Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Misbehaving User Detection using Nymble Counter Measures in Anonymization Networks

Aryan Chandrapal Singh
Dept. Of Computer Engg.
Jaihind College of Engg., Pune, India

Wavhal Dnyaneshwar N.
Dept. Of Computer Engg.
Jaihind College of Engg., Pune, India

Tambre Keshav G.
Dept. Of Information Tech.
Dnyanganga College of Engg., Pune, India

Abstract— In anonymization networks users share data with another network services included with semantic working procedure for accessing one user to user data communication process. For performing these results efficiently in commercial element generation in each user. But user behavior is main task in present days. For doing this task efficiently, traditionally Nymble a misbehaving user detection mechanism can be developed. This process can do efficient working with detection of misbehaving user using Nymble Manager services in anonymization networks. Nymble system was effective mechanism for solving relevant applications efficiently. 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. In this paper we proposed to extend existing nymble networks can be support to multiple servers or multiple users recommendation. This implementation can be validates to user communication efficiently. Our experimental results show efficient third party generation for detecting anonymization user prediction.

Keywords— Anonymization Networks, Nymble manager, Pseudo Manager, Tor Networks.

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.

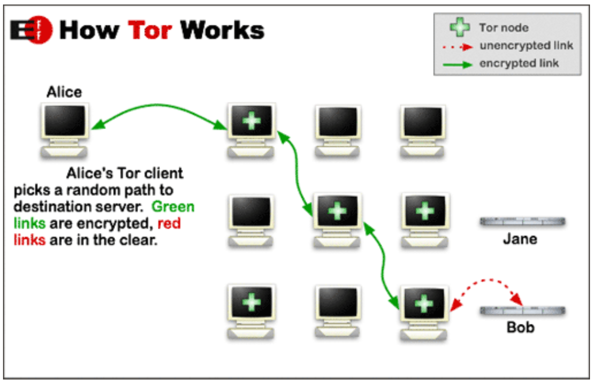
How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

Figure 1: Anonymization Networks.

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. BACK GROUND WORK

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.

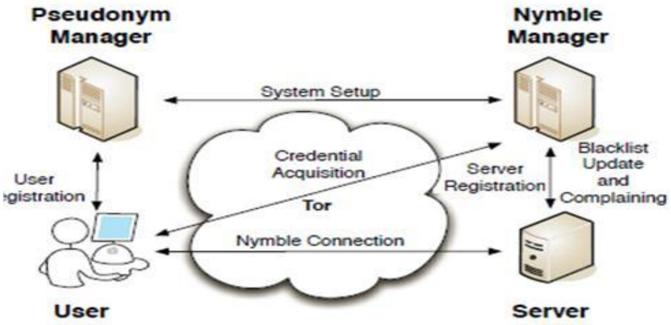

Figure 2: Nymble mechanism for accessing services from server.

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.

III. 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.

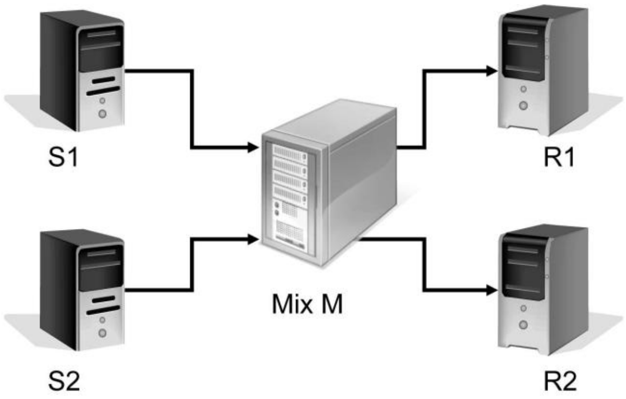

Figure 1: A single mix.

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 ε
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.

IV. EXPERIMENTAL RESULTS

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.

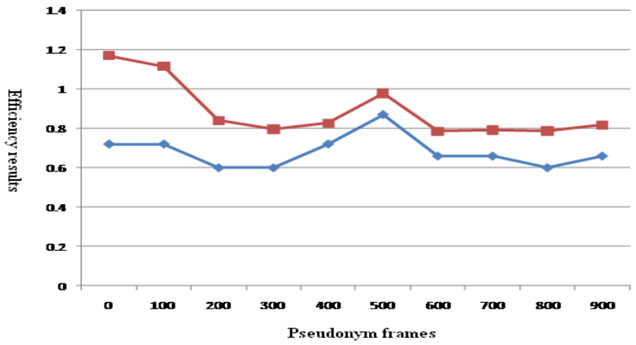

Figure 2: Comparison results with pseudo frames with time efficiency results.

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.

V. CONCLUSIONS

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. Nymble system was effective mechanism for solving relevant applications efficiently. 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. In this paper we proposed to extend existing nymble networks can be support to multiple servers or multiple users recommendation. This implementation can be validates to user communication efficiently. Our experimental results show efficient third party generation for detecting anonymization user prediction.

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] 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.

[3] 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.

[4] 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.

[5] Reshma Balanagu, , Dr A Jayalakshmi, "Nymble Counter Measures for Failure Tolerant Anonymzing Networks ", Reshma Balanagu et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 3, Issue 6, Nov-Dec 2013, pp.1425-1429.

[6] P.P. Tsang, M.H. Au, A. Kapadia, and S.W. Smith, "Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 72-81, 2007.

[7] 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- 344, 2008.

[8] 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.