A SURVEY ON ANONYMOUS NETWORKS AND RELATED MENACES

Gayathri. S

Dept. of Computer Science and Engineering, Karunya University,
Coimbatore, Tamil Nadu – 641114, India
sgayathri033@gmail.com

Abstract

Anonymous network helps to preserve user identity for secure communication in the network. The paper depicts a survey of anonymous networks and the various forms of threats faced by these networks. The survey begins by the e-mail anonymity which is treated to be the first conception in the field of network anonymity. A diversified set of attacks inimical to the anonymous networks are illustrated.

Keywords: Anonymity, crowd, tor, hidden services, denial of service

1. Introduction

The exigent demands on privacy and security have received considerable attention along with the expeditious growth and favorable reception of the internet. The brisk expansion of usage of the internet and its high demand has paved ways to various threats. The security of the internet is now a crucial factor. Anonymity helps to camouflage user identity within the network. It is treated as a very essential factor in many applications, which includes web browsing, location based services like navigation systems, information services, tracking services, applications like social networking and E-Voting etc. Encrypting the data being transferred alone cannot provide the required amount of anonymity expected by the participants. Various types of anonymity providing networks are widely used nowadays.

2. Motivation

The motivation of this survey is to explore the anonymous networks and various kinds of threats to these networks so that the researchers can pinpoint the essential metrics for evaluating the anonymity level of networks and curtail threats against these networks.

3. Anonymous Networks

With the growth of electronic mail, the factors like anonymity of the sender, receiver and the message confidentiality have to be seriously considered. A public key cryptography technique is depicted that allows the mailing system to hide the participant details as well as the content of the communication [2]. The basic idea of anonymous communication system was introduced which was termed as mixes. By using the concept of roster of pseudonyms, anonymity is provided. It is based on two assumptions, where the first one is that, no one can determine anything about the correspondences between a set of sealed items and the corresponding set of unsealed items, or create forgeries without the appropriate random string or private key. The second assumption is that anyone may learn the origin; destination(s) and representation of all messages in the underlying telecommunication system and anyone may inject, remove, or modify messages. The advantage of the paper is that security for message passing system is achieved and the secondary party can reply to the first via an untraceable return address, which ensures anonymity. The disadvantage is that the mixes do not provide sender anonymity. The length of message routed through a mix network grows proportionally to the number of mixes through which it is routed. It also hurts the performance. The method is too expensive.

3.1. The Crowd Network

Following the anonymity the crowd network was instigated to increase the privacy of web transactions [5]. It was based on the idea of “blending into a crowd”, i.e. hiding ones action within the action of many others. The user joins the crowd and can submit the request either directly to the server or by forwarding it through randomly chosen members. These members too have the freedom to choose whether to forward the request to another member or to submit it to the server. Thus even crowd members cannot identify the initiator from a member that simply forwards the request. The Fig. 1. illustrates the path formation in the crowd network. The system also presents no single point at which a passive attack can cripple all users’ anonymity, because we don’t have a proxy which is often a single point failure. If a proxy fails then the anonymous communication cannot be continued. Thus in Crowd no single failure discontinues all ongoing web transactions. The advantage is that the systems do not present a single point where a passive attack is done. Anonymity increases as number of times the request is forwarded with less impact in performance. These networks do not require private or public key operation or decoy of messages. The crowd network makes no effort to defend against denial of service attack. It does not provide anonymity against global eavesdropper.

