International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013)

A New Approach towards The Onion Router Network Using An Attack Dependent on Cell-Counting

Nakil Komal [1], Prof. Sonkar Shriniwas [2]
[1]*M.E. Computer, AVCOE, Sangamner*
[2]*Asst. Prof. Computer Dept. AVCOE, Sangamner*

***Abstract*— The onion router (TOR) may be a communication system that permits to cover our identity. Numerous software system below this classes are accessible that permits on line anonymity. It does not enable network surveillance or trafficanalysis tourge tracked however most of those code used equal size cells. during this paper we are analysing a brand new cell-counting attacks against TOR that permits us to spot anonymous communication among user. First of all we want to buy one onion router then attacker will include special signal i.e. cell counting into network traffic. We've developed this technique against TOR and experimental result shows the effectiveness of algorithms and permits detection TOR networks.**

***Keywords*— Anonymous Network, Cell-Counting Attack, Mix Network, Signal, TOR**

I. INTRODUCTION

Today within the world of high speed web most of user wants to preserve their identity privacy numerous applications are accessible in market that permits anonymous browsing over cyber web. This application will be divided into 2 major classes' high latency and low latency. High latency application includes internet browsing P to P networks [2],[6] low latency application area unit message based application e.g. email namelessness that is investigated. In this paper to scale back the performance of service network traffic attacks has been studied [7]-[14] network traffic analysis attack will be categorised into two parties inactive traffic analysis and active traffic analysis. The active traffic analysis can record traffic and notice arriving and outward-bound victimisation statistics. This attack doesn't modification traffic. during this paper we tend to working on active traffic analysis technique. In active traffic analysis technique flow creating technique is employed.

In this technique the offender embeds a symptom into current flow and currently attacker will notice the link between the users. In this paper we introduced attack against anonymity network by using cell counting attacks. It is used to quickly confirm the relationship between user is anonymity or not firstly the attacker need a malicious being transmitted to user here at this malicious onion exit router from which data is transmitted to user.

Here at this malicious onion router attacker gets information like relay cell control cell. After executing control cell attackers can get number of relay cells in circuit queue.

In this paper we tend to introduced attack against anonymity network by exploitation cell investigating attacks. It is used to quickly ensure the connection between user is anonymity or not first of all the attacker want a malicious being transmitted to user here at this malicious onion exit router from that information is transmitted to user. Here at this malicious onion router aggressor gets data like relay cell management cell. Once offender management cell attackers will get range of relay cells in circuit queue. Here the attacker will embedded signals into stream and build variation for brief amount of your time. How at entry level onion router detects excluder management cells record the quantity of relay cells in circuit queue and recovers embedded signal. The signal that aggressor have embedded in target traffic can be distorted as a result of cells having completely different bits (units) of original signal or will be separated at middle union router. We have implemented this technique in our web application and tested the feasibleness and potency of attacks against TOR. This sorts of attacks area unit extremely economical is used to realize obscurity for brief vary communication. These attacks area unit terribly economical and detection rate is 98% and short signal value-added into traffic n completely different to detect by user.

II. RELATED WORK

The communication systems with low latency, like TOR and also the Anonymizer were initially introduced by David Chaun [10]. TOR may be a second generation Onion Router [2], supporting the anonymous transport of transmission control protocol streams over the net. Since it's a coffee latency system, it's significantly appropriate for common tasks, like internet browsing, however insecure against traffic analysis attacks by a worldwide passive antagonist. Issues concerning privacy and security have received bigger attention with the ascension and public acceptance of the net that has been wont to produce our international E-economy.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013)

The attack that we tend to square measure progressing to introduce uses the active watermarking technique to actively introduce signals into the sender's departing traffic to recognise the embedded signals at the receiver's arriving traffic [13],[14].

