of the multiple routers based ip hiding approach of prior systems. Along with that, to extend Pseudo Manager with proxy allocation strategies along with nymble token operations instead of ip hiding activities. These methods ensure that the number of algorithms to sync target servers with Nymble system is not beyond 10 thus reducing the computation overhead. List of the reduced/modified algorithms are: PMCreatePseudonym, NMVerifyPseudonym, NMCreateCredential, NMVerifyTicket, NMUserCheckIfBlacklisted, NMGrantAccess, ServerVerifyTicket, NMHandleComplaints, NMComputeBLUpdate, ServerUpdateState. So a mix server based approach along with proxy allocation strategies provides an efficient anonymization network.

II. RELATED WORK

Some of the authors of the Nymble system[1] tried to eliminate the role of a trusted third party (TTP). They developed an anonymous credential system called BLAC using a signature proof of knowledge (SPK) scheme. In this system there is an entity called Group Manager (GM) who is responsible for issuing credential for users. This entity should not be considered a TTP since GM does not know the credential of a user and hence can't revoke user's privacy.

As a consequence, the anonymity of a user is preserved permanently and this system is more scalable and more robust than the Nymble system. The major problem with this solution is that it degrades the performance of the system. The computation cost of authentication protocol including proof verification and blacklist checking, grows linearly with the size of the blacklist[5]. Unfortunately, high computation cost directly affects the overall latency perceived by the end user.

In some systems, misbehavior can be defined precisely. For instance, double-spending of an "e-coin" is considered misbehavior in anonymous electronic cash systems. Likewise, compact e-cash, k-times anonymous authentication and periodic ntimes anonymous authentication deem a user to be misbehaving if she authenticates "too many" times. In these cases, convincing evidence of misbehavior is easily collected and fair judgment of misbehavior can be ensured. While such approaches can encourage certain kinds of fair behavior in anonymizing networks (e.g., e-coins can be used to control bandwidth consumption of anonymous users), it is difficult to map more complex notions of misbehavior onto "double spending" or related approaches.

Chaum et al.[3] provide a solution to a closely-related problem. To facilitate anonymous and unlinkable transactions, users are issued a blind signature for access to a service. This blind signature can be renewed with another blind signature (for the subsequent connection) each time the user has been served. If a user misbehaves, a server can terminate its service to that user by not renewing that user's blind signature. As a result, misbehavior must be detected during the user's connection.

In PEREA [4], an anonymous authentication scheme without TTPs using accumulators as blacklists is introduced. In this system, the user must maintain a queue of his past K authentication tickets and prove in zero knowledge that none of these tickets are on the blacklist. Therefore, the computation cost at the side of service provider is independent of the size of the blacklist and instead merely depends on the size of revocation window, K, that is much less than the blacklist size.

Complexity analysis of PEREA[4] shows that it is more efficient than BLAC; however, the computation complexity of proof generation at the client side is still $O(K\Delta L)$, where ΔL is the difference between the size of current blacklist and the size of the previous one, and it is $O(K)$ at the server side. Taking the cost of zero knowledge proof into account, we can say there is still room for improving the performance of this system. Moreover, making PEREA[4] more flexible by enabling forgiveness option changes the performance of the authentication protocol.

III. OVERVIEW TO NYMBLE

The Pseudonym manager[1] : The user initially must connect to Pseudonym Manager (PM) and establish control over a resource; so as to block the IP-address, the user ought to connect to the Pseudonym Manager directly. We presume that PM has knowledge of Tor routers and can ensure that users are communicating with it directly. Pseudonyms are chosen based on the controlled resource, making sure that the very pseudonym is always issued for the same resource. The user does not disclose what server he wants to connect to, and the PM's duties are restricted to mapping IP addresses (or other resources) to pseudonyms. The user connects to the PM only once per likability window (e.g., once a day).

The Nymble Manager *[1]:* Post gaining a pseudonym from the PM, the user connects to the Nymble Manager via the anonymizing network, and then request for nymbles to obtain 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. Nymbles are thus specific to a particular user-server pair. As long as the PM and the NM do not collude, the NM knows only the pseudonym-server pair, and the PM knows only the user identity-pseudonym pair. In order to provide the required cryptographic protection and security properties, nymbles are encapsulated within nimble tickets. Servers pack seeds into linking tokens, and therefore, we will speak of linking tokens being used to link future nymble tickets.

Time: Nymble tickets are linked with specific time periods. Time is divided into linkability windows of duration W, each of which is split into L time periods of duration T.