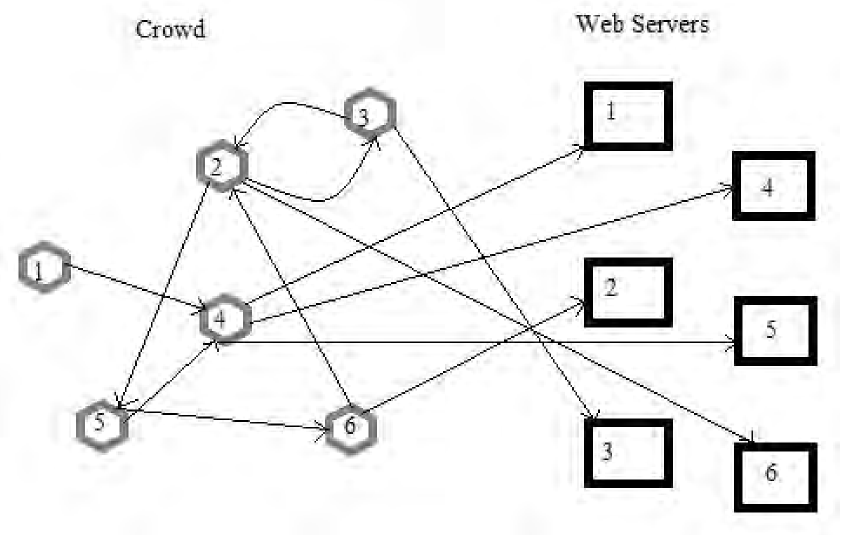

Fig. 1. The crowd path – the beginner of communication and web server of each path labelled same

3.2. *The Tor Network*

Tor is a circuit based low latency anonymous communication service [9]. This can be said as onion routing concept with added features like forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies etc. Tor uses incremental or telescoping path-building design, where the initiator negotiates session keys with each successive hop in the circuit. When initiator knows that a hop failed then it can try extending to a new node and thus continue the process. Or uses standard SOCKS proxy interface allowing users to support most TCP based programs without modifications. Several considerations like deploy ability, flexibility, simple design etc. has directed Tor's evolution. Also Tor is not completely decentralized. The advantage is that Tor interfaces allows supporting most TCP-based programs without modification. Many TCP streams can share one circuit. It also achieves Congestion Control. Rather than flooding state information throughout the network, tor maintains directory servers which provide signed directories describing known routers and their current state. Or verifies data integrity before it leaves the network. It is not secure against end to end attacks. Tor does not try to conceal who is connected to the network. The table 1a shows the summarized characteristics of the above depicted anonymous networks.

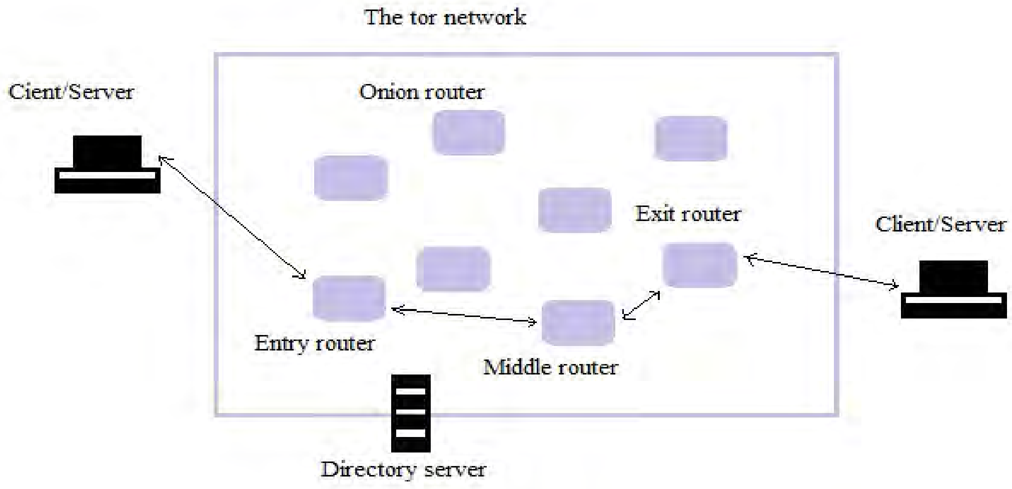

Fig. 2. The tor network

The tor network consists of a client, a server and number of onion routers. The network is depicted in Fig. 1. The application data between the client and the server is relayed using an Onion Router. The overlay link encryption between two users is done by the Transport Layer Security (TLS) connections. A short term link key is also established by the TLS when communicating between Onion Routers. To limit the impact of key compromise in the network, the link key is rotated periodically and independently. An entry router is chosen which then transfers data to the middle router and finally the exit router delivers the message.

Table 1. Features of anonymous networks studied in the survey

	Email Anonymity	Crowd Network	Tor Network
Cost of Implementation	Public Key Cryptography to hide Sender and Data.	Concept of mixes .No private/public key operation used. No decoy of messages.	Onion routing with added features. TLS protocol is used to establish links. Traffic passes along fixed sized cells of 512 bytes.
Anonymity Level	Receiver Anonymity, Data Confidentiality	Sender and Receiver Anonymity	Sender and Receiver Anonymity, Data Confidentiality
Probability of Compromising Anonymity	High chances to compromise	Less chance to compromise than email	Less chance to compromise than email and crowd
Latency	Medium	Performance degrades as the number of mixes passing data increases	Better performance than crowd.

