Open access Journal

International journal of Emerging Trends in Science and Technology

Security to Anonymous Network

Author

Prof. Devendra Shamkuwar. Mr. Arote Nikhil S. Mr. Kamble Kailas R. Miss. Hinge Apurva R.

Deptartment of Information Technology
SharadchandraPawar College OfEnginnering, Otur (Pune)
Email: *nikhilarote07@rediffmail.com*

Abstract- In the today's world there is mainly people are concentrate on the security and privacy of the data. As there is some change in security system behavior it not as per user intension. In the network some people make unintentional expose of personal information, or relationships and other things in front of people.Technology gives us solution for these types of exposures that is encryption and decryption for data i.e. change view and appearance of data for other or unknown persons. In networking there are mainly two types of attacks Passive and Active attack.Passive i.e. only monitoring the system network and datawhich is send. But the active attack is focus about the only change in data send by client.Attackers interested in the changing of data and to get detail about the communicationhappen in the sender and receiver. In TOR, attack happen at the exit onion router.While searching basically this attack is based on active attacks. But main problem inthis type is degrading attacks and hidden services. In this attack attacker select particular IP packet at exit onion router and changes that packet. So our aim is to detectattacker and degrade anonymous services.

Keywords- Mix network, Onion routing network, Hidden services.

INTRODUCTION

A network is simply defined as something that connects things together for a specific purpose. Eventually, networked devices everywhere will provide two-way access to a vast array of resources on a global computer network through the largest network of all, the Internet. In today's businessworld a computer network is more than a collection of interconnected devices. In different areas the computer network is the resource that enables to collect and spread information that is essentialtotheprobability. The riseof intra-nets and extra-nets business networks based on Internet technology is an indication of the critical importance of computer networking to various domains.They establishedintra-nets simply to remain strong urge to win. Company network to the Internet isthe next technological transformation of the traditional business.

I. LITERATURE SURVEY

A) Basic Concept

In onion routing [9], [10] anonymous email can be traced. In network MIX nodes are there and role of that by accepting data, encrypting,decrypt by public key and transfer to all node present in network.Mix node performs certain timing change of the data packetto make it complicatedin a network analyzer or observer to checkand trace the path that emails take. In Onion Routing has two phases that way for two parties - a connection originator and responder for anonymous communication with other. Onion Routing gives protection in anticipation of trafficanalysis attacks or passive attack. Packets are kept hide from eavesdropper also initiator and responder is hide. Encryption technique is handling by using any of algorithms for sending packet.Onion routers are present they are machines available in network. There are some entry points consist, that accepts connection request from client also called entry router and some are exit routers. Such services can be WWW, electronic mail, node-to-node applications, etc. When a client application wishes to establishan anonymous connection to a server (such all proxy are firstly connected who wishes to communicate.Data is transferred to next node or router.The OR proxy design data structure an onion.Packet is passed to an entry node. When an entry node receives packet, it decrypts it, which reveals a layer containing information about the next hop in the route constructed. This packet is forwarded on to this next node. Onion packet is reaches an exit node.Decryption is held by the application proxyat the beginning of the connection establishment.Packet is forwarded to receiver. Onion Routing relies on using Public Key encryption and decryption provide it to encryptlayers of packet such that only intended recipients of each layer can decrypt it withprivate key.All nodes throughpath only know about the previous hop (that itreceived the onion from) and the next hop (that it was instructed to forward the packets).Whole packet is decrypted at each router present in the path.Means other analyzer sees the onion fora specific message enters a nodedoes not know which of the onions leaving that node corresponds to that same data.If an attacker compromises a host in the network of OR, an attacker see from which node this packet is came and to which is destination. The absolute source and destination of the onion are hidden.

B) Mix Networks And TOR Network:

Mixes get their security from the mixing done by their component mixes, andmay or may not use route that cannot be predicted to enhance security [8]. It is very difficult to detect and observe path for any packet or route from which path data is send, which for designs deployed to date has meant choosing unpredictable routes.OR (i.e. onion routers) typically no use of mixing.This gets at the fundamental nature of two even if it is a bit too quick to each side. A Mix network also intends to resist an adversarythatcanobservealltraffic everywhere.Onion routing assumes that an adversary who observesboth ends of a communication path will completely break the anonymity of its traffic.To resist local attacker OR networks are designed, one that can only see networkandthetraffic on it.

C) ExistingCell Based Attack Against TOR

Firstly discuss about components presentin network and role and which processthe cell and provide communication.

