Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Anonymous Communication in Computer Networks: A Survey

Maheshkumar S. Kamble[#1], **Hatkar S. S.**[*2]

[#]M. Tech. Student, Dept. of CSE, SGGS IE&T,
Nanded, India.

[*]Associate Professor, Dept. of CSE, SGGS IE&T,
Nanded, India.

Abstract— Anonymous network enables users to access the World Wide Web while blocking any tracking or tracing of their identity on the Internet. The goal is to hide the identities of sourced and destination nodes, and route of information flow in the network. This type of online anonymity forward Internet traffic through a worldwide network of different kind of servers. Anonymous networks prevent traffic analysis and network surveillance and help to maintain privacy and integrity which helps end user to remain anonymous within shared public network. The existing anonymous networks like The Onion Router (Tor) achieve diverse levels of anonymity against a variety of harmful attacks.

Keywords— communication anonymity, relationship anonymity, address anonymity, pseudonymity, unlinkability.

I. Introduction

Anonymity on the internet is an interesting problem, for which several different solutions have been implemented such as Tor, Freenet, etc. Creating such a network is an interesting exercise for one thing, but using one is also highly useful to avoid various kinds of internet activity monitoring. It takes a random pathway through several servers that cover your tracks so no observer at any single point can tell where the data came from or where it's going. Communication anonymity applies end-to-end encryption which can protect transferred data from unfavourable access. An attacker can still gain the information about network traffic which results in the act of *traffic analysis*. Although data is encrypted, routing information is still open to network because routers always needs destination address to forward the incoming packet.

In addition, people trying to share sensitive information always wants to remain anonymous so as to stay clear form intended harm caused by attacker. Data communication networks use addresses to perform routing which are visible to anyone observing the network. Often addresses such as IP addresses, or Ethernet Hardware Address, are a unique identifier which appear in all communication of a user, linking of all the user’s transactions. Furthermore these persistent addresses can be linked to physical persons, seriously compromising their privacy. So as to avoid such disaster these networks also support anonymization techniques at the application layer, such as pseudonym systems [7], and Nymble [2] like systems.

The research leads to anonymous communication was initiated by Chaum in his work “untraceable electronic mail, return address, and digital pseudonyms” published in 1981 [10]. According to Jian Ren and Jie Wu [9] existing anonymous communication systems can divided into catagories like: cryptosystem-based schemes, routing-based schemes, broadcasting-based systems, and peer-to-peer communication systems.

II. TERMINOLOGY

In this section, we will discuss some aspects of anonymous communications over computer networks.

A. *Address Anonymity*

While surfing the web, the computer connects to the target server by contacting the web page with the help of user’s IP address and sharing other information like the browser and operating system version. This information can be used to track down the user. However, a certain degree of anonymity can be achieved by using a proxy server and anonymous networks like Tor [1] and Crowds [11]. The proxy server works by redirecting the communication through itself. The browser’s IP address is then only shared with the proxy server while the target website only sees the proxy server’s information. Tor makes use of Onion Routing for hiding IP address of communicating users while forwarding packets through random set of dedicated routers.

In this way both sender and receiver remains anonymous which is basic need for privacy preservation in shared public network.

B. *Unlinkability*

This is most important aspect of anonymous communications between end users which assures that two or more related events in an information processing system cannot be related to each other. In other words, a user may make multiple uses of resources or services without others being able to link these uses together. Unlinkability is considered to be a sub property of privacy.

C. *Unobservability*

Undetectability of an item of interest from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not. Unobservability of an item of interest means undetectability of the item of interest against all subjects uninvolved in it and anonymity of the subject(s) involved in the item of interest even against the other subject(s) involved in that item of interest.

Following TABLE I defines the relationship between above mentioned aspects of anonymous communications.

TABLE I

Relationships between aspects		
unobservability	→	anonymity
sender unobservability	→	sender anonymity
recipient unobservability	→	recipient anonymity
relationship unobservability	→	relationship anonymity
sender anonymity	→	relationship anonymity
recipient anonymity	→	relationship anonymity
sender unobservability	→	relationship unobservability
recipient unobservability	→	relationship unobservability
unobservability	→	undetectability

D. Pseudonymity

Pseudonymity means using a pseudonym instead of one's "real" name. Pseudonyms are typically assumed to be the same person or collective working as one entity over time. Most websites have login controls so that a registered username must be unique, and that whoever is posting under that username must know the password or have access to the email address controlling the account.

We found that users of a large anonymity network were being denied access to popular internet services as a result of the abuse made possible by strong anonymity. *Pseudonymity* allows clients to obtain and use pseudonym credentials with a minimum of effort, without even installing additional software. It allows service providers to accept these credentials with a minimum of effort.