4. Classification of existing attacks on anonymous networks

4.1. Attacks using network traffic

The identification of World Wide Web traffic using samples of web pages based on certain revealed or unconcealed information which may include HTTP object count and sizes etc. Web browsers do not hide all information about the encrypted plain text [8]. HTTP object count and sizes are often revealed. The main theme of the paper is investigating the identification of World Wide Web traffic based on unconcealed information in a large sample of web pages. The adversary may have a collection of his pages of interest. He then evaluates the similarity of a user’s traffic pattern with one of his pages of interest which can be termed as “target pages”. The comparison of traffic pattern is done and attempting to identify web pages with as low a false positive rate as possible. The advantage is that the attack proves effective for an attacker to undermine the privacy of web browsing. The countermeasures provided are of extra cost and so too expensive to implement. And it is highly dependent on traffic analysis.

The preferential routing scheme that provides low latency, high throughput performance which is suitable for interactive applications are dangerous as an attacker cam compromise the anonymity of large amount of the communication channels through the network [3]. Malicious low-resource nodes that are falsely given the illusion of high performance nodes are highly effective at compromising the end to end anonymity of the system. This method effectively attacks the mix systems.

Some form of attack modifies the user’s website by sending distinctive signal which can be found out using traffic analysis in the tor network [1]. Both the attack as well the analysis is done by an adversary. The paper also suggests methods to simplify the method of traffic analysis and the usage of Firefox extension tor button and anticipated attacks by that. The advantage is that the attack is done effectively without affecting the target communication.

The network traffic analysis attack can be mainly classified into two, one is the active traffic and the other is inactive traffic analysis [7]. It deals with active traffic analysis which records traffic and find inbound and outbound using statistics. This attack does not change traffic. The extensive research on tor shows that the size of IP packet in the tor network can be very dynamic because the cell is an application concept and the IP layer may repack the cells. As the cells can be repacked, by marginally varying the number of cells in the target at the malicious exit router the attacker embeds a secret signal into the current flow and thus infers the relationship between the users. An assumption is made that the attacker controls small percentage of exit and entry or malicious node. The attacker first selects a traffic flow and then selects sequence of binary bits with time and then updates the cell in targeted traffic with random signals. This which is carried to the client may be recognized by the embedded signal in it. If matched pattern is found the relationship between client and server is identified and thus spoils the anonymity. The attacks are very stealthy and so very hard to be found out. The anonymity can be found only for short range communication. Also the attack is very complex. The characteristics of various attacks are depicted in Table 1.

4.2. Attacks for locating Hidden Services

One of the major features of the Tor network is the hidden services provided by this network [4]. In order to offer various kinds of services tor makes it possible for users to hide their locations. The tor “Rendezvous Point” is used to connect to these types of hidden services where each one’s unaware of others network identity. The paper aims at attacking these hidden services by using a single hostile Tor node to disclose these hidden servers in a matter of minute if it is in the client node or a couple of hours if it is in the server node. The advantage is that one compromised node is more than enough to attack the tor network. The traffic and increasing path length will not affect this attack. The precise timing information is needed of when cell is received and transmitted. The cell direction is needed in its own order to determine the circuit match.

The Tor overlay network services hosting hidden services are accessible both directly and over anonymous channel [10]. Traffic pattern through one channel have observable effects on the other, thus allowing a services pseudonymous identity and IP address to be linked. In a connection the total throughput affect the load on CPU and thus its heat output. And the result of clock skew can be remotely detected through observing timestamps. The advantage is that the Clock skew changes may be remotely detected even over tens of router hops. CPU load on one communication channel may affect clock skew measured in other and thereby linking pseudonym to a real identity. The method is dependent on traffic analysis and timestamps.