- Alice is the client called onion proxy (OP) to anonymizethe client data into TOR.
- Bob is TCP applications such as a Web service.
- Onion routers are special proxies that relay the application data between Alice and Bob. In TOR, transport-layer security (TLS) connections are used for the overlay link encryption between two onion routers. Data is encapsulates into same-sized cells (512 B) carried through TLS connections.
- Directory servershold onion router information such as public keys. Directory server authorizes hold information on onion routers and directory caches download directory information of onion.

Traffic analysis attack i.e. passive attack studied to degrade anonymity service provided in the communication.There is happened existing traffic analysis attack can be categorizedinto two groups: passive traffic analysis and active watermarking techniques. On the basis of sender's outbound traffic and receiver's inbound traffic based on statistical measures will passive traffic analysis. Based on the active watermarking technique, for example, proposed a flow-marking scheme direct sequence spread spectrum technique [3]. Attacker includes secret signal into target traffic by interfering rate of suspect sender's traffic and changing rate.By get determining relay or control cell by attacker in TOR.Suspect flushes all cells in queue and manipulates the control cell. In this way, theattacker can embed a series of 1/0 bits into the variation of the cells during a small amount of time period in the network target traffic.

D) IdeaOf Cell Base Attack

There is intends to confirm that Alice communicates with known server Bob in the rest of the paper; we assume that the attack initiates at an exit onion router. During the attack he selects traffic flow between Alice and Bob at the exit onion router.Attacker then selects a random signal chooses an exacttime, and changes the count of cell from target traffic based on the selected random signal. Due to network delay and congestion signal will be distorted while transmitted through TOR. When the chunks of three cells for encrypting bit "1" arrive at the mid onion router, if there is no data in the outputbuffer the first cell will be flushed to the output buffer. The subsequent two cells are in the circuit queue.First cell is sent to network when write event called,while the two cells are flushed into the output buffer.Therefore, the piece of the three cells for carrying bit "1" maybe split into two portions. The first portion having the first cell and the second portionhaving the second and third cell together.

Due to the network congestion and delay, attention must be paid to takethese into account to recognize a signal bit the cells may be combined or separated at the middle OR, or the network linkbetween the OR i.e. onion routers. The write event is added to the queue,and the cell waits to be written to the network by the write event. Since the interval issmall, the three cells for the second bit 1 and the cell for the third bit 0 also arrive atthe middle onion router and stay in the queue. When the write event is called, the first cell for carrying the first bit 0 will be written on network, while nextthree cells for carrying the second bit of the signal and one cell for carrying the third bitof the signal will be written to the output buffer together.After this original signal will get distort. Therefore,the attacker needs to choose the proper delay interval for transmitting cells[4], [7].

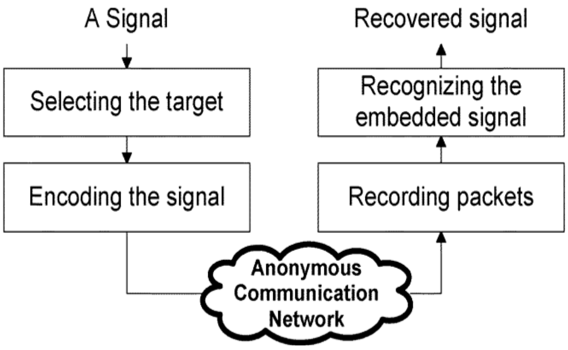


Fig 1Cell-counting-based attack.

II. SYSTEM IMPLEMENTATION

In this project, we focus on the active watermarking technique, in which as perattacker point of view that changing of data. By interfering with the rate of asuspect sender's traffic and marginally changing the traffic rate, the attacker can embed a signalinto the target traffic i.e. make changes in the packet arriving at exit router. Theembedded signal is carried along withthe target traffic from the sender to the receiver,traffic analyzer recognizes communication relationship.Tracing the messages in spite ofthe use of anonymous networks. Our motive behind this projectis to detect that particular attacker and as overall analysis it can be concluded thatfor knowing the services and communication between the users. So while at exit nodeattacker changes packet data at that time it be get detect by using IP address providedto his computer.

A) Parameters

- Sender.
- Receiver.
- OR Node.
- Attacker.
- Encryption.
- Decryption.
- Port No.
- IP Address.