Existing traffic analysis attacks against anonymous communication will mostly be categorized into 2 groups: passive traffic analysis and active watermarking techniques. Passive traffic analysis techniques have shown that the attacks record the traffic passively and identify the similarity between server's outgoing traffic and client's arriving traffic [8], [9]. Different recent analysis works have shown that the attackers will infer sensitive info from the encrypted network traffic by examining patterns in terms of the sizes of packet and its temporal order [1], [18],[19],[20]. For example, Liberatore and Levine [19] examined the packet sizes of hypertext transfer protocol traffic transmitted over persistent association or tunnelled via SSH port forwarding will statistically determine the Web pages. Wright et al. [20] investigated the organization of packet sizes in encrypted vocalisation informatics (VoIP) connections and known the language spoken supported the distribution in each language.

The active watermarking techniques shall insert specific secret signal (or marks) into the target traffic [10], [13], [17]. Such techniques will scale back the false positive rate significantly if the signal is long enough and doesn't need massive coaching study of traffic cross correlation PRN in passive traffic analysis. As an example, Yu et al. [13] planned a flow-marking theme supported the DSSS technique. This approach may well be employed by attackers to on the Q.T. make sure the communication relationship via combine networks. Overlier et al. [3] studied a theme victimisation one compromised combine router to spot the hidden server anonymized by Tor. Wang et al. [17] also investigated the practicableness of a timing based watermarking scheme in distinctive the encrypted peer-to-peer VoIP calls. This multiflow-based approach intends to average the speed of multiple synchronic watermarked flows and expects to look at a peculiar long silence amount while packets are not a peculiar long amount of low-rate traffic.

III. BACKGROUND

In this Section we will see the Components of Tor, Transmission and the Processing of the cell.

A) The Onion Router (TOR):

The onion router is very popular anonymity network [15]. Its open source project and provides anonymity of TCP application following components:

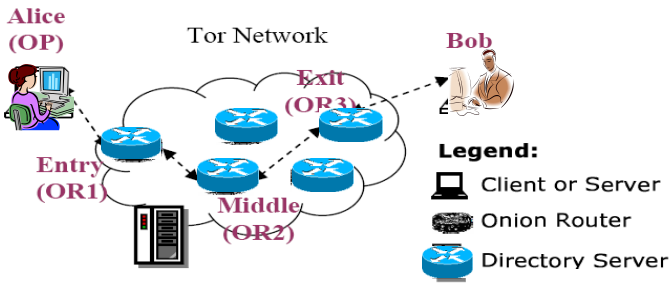


Fig 1: TOR Anonymous Network

1) Client:

Client side runs a local software, Onion Proxy (OP) to hide clients data.

2) Server:

Server runs the TCP applications.

3) Onion Routers:

These are the special routers which connects server and client. There is multiple times encrypted data that traverse in these routers.

4) Directory Server:

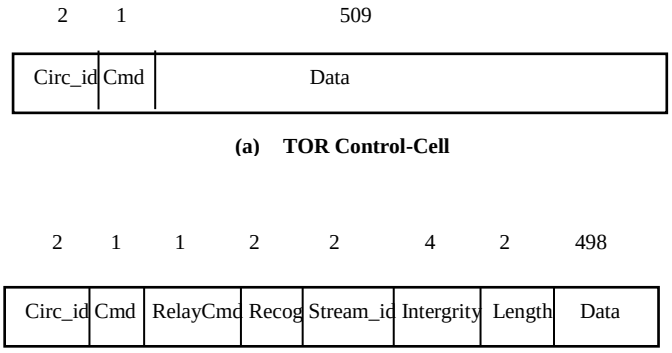
Directory server contains information of onion router as symmetric or the public keys. They are hard coded and build by using circuit network.

B) Transmission of Cells:

There are two types of cells. Fig.2 shows the control cell and relay cell formats of Tor network. Both the cells are of 512B. Tor work on transmission control protocol. Data traverse on onion router maintains transmission layer security.