Blacklisting a user: In case of misbehavior, the server may link any future connection from this user within the same linkability window. A user misbehaves at a server during time period within linkability window. The server then finds this misbehavior and reports it to the NM in time period of the same likability window. In the complaint, the server presents the nymble ticket of the misbehaving user and obtains the corresponding seed from the NM. Even though misbehaving users can be blocked for the future too, the past connections anyhow remain unlinkable, providing subjective blacklisting and backward unlinkability.

Notifying the user of blacklist status: Users using anonymizing networks want their connections to be anonymous. When a server obtains a seed for that user, it can still link the user's subsequent connections. It is very important that users be notified of being blacklisted before presenting a nymble ticket to a server. The user can thus download the server's blacklist and verify its status. When blacklisted, the user immediately gets discontinued.

IV. PROPOSED SYSTEM

In proposed system, in order to tweak Nymble System to allow users to access Internet services privately by using a series of mix servers and proxy repositories to hide the client's IP address from the target servers instead of the multiple routers based ip hiding approach of prior systems. A mix network consists of multiple mixes that are interconnected by a network as shown in figure 1. Such a mix network may provide enhanced anonymity, as payload packets may go through multiple mixes. Since the end-to-end performance of any mix network eventually relies on the performance of its individual mixes, the analysis of the single mix provides a foundation for analyzing the end-to-end performance of mix networks.

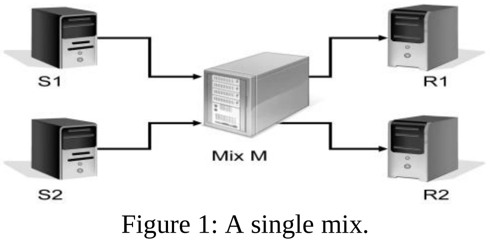

Figure 1: A single mix.

In order to design proposed nymble system along with mix servers, proposed system uses Distributed Pseudonym Manager and Distributed Nymble Manager. The PM issues pseudonyms to users. A pseudonym pnym has two components nym and mac: nym is a pseudorandom mapping of the user's identity (e.g., IP address),the likability window w for which the pseudonym is valid, and the PM's secret key nymKeyP; mac is a MAC that the NM uses to verify the integrity of the pseudonym. Initially creating and verifying pseudonyms are done. Later, The NM executes all initial states and initializes nmState in order to generate the algorithm's output. The NM extracts macKeyNP from nmState and sends it to the PM over a type-Auth channel. macKeyNP is a shared anonymously between the NM and the PM, so that the NM can verify the authenticity of pseudonyms issued by the PM.

Propose to tweak Nymble System to allow users to access Internet services privately by using a series of mix servers and proxy repositories to hide the client's IP address from the target servers instead of the multiple routers based ip hiding approach of prior systems. Propose to extend Pseudo Manager with proxy allocation strategies along with Nymble token operations instead of ip hiding activities.

These methods ensure that the number of algorithms to sync target servers with Nymble system is not beyond 10 thus reducing the computation overhead. Nymble, a pseudorandom number, plays the role of an identifier for a particular time period. Nymbles (presented by a user) across periods are unlinkable unless a server has blacklisted that user. A credential contains all the nymble tickets for a particular linkability window that a user can present to a particular server. NMCreateCredential has a procedure that generates a credential when requested: A ticket contains a server specific nymble, linkability window and time period. ctxt is scrambled data that NM uses during a nymble ticket complaint. In particular, ctxt contains the first nymble in the user's sequence of nymbles, and the seed used to generate that nymble. Upon a complaint, the NM extracts the user's seed and issues it to the server by evolving the seed, and nymble helps the NM to recognize whether the user has already been blacklisted.

The MACs macNS and macNS are used by the NM and the server, respectively, to verify the integrity of the nymble ticket uses NMVerifyTicket and ServerVerifyTicket algorithms. The NM will need to verify the ticket's integrity upon a complaint from the server. Now, Server Link Ticket algorithm performs the task of checking if the likability of the ticket. If the nymble is linked to the server then we can conclude that the user has misbehaved and thus the status of the user is updated using Server Update State algorithm. We are performing following operations in attacking a frame in to different levels of processing using Grant Access algorithms as follows:

```
Algorithm: NM Grant Access
Input: (Token t,PM,Anonymization network)
Output: Return $GA_s$
Extract token(t) from PM present in nmState
Verify token t in NM
Mac(key) ε nmState
Verify mac(key) & token generation
Return : Verify Token
Return: Grant Access from Nymble Manager
```

Algorithm 1: Grant Access algorithm for server verification.