III. CRYPTOGRAPHIC PRIMEVAL

In this section we will summarize some cryptography related terms used to provide some degree of privacy to users involved in anonymous communications.

A. Group signature

The concept of group signature was first introduced by Chaum and Heyst in 1991 [8]. Group signatures are a "generalization" of credential mechanisms and of membership authentication schemes in which a group member can convince a verifier that he belongs to a certain group, without revealing his identity, 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.

1) Correctness: Valid Signatures produced by a group member using must be accepted by a verifier.

2) *Unforgeability:* Only group members are able to sign messages on behalf of the group.

3) *Anonymity:* Given a valid signature of some message, identifying the actual signer is computationally hard for everyone but the group manager.

4) Unlinkability: Deciding whether two different valid signatures were computed by the same group member is computationally hard.

5) *Exculpability:* Neither a group member nor the group manager can sign on behalf of other group members.

6) Traceability: The group manager is always able to open a valid signature and identify the actual signer.

B. Ring signature

Ring signatures, first introduced by Rivest, Shamir, and Tauman, in 2001 [12]. These type of signatures allows a user to sign a message so that ring formed by possible signers is identified without revealing identity of member of group who generates the signature. Unlike a group signature, a ring signature scheme does not require a group manager to administrate the set of ring members.

In this scheme, coordination among users is not necessary and rings are formed in ad-hoc pattern. If we consider an e-mail, ring signatures enable the sender of an e-mail to sign the message with respect to the ring containing the sender and the receiver. The receiver is then assured that the e-mail originated from the sender but cannot prove this to any third party.

IV. ROUTING BASED SCHEMES

In this section, we will describe some routing based schemes used in anonymous communications.

A. Tor: the second-generation onion router

Tor is a free software implementation of second-generation onion routing: a system enabling its users to communicate anonymously on the Internet. Originally sponsored by the US Naval Research Laboratory, TOR became an Electronic Frontier Foundation (EFF) project in late 2004.

Onion Routing relies on using Public Key Cryptography, which allows it to encrypt layers of onions such that only intended recipients of each layer can decrypt it with their private keys. Each hop along the route then only knows about the previous hop that it received the onion from and the next hop that it was instructed to forward the onion. Plus, as the entire onion is decrypted at each router, there is no correspondence on the data layer between an onion entering a router and an onion leaving the router as shown in Fig. 1. This means that an outside observer who sees the onion for a specific message enter a node does not know which of the onions leaving that node corresponds to that same message. If an eavesdropper compromises a host in the network of onion routers, they will only be able to see where the onion came from on the last hop, and where it should be sent to on the next hop. The absolute source and destination of the onion are hidden.

We will number all the routers in the network with numbers 1 to N. Onion Router S which is an essential part of anonymous network has a public key S_u and a private key S_r with encryption and decryption function E and D respectively. The public key is well known to onion proxies. Private keys are only known to the router. Set of such routers involved in the process packet transfer is considered as Onion Cloud.

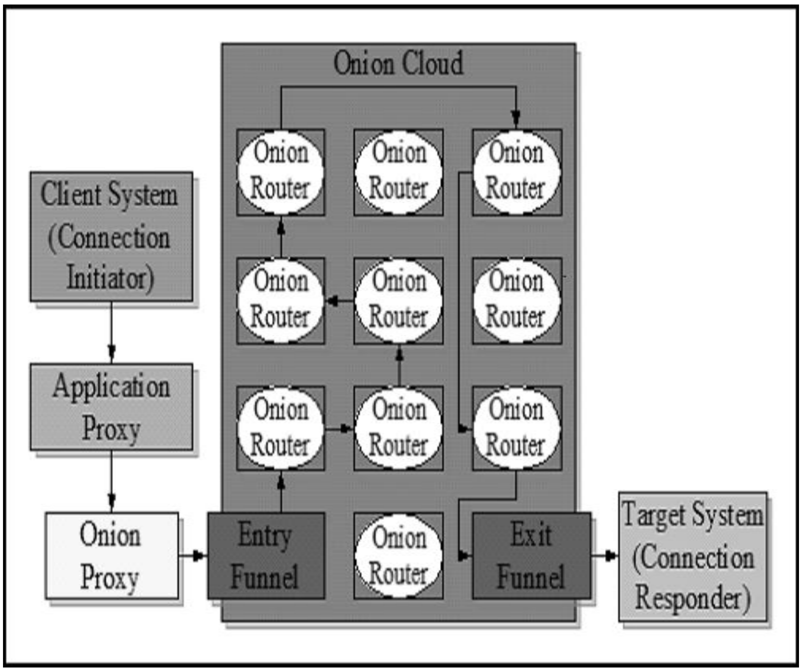

Fig. 1 Onion Routing

There also exists an encryption function *E[key](data)* and a decryption function *D[key](data)* with the property that data encrypted with a public key S_u can be decrypted with the corresponding private key *Sr*, and vice versa.