TOR cells have 3B header and 509B of data. In the 512B cell the header is not encrypted in Onion like Encryption, the remaining 509B are Encrypted in the onion like fashion. There are different commands available to operate these cells.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013)



(a) TOR Control-Cell

(b) TOR Relay-Cell Format

Fig 2: Cell Format by TOR

D) Onion Routers Processing:

All onion routers receive data from port. When data is received, it is forwarded to Translation Look Aside TLS protocols and TLS buffer. In TLS buffer read operation is performed to get data. Each connection of onion router is implemented using linked list. Each data fetched is attached to the tail of list. At earlier stages cell size is 512B so data will be pulled out till input buffer contains data smaller than size of 512B. Since each router contains map of source and destination with circuit ID so that allow transmission of data. Then respective symmetric key is used to encrypt & decrypt the transmission.

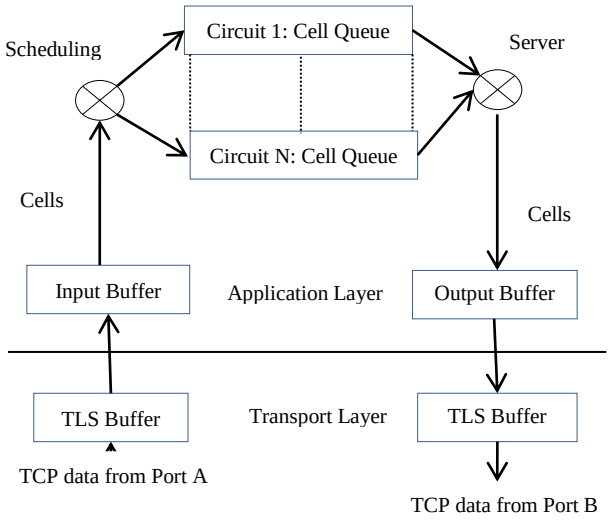


Fig 3: Cell Processing at the Onion Router

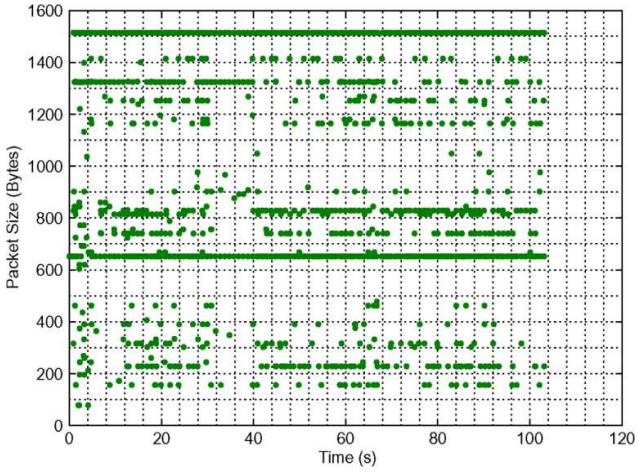


Fig 4: Packet sequence Vs. Packet Size

IV. TOR AND THE CELL-COUNTING ATTACKS AGAINST IT

As the size of IP packets is dynamic so based on some construction we need to initiate attack on streams.[1]

A) Changing IP packet size:

For application data packets are of size 512B Fig 4 shows the size of IP packets received over time period and fig. 5 shows frequency of IP packet size.

B) Core Part:

We assume that the attacker management little share of exit and entry or by malicious or this we tend to taken from alternative paper [3],[4],[5],[10] as example we will get amazon Ec2VM and deploy them on TOR. an attacker is at exit or first selects traffic flow between client and server. Now attacker then selects sequence of binary bits with time and updates cell in targeted traffic looking on random signal this updated packets are carried to client through or entry or record variation of received cells and acknowledge embedded signal. If a number of matched pattern found, we will make sure relationship in client and server for delineate illustration follow Fig.4 now we will discuss every step in additional details.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013)