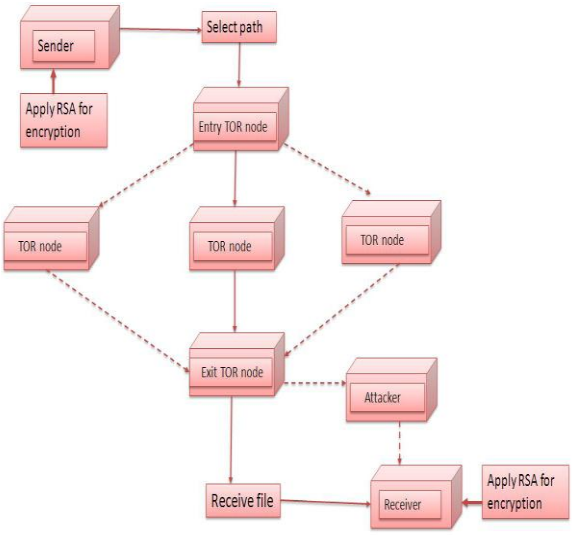


Fig.2 Block diagram of Anonymous network

A) *Algorithm Used*

RSA (which stands for Rivest, Shamir and Adleman who first publiclydescribed), an algorithm for cryptography involves three steps key generation, encryptionand decryption. RSA is a block cipher with each block having a binary value less than**some** number n. Size of block need to less than or equal to log 2 (n). Encryptionand decryption is of the following form, for some plaintext as M and cipher text as C:

$$C= M^e \ mod\ n$$
$$M= C^d \ mod\ n$$

Both sender and receiver must know the value of n. e is value known to senderand d value knows only to the receiver.This is a public-key encryptionalgorithm with a public key of PU = e, n and a private key of PR = d, n. For thisalgorithm to be satisfactory for public key encryption, the following requirements mustmeet:

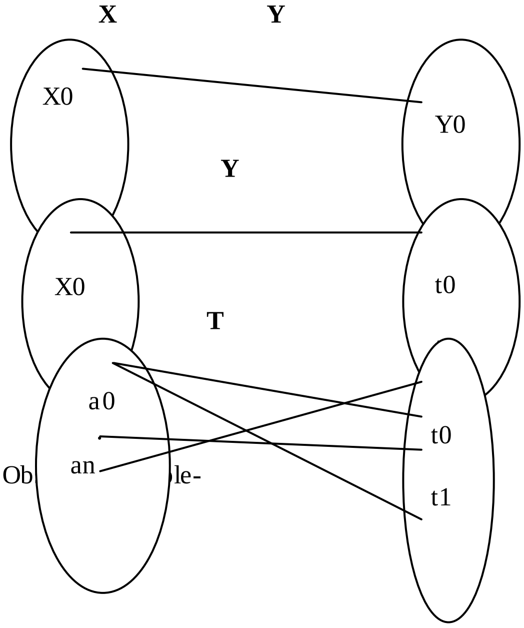
- It is possible to and values of e, d, n such that $M^{ed} = M$ mod n for all M<n.
- It is easy to calculate M^e and C^d for all values M<n.
- It is not possible to determine d given e and n.

B) Mathematical Model

Problem Description-
S =Secure communication channel.
X = Sender.
Y =Receiver.
T =Tor Node.
A =Attacker.
E =Encryption Algorithm.
D=Decryption Algorithm

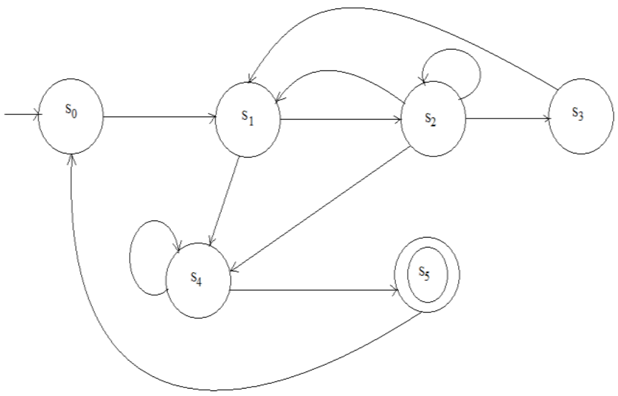
S ={X, Y, T, A, E}
X ={x_0}
Y ={y_0}
T ={t_0,t_1,t_2}
A ={a_0,…………,a_n}
E ={e_0}
D={ d_0 }