$D[S_u](E[S_r](data)) = data$ and $D[S_r](E[S_u](data)) = data$

B. Crowds

Crowds was designed by Reiter and Rubin [11] to defend against attackers in an anonymous network. It provides same anonymity mechanism provided by Tor. The main concept behind achieving anonymity is hide user's communication which are part of anonymous network. Those users kept hidden by routing them randomly within a group of similar users. Even if any group member is corrupted, it is hard for that corrupted member to identify whether the user is the actual sender, or is simply routing another user's message.

Web transaction model of Crowds includes following steps to achieve desired level of anonymity.

- The user's request to a Web server is first passed to a random member of the crowd.
- When the request is eventually submitted, it is submitted by a random member.

Hence, it prevents an attacker, or even the crowd members, from identifying its true initiator of the message, since the initiator is indistinguishable from a member that simply forwards a request from another. It makes a group of geographically diverse crowds which is a collection of nodes in anonymous networks. For initiator of each group every node act as proxy server. To achieve this functionality each node issues a request to web servers such that initiator cannot identified by attacker.

A series of nodes in crowd receives initialization message from initiator and form a path for all future messages from the initiator. If any request is arrived at a crowd member, that member decides whether the request is forwarded to another random member or to submit the request to destination server.

V. BLOCKING USERS IN ANONYMOUS NETWORKS

Anonymous networks 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".

As a result of this, 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:

A. Nymble-like Systems

Anonymous blacklisting systems are the Nymble-like systems. P. P. Tsang proposed Nymble [2] 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.

Nymbles are generated by the "Nymble Manager" based upon pseudonym and server identity. 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.

1) Pseudonym Manager (PM): 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 PM 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. PM 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).

2) *Nymble Manager* (NM): After getting the pseudonym from the pseudonym manager, the user connects to the NM 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. NM doesn't know anything about the user's identity. It knows only the pseudonym-server pair. NM encapsulates nymbles within "nymble tickets" in order to provide cryptographic protection and security properties.

This system also used in wireless sensor networks as a part of a K-Anonymity privacy preserving location monitoring system [13] 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 area 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.

B. PEREA

Blacklistable anonymous credentials (BLAC): It is a scheme for blocking misbehaving users without Trusted Third Party (TTP). 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.

This system popularly known as PEREA [4] which is a practical TTP-free revocation of repeatedly misbehaving anonymous users in an anonymous network. 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, this fact leads to misbehavior of a user. So, here to defend such type of activities in an anonymous network user have to authenticate itself to Service Providers. In Nymble system, as a part of revocation of such users TTP can take action against misbehaving users. Authentication made by TTP 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 across anonymous networks. The only drawback with the TTPs is Service Provider must have to trust TTPs which seems unfair to users like Whistleblowers etc.

VI. Conclusions

In this survey we reviewed different types of anonymous communication systems. We summarize and compare various anonymous networks types used in day today life which plays an important role in preserving privacy of end users by applying various cryptographic techniques.

We also reviewed blocking techniques for misbehaving users in anonymous networks and compare those techniques on the basis of TTP and TTP-free degree of anonymity. Research area of anonymous communications evoke many problems related to performance and efficiency of various anonymous networks. In future this area emerges with many trends of anonymity in shared public network.

References

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

[2] 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.

[3] 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.

[4] 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*, 2008, pp. 333-344.

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

[6] P. P. Tsang, M. H. Au, A. Kapadia and S. W. Smith, “Blacklistable anonymous credentials: Blocking misbehaving users without TTPs,” *Proceedings of the 14th ACM conference on Computer and communications security*, 2007, pp. 72–81.

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

[8] 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*, 2005, pp. 136-153.

[9] Jian Ren, Jie Wu, “Survey on anonymous communications in computer networks,” *Computer Communications,* vol. 33 issue 4, pp. 420-433, 2010.

[10] D. Chaum, “Untraceable electronic mail return addresses and digital pseudonyms,” *Communications of the ACM,* vol. 24 issue 2, Feb. 1981.

[11] M. Reiter, A. Rubin, “Crowds: anonymity for web transaction,” *ACM Transactions on Information and System Security (TISSEC),* vol. 1 issue 1, pp. 66-92, Nov. 1998.

[12] R. Rivest, A. Shamir, Y. Tauman, “How to leak a secret, in: Advances in Cryptology,” *ASIACRYPT, Lecture Notes in Computer Science,* vol. 2248, *Springer*, Berlin-Heidelberg, 2001.

[13] 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.