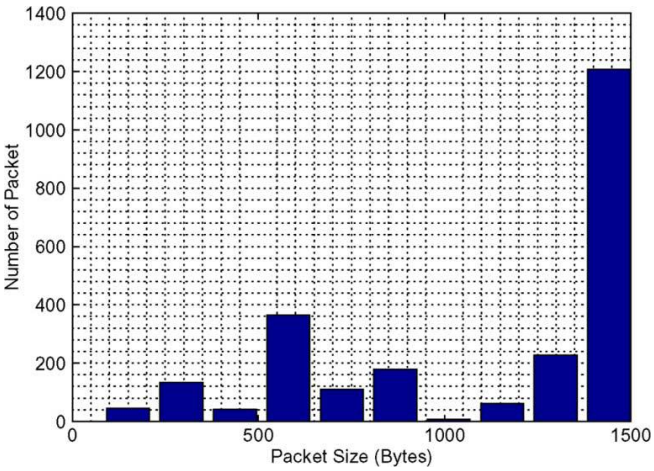


Fig 5: Number of packets versus packet size

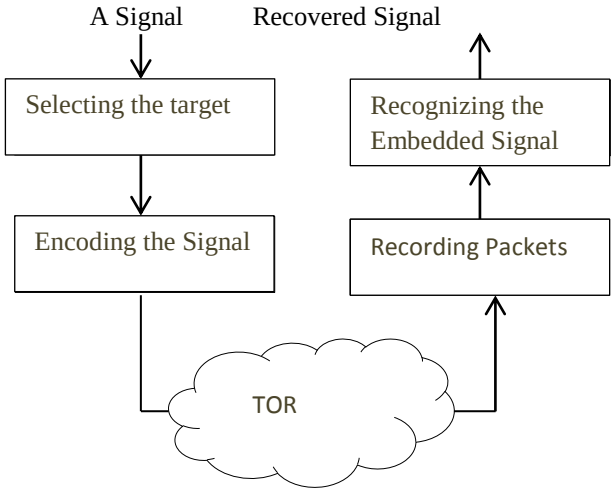


Fig 6: Cell-Counting based attack

1) Selection of the Target:

Log of all data if maintained by attacker at malicious onion router it conjointly embody information science of server with circuit ID. Here at malicious OR for information assortment we are able to use relay information in data stream.

2) Encoding of the Signal:

Here we used onion router process. We tend to use relay information that's out there in connection queue which is able to be flushed in output buffer. Here the attacker will send his own bits i.e. "10101" briefly amount of your time. The attacker counts variety of cells in circuit queue, attacker calls circuit write and every one cells flushed to output buffer instantly.

For secret writing 2 cells encoding "1" bit not enough attributable to variety of cells engraft the key signal into the variation of cell count briefly time. The attacker have a pair of cells to encrypt for bit "1" and can be simply lost are laborious to recover then. once 2 cells out there at input buffer in between OR initial cell is force out and queue are empty, and as input buffer is empty cells out there are flushed output buffer. Here second can keep in queue and once arrive are out there 1st cell is unavailable is flushed to network thence attacker can see two totally different cells returning in to resolve this issue attacker ought to select a minimum of three cells for carrying bit "1". If middle Onion Router splits them into one cell and 2 cells attacker will still acknowledge pattern.

3) Recording of the Streams:

In step a pair of output buffer can flush cell to network and at last can reach to Entry Onion Router can record the received cells. It'll conjointly embody attacker accessorial signals, Server information science and port with circuit ID. Here signals embedded in relay information entry Onion Router must verify whether they are cell relay information. This will be done same as step-4. From here attacker starts to record cells inbound in circuit queue.

4) Finding the Embedded Signal:

With embedded signal cells travels on the network to client. So as to acknowledge attacker used recovery mechanism as following to decipher the signals. Arrived cells combination will be categorized into four sorts.