Activity-
f(x) → T
i.e. f(x_0) → {t_0,t_1,t_2} € T
f(x) → Y
i.e. f(x_0) → {y_0} € Y
f(A) → T
f (E) → X
i.e. f (e_0) → {x_0} € X
f(D) → R
i.e f(d_0) → {r_0 } € R
Venn Diagram-



	Function	f(n)	N	S(n)
Sender.	Send Data	f_0	1 Time	S_0
Tor Node.	Tor	f_1	n Time	S_1
Encryption.	Encrypt Data	f_2	1 Time	S_2
Attacker.	Attack	f_3	n Time	S_3
Decryption.	Decrypt Data	f_4	1 Time	S_4
Receiver.	Receive Data	f_5	1 Time	S_5

Finding-
Data from Sender = d1
Data from Receiver = d2
If $d_1 = d_2$ then Tor network established successfully else failure in communication.If Receiver does not receive data d_2 then connection failure.
State Diagram-



S_0 S_1 → (Sender- TOR network)
S_1 S_2 → (TOR network- Encryption)
S_2S_2 (For Multiple Files)
S_2 S_3 → (Encryption-Attacker)
S_4 S_5 → (Decryption-Receiver)
S_4S_4 (Decryption of multiple files)
S_2 S_1 → (Encryption-TOR node)
S_2 S_4 → (Encryption-Decryption)

Functional Dependency chart:-

	f_0	f_1	f_2	f_3	f_4	f_5
f_0	0	1	0	0	0	0
f_1	0	0	1	0	0	0
f_2	0	1	1	1	1	0
f_3	0	0	0	0	0	0
f_4	0	0	0	0	1	1
f_5	0	0	0	0	0	0

In TOR network while attacker get the file at exit onion router. He makes changesin that file. Attacker may attack at any point but we consider as mentioned in previous system that attacker present at exit onion route. While attacker get enters in networkcommunication and send file to receiver. For this we give solution that IP addresses ofrouter present in network are stored at receiver side while attacker is from outside ofnetwork and his IP address is not stored at receiver his IP address get matched with alladdress stored in it, if match not found then attacker get detected and acknowledgementsent to the sender that attack happen in this way we can detect attacker.

III. CONCLUSION

In this project we introduced attack on TOR which isdifficult to detect and is able to quickly and accurately confirm the anonymous communication relationship amongusers on Tor. An attacker at the malicious exit onion router slightly manipulates thetransmission of cells from a target stream and embeds a data stream and sends to receiver.At receiver we can detect the attacker and achieve goal by using IP address.

IV. REFERENCES

[1]. "Protecting Computer Network with Encryption Technique:" A Study Dr. Ka-maljit I. Lakhtaria MCA Department, Atmiya Institute of Technology and Science,Yogidham, Rajkot, Gujarat, INDIA, Vol. 4, No. 2, June, 2011.

[2]. L. verlier and P. Syverson, "Locating hidden servers", in *Proc. IEEE Sand P*, May2006, pp. 100114.

[3]. W. Yu, X. Fu, S. Graham, D. Xuan, and W. Zhao, "DSSS-based flow markingtechnique for invisible traceback," in *Proc. IEEE S and P*, May 2007, pp. 1832.

[4]. "A New Cell-Counting-Based Attack Against Tor," Volume:PP, Issue:99, *IEEE*2012.

[5]. A. Serjantov and P. Sewell, "Passive attack analysis for connectionbasedanonymitysystems," in *Proc. ESORICS*,Oct. 2003, pp. 116131.

[6]. B. N. Levine,M. K. Reiter, C.Wang, and M.Wright, "Timing attacks in low-latencyMIX systems," in *Proc. FC*, Feb. 2004, pp. 251565.

[7]. X. Fu, Z. Ling, J. Luo, W. Yu,W. Jia, and W. Zhao, "One cell is enough to break Tors anonymity," in *Proc. Black Hat DC*, Feb. 2009.

[8]. Danezis, George. "Mix-Networks with Restricted Routes".InDingledine, Roger.*Privacy Enhancing Technologies: Third International Workshop, PET 2003, Dresden, Germany, March 26-28, 2003, Revised Papers*. Vol. 3.Springer.ISBN 9783540206101.

[9]. Roger Dingledine; Nick Mathewson, Paul Syverson. "Tor: The Second-Generation Onion Router". Retrieved 26 February 2011.

[10]. R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The secondgenerationonion router,” in *Proc. 13th USENIX Security Symp*., Aug.2004, p. 21.