4.3. Attacks based on cell

The basic principle of a protocol level attack is to conform whether the sender is communicating with receiver over the circuit [11]. An assumption is made that the attacker can compromise both exit and entry onion routers. These nodes can otherwise be termed as malicious onion routers. By manipulating a cell the attacker launches the protocol level attack. The malicious entry node can determine the source IP address port used for a given circuit. Also it knows the circuit ID as well as the time of cell manipulation. Now as in the same way the exit onion router also has details of the Destination IP address, port number and the circuit ID. Thus whenever a manipulation is done to the cell in the entry node it can be found out in the exit node, due to the cell recognition error raised by the network. Thus the anonymity of the sender and the receiver is lost and thus the Tor anonymity is highly affected. Effective steps have to be considered in order to preserve the anonymity of the tor network. An accurate modus operandi for bringing down such type of attacks against the network should be discovered and should be implemented effectively to safe guard tor network.

4.4. Denial Of Service attack

Introducing the denial of service reduces anonymity as messages are retransmitted to be delivered to the corresponding destination [6]. Thus it provides a chance for attack within the network. If the network consists of only a few honest nodes then it is subjected to denial of service attack and only fully honest or fully compromised path will survive. The impact of Dos in reducing anonymity is clearly mentioned depending on traffic analysis.

Table 2. Comparison of various attacks on the anonymous networks

Reference#	**[3]**	**[1]**	**[6]**	**[8]**	**[7]**	**[11]**
Year	2007	2007	2007	2002	2013	2013
Scalability	3 to 6 out of 60 nodes	Any Single Node	-NA-	100,000 web pages	Any single node	A single Cell
Ease of Implementation	Easy	Easy	Moderate	Easy	Complex	Easy
Level of Compromise	Sender and Receiver Anonymity	Sender Anonymity and Downloaded web page	Sender and Receiver Anonymity	Sender Anonymity	Sender and Receiver Anonymity	Sender and Receiver Anonymity
Probability of Choosing Malicious Router(s)	High	High	Moderate	-NA-	-NA-	High

Conclusion

The paper has depicted a survey on various anonymous networks and the threats faced by these networks. As the usage of anonymous network is a predominant factor in this 21st century the effort to combat threats on these networks should be seriously considered. We delineate various types of anonymity and a series of attacks that has to be seriously dealt with. Therefore the design and development of an anonymous network with low latency and robustness against threats is very essential.

References

[1] T. Abbott, K. Lai, et al. (2007) Browser Based Attacks On Tor, In Proceedings Of Pet'07 Proceedings Of The 7th International Conference On Privacy Enhancing Technologies, Isbn:3-540-75550-0 978-3-540-75550-0, Pages 184-199.

[2] D. Chaum (1981), Untraceable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM 4 (2), pages 84-88.

[3] K. Bauer, D. McCoy, et al. (2007), Low-resource routing attacks against anonymous systems, in: Proceedings of ACM Workshop on Privacy in the Electronic Society (WPES), Pages 11-20.

[4] L. Overlier, P. Syverson (2006), Locating hidden servers, in: Proceedings of the IEEE Security and Privacy Symposium (S&P), Pages 100 - 114

[5] M. Reiter, A. Rubin (1998), Crowds: anonymity for web transactions, ACM Transactions on Information and System Security 1 (1), Pages 66-92.

[6] N. Borisov, G. Danezis, et.al (2007), Denial Of Service Or Denial Of Security?, Proceedings Of The 14th Acm Conference On Computer And Communications Security , Isbn: 978-1-59593-703-2, Pages 92-102

[7] N. K. Mahendrakumar, S.Shriniwas (2013), Analysis Of Cell-Counting Based Attack Against Tor, Ijetae, Issn 2250-2459, Iso 9001:2008 Certified Journal, Volume 3, Issue 5, pages 208-212.

[8] Q. X. Sun, D.R. Simon,et al. (2002), V.N. Padmanabhan, L.L. Qiu, Statistical identification of encrypted web browsing traffic, in: Proceedings of IEEE Symposium on Security and Privacy (S&P), Page 19-31.

[9] R. Dingledine, N. Mathewson, et al. (2004), Tor: The second generation onion router, in: Proceedings of the 13th USENIX Security Symposium.

[10] S.J. Murdoch, G. Danezis (2006), Low-cost traffic analysis of tor, in: Proceedings of the IEEE Security and Privacy Symposium (S&P), Pages 183 – 195.

[11] Z. Ling, J. Luo, et al. (2013), Protocol Level Attack Against Tor, Computer Networks, The International Journal of Computer and Tele-communications Networking, Volume 57 Issue 4, Pages 869-886