Let C = $\{C_0,C_1,\ldots,C_i,\ldots,C_{m-1}\}$be the cell numbers recorded in the circuit queue at the entry onion router, C_i (i € [0,m-1]) is the number of the cells, which is a positive integer. The original signal is denoted as S = $\{S_0,S_1,\ldots,S_j,\ldots S_{n-1}\}$. Let S_j be the j^{th} signal bit, S_j' as the part of the j^{th} signal bit, and let S_x be the integral signal bits or a remaining signal bit in the packet or a null signal bit.[1]

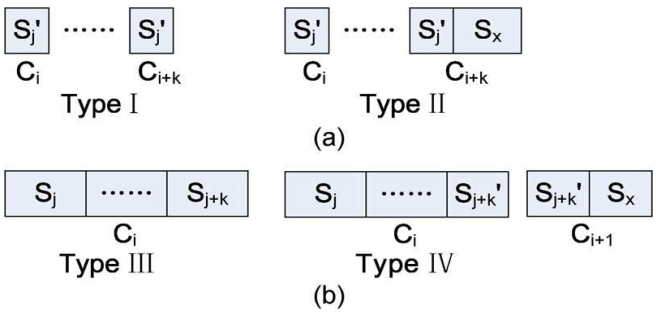


Fig 7: Signal division and combination.

(a) Types I and II. (b) Types III and IV.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013)

V. ALGORITHMS TOBE USED

The signal recovery mechanism with continuously embedded bits at a malicious Tor entry node is given by Algorithm1 and the Recovery Mechanism is given by Algorithm2.[1]

Algorithm 1 : Recovery Mechanism for Continuously Embedded Bits.

Require:

- C[1*m], an array to store cell counter variation in the circuit queue at the entry router.
- S[1*n], an array storing the original signal bit.

1: i = 0; j = 0
2: while i ≤ m do
3: if C[i] = = S[j] then
4: Signal S[j] is matched.
5: else if C[i] < S[j] then
6: Signal S[j] is spitted.
7: If C[i] +c[i +1] = = S[j] then
8: Signal S[j] is processed as Type I with k = 1
9: else if C[i] + C[i + 1] > S[j] then
10: Signal S[j] and S[j + 1] are processed s Type II with k = 1.
11: else if C[i] + C[i + 1] < S[j] then
12: Find the value of k
13: if C[i]+....+C[i + k] = = S[j] then
14: Signal S[j] is processed as Type I with k ≥ 2.
15: else
16: Signal S[j] and S[j + 1] is processed as Type II with k ≥ 2.
17: end if
18: I = I + k;
19: end if
20: else if C[i] > S[j] then
21: Two or more signals combined together.
22: if C[i] == S[j] + S[j+1] then
23: Signal S[j] and S[j+1] are processed as Type IV with k = 1
24: else if C[i] < S[j] + S[j+1] then
25: Signal S[j] and S[j+1] are processed as Type IV with k = 1
26: else if C[i] > S[j] + S[j+1] then
27: Find the value of k
28: if C[i] == S[j] + … + S[j+k] then
29: These combined signals are processed as Type III with k >= 2
30: else
31: These combined signals are processed as Type IV with k >= 2
32: end if
33: j = j + k
34: end if
35: end if
36: i = i + 1; j = j + 1
37: end while

Algorithm 2 : Recovery Mechanism for hoping based Encoding.

Require:

- C[1*m], an array to sorting the number of cell counter variation in the circuit queue at the entry router.
- S[1*n], an array storing the original signal bit.
- Q[1*n],an array storing the number of nonwatermark cells.

1: i = 0; j = 0
2: while i ≤ m do
3: Remove the nonwatermark packets Q[j] from C[i]
4: while Q[j] > C[i] do
5: C[i+1] = C[i+1] + C[i]
6: End while
7: If Q[i] == C[i] then
8: i = i+1; Q[j] is removed.
9: Detect S[j] with C[i] by using Algorithm 1
10: Else if Q[j] < C[i] then
11: The signal S[j] is combined with Q[j]
12: C[i] = C[i] – Q[j]
13: Detect S[j] with C[i] by using Algorithm 1
14: end if
15: i = i+1; j = j + 1
16: end while

VI. MATHEMATICAL MODEL

1. Problem Description:

Let S be the system that uses Cell-counting to validate the anonymity of TOR network using embedded signals such that S= {I, F, O}

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013)

Where,

'I' represents the set of inputs;
I = {I1, I2}
I1= Encrypted cells
I2= Embedded Signals

And F is the set of functions;

F= {F1, F2, F3, F4}
F1=Path Selection.
F2=Send Encrypted Cells.
F3=Receive Cells.
F4=Analyse the Traffic.