Nymble server access services to all the user present in the Nymble system process. Those accessing results are obtained by the individual verification about each Nymble client. A server's blacklist is a list of nymbles corresponding to all the nymbles that the server has complained about. Users can quickly check their blacklisting status at a server by checking to see whether their nymble appears in the server's blacklist by using User Check If Blacklisted algorithm.

NMComputeBLUpdate algorithm creates new entries to be appended to the server's blacklist. Each entry is either the actual nymble of the user being complained about if the user has not been blacklisted already or a random nymble otherwise. This way, the server cannot learn if two complaints are about the same user, and thus, cannot link the Nymble connections to the same user.

V. PERFORMANCE ANALYSIS

Multiple Likability: With multiple likability windows, our Nymble construction still has Accountability and Nonframeability because each ticket is valid for an d only for a specific likability window; it still has Anonymity because pseudonyms are an output of a collision-resistant function that takes the likability window as input.

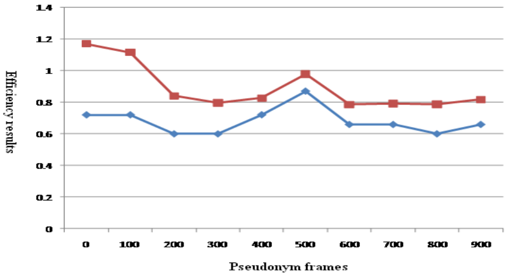

Figure 2: Comparison results with pseudo frames with time efficiency results.

As shown in the above figure comparison results of each Nymble client associated with Nymble server presented in the component process of the anonymizer network for individual development of each client results with time comparison.

Side-channel attacks: While our current implementation fully protect against side-channel attack with the help of mix servers. In existing system, while implementing various algorithms in a way that their execution time leaks little information that cannot already be inferred from the algorithm's output. In proposed system, those kinds of problems and attacks are resolved with the help of mix servers.

Blacklist ability: An honest PM and NM will issue a coalition of unique users at most valid credentials for a given server. Nymble Manager can issue valid tickets, and for any given time period, the coalition has at most valid tickets, thus making at most connections in any time period irrespective of server's blacklisting. It is sufficient to show that if each of the c users has been blacklisted in some previous time period, the coalition cannot authenticate in the time period.

VI. CONCLUSION

Anonymizing networks allows users to access Internet services privately by using a series of routers to hide the client's IP address from the server. Anonymity covers certain adversaries have repeatedly defaced/dos attacked popular Web sites such as Wikipedia. Previously to counter these issues Nymble System was proposed. Although Nymble System was effective in syncing target servers with the system for an efficient reporting and countering mechanisms, it has a huge computation overhead. In proposed system, in order to tweak Nymble System to allow users to access Internet services privately by using a series of mix servers and proxy repositories to hide the client's IP address from the target servers instead of the multiple routers based ip hiding approach of prior systems. Along with that, to extend Pseudo Manager with proxy allocation strategies along with nymble token operations instead of ip hiding activities. These methods ensure that the number of algorithms to sync target servers with Nymble system is not beyond 10 thus reducing the computation overhead. In this paper we are introduce the fixed blocking mechanisms for detecting attacker. Further improvement of our Nymble is above considerations can be developed in variant blacking mechanisms for detecting attacker.

REFERENCES

[1] 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*, 99(1), 2009.

[2] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-90, Feb.1981.

[3] David Chaum. Blind signatures for untraceable payments. *Advances in Cryptology - Cryptography*, 82, 1982.

[4] Patrick P. Tsang, Man Ho Au, Apu kapadia, and Sean W. Smith. Perea: towards practical ttp-free revocation in anonymous authentication. In *CCS '08: Proceedings of the 15th ACM conference on Computer and communications security*, pages 333–344, New York, NY, USA, 2008. ACM.

[5] Patrick P. Tsang, Man Ho Au, Apu Kapadia, and Sean W. Smith. Blacklistable anonymous credentials: blocking misbehaving users without ttps. In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pages 72–81, New York, NY, USA, 2007. ACM.

[6] 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.

[7] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, “A Practical and Provably Secure Coalition-Resistant Group Signature, Scheme,” Proc. Ann. Int’l Cryptology Conf. (CRYPTO), Springer, pp. 255-270, 2000.