And O is the set of outputs;

O= {O}
O = Anonymity Validation.

2. Venn Diagram:

S is a system having functions F1, F2, F3, and F4.

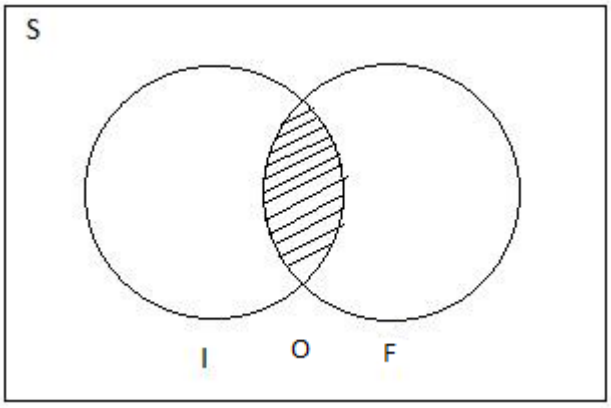


Fig 8: Venn Diagram

3. Set Diagram:

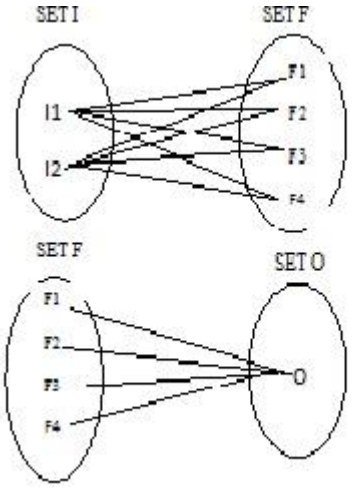


Fig 9: Set Diagram

VII. Additional Work

In our project we are supposed to send a file which will be divided into not only 512B but also in 256B and the 1024B. After login, IP will be asked to user then user will be asked to select one of the cell sizes. Every time a file is transferred a different path will be choose. For eg.

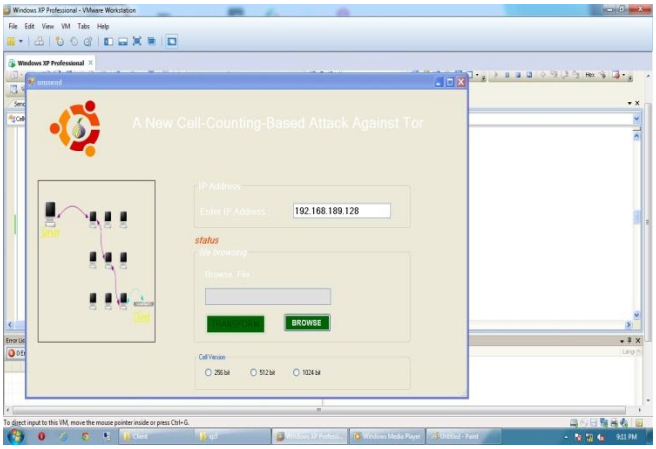


Fig 10: screen shot for selection of different cell-sizes.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013)

Fig 11: Screen shot for selection of cell-size and transformation of file.

VIII. Dynamic Programming Approach

We have divided the system into three modules as:

1. Data Transmission.
2. Components of TOR.
3. Cells at Onion Routers.

1. Data Transmission

In Tor, Associate in Nursing maintains an association to alternative on demand. The uses how of supply routing and chooses many from the domestically cached directory, downloaded from the directory caches. The quantity of the chosen is referred because the path length. We tend to use the default path length of 3 as Associate in nursing example. The iteratively establishes circuits across the Tor network and negotiates a isosceles key with every, one hop at a time, also as handles the streams from shopper applications. The facet of the circuit connects to the requested destinations and relays the information. We have a tendency to currently illustrate the procedure that establishes a circuit and downloads a file from the server.

2. Components of Tor

Onion routers are special proxies that relay the applying knowledge. In Tor, transport-layer security connections are used for the overlay link cryptography between 2 onion routers. The applying data is packed into equal-sized cells. They hold onion router data like public keys for onion routers. Directory authorities hold authoritative data on onion routers, and directory caches transfer directory data of onion routers from authorities.

3. Cells at Onion Routers

To begin with, the onion router receives the info from the affiliation on the given port A. Once the info is processed by protocols, the info are going to be delivered into the buffer of the affiliation. Once there‘s unfinished knowledge within the buffer, the scan event of this affiliation are going to be known as to scan and method the info. The affiliation scan event can pull the info from the buffer into the affiliation input buffer. Every affiliation input buffer is enforced as a coupled list with little chunks. The info is fetched from the top of the list and additional to the tail. Once the info within the TLS buffer is force into the affiliation input buffer, the affiliation scan event can method the cells from the affiliation input buffer one by one.

IX. Conclusion

In this paper we tend to introduced cell-counting analysis attack against connection primarily based TOR. This attack is difficult to observe and may quickly ensure the anonymity relationship among client and server. an attacker with malicious onion router can slightly modify target stream with protocol signal. Recovery algorithms used to recover bits at entry level onion router with show anonymity relationship among users. Our experiment shows these attacks are going to be complicated and difficult task. We'll keep those things for future analysis.

REFERENCES

[1] Zhen Ling, JunzhouLuo, Wei Yu, Xinwen Fu, Dong Xuan, and WeijiaJia, “A New Cell-Counting-Based Attack Against Tor” in Proc. IEEE/ACMansactions on networking. 2011,1063-6692

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

[3] L. Øverlier and P. Syverson, “Locating hidden servers,” in Proc. IEEE S&P, May 2006, pp. 100–114.

[4] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, “Lowresource routing attacks against anonymous systems,” Univ. Colorado Boulder, Boulder, CO, Tech. Rep., Aug. 2007.

[5] X. Fu, Z. Ling, J. Luo, W. Yu,W. Jia, and W. Zhao, “One cell is enough to break Tor’s anonymity,” in Proc. Black Hat DC, Feb. 2009 [Online]. Available: http://www.blackhat.com/presentations/bh-dc 09/Fu/BlackHat-DC-09-Fu-Break-Tors-Anonymity.pdf

[6] “Anonymizer, Inc.,” 2009 [Online]. Available: http://www.anonymizer.com/

[7] A. Serjantov and P. Sewell, “Passive attack analysis for connectionbased anonymity systems,” in Proc. ESORICS,Oct. 2003, pp. 116–131.

[8] B. N. Levine,M. K. Reiter, C.Wang, andM. Wright, “Timing attacks in low-latency MIX systems,” in Proc. FC, Feb. 2004, pp. 251–565.

[9] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "On flow correlation attacks and countermeasures in Mix networks," in Proc. PET,May 2004, pp. 735–742.

[10] S. J. Murdoch and G. Danezis, "Low-cost traffic analysis of Tor," in Proc. IEEE S&P, May 2006, pp. 183–195.

[11] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, "Lowresource routing attacks against anonymous systems," in Proc. ACM WPES, Oct. 2007, pp. 11–20.

[12] X.Wang, S. Chen, and S. Jajodia, "Network flow watermarking attack on low-latency anonymous communication systems," in Proc. IEEE S&P, May 2007, pp. 116–130.

[13] W. Yu, X. Fu, S. Graham, D. Xuan, and W. Zhao, "DSSS-based flow marking technique for invisible traceback," in Proc. IEEE S&P, May 2007, pp. 18–32.

[14] N. B. Amir Houmansadr and N. Kiyavash, "RAINBOW: A robust and invisible non-blind watermark for network flows," inProc. 16th NDSS, Feb. 2009, pp. 1-13.

[15] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: Anonymity online,"2008 [Online]. Available: http://tor.eff.org/index.html.en.