INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING

ISSN: 2320-1363

A Novel Cell Counting Based Attack Against Tor Network

Rizwan Aquib Khan*1, Akheel Mohammed*2, Dr. Vasumathi*3

Abstract

The Onion Router (TOR) allows to hide your identity various software under this categories are available that allows online anonymity. Via extensive experiments on Tor, we found that the size of IP packets in the Tor network can be very dynamic because a cell is an application concept and the IP layer may repack cells. It doesn't allow network surveillance or traffic analysis to get tracked but most of these software used equal size cells (512B). In order to hide the communication of users most of the anonymity systems pack the application data into equal sized cells. Based on this finding we investigate a new cell counting based attack against Tor which allows the attacker to confirm anonymous communication relationship among users very quickly.

Keywords: Anonymous network, Cell-counting, attack, TOR.

1. Introduction

Today in the world of high speed internet most of users wants to preserve their identity and privacy so many applications are available in market that allows anonyms browsing over the net. This application can be dived into two major categories high latency and low latency. High latency application includes web browsing P to P networks. Low latency application are message based application e.g. email anonymity which is invested in this paper to reduce the overall performance of service network traffic attacks has been studied network traffic analysis attack can be categorized into two parties inactive traffic analysis and active traffic analysis in active traffic analysis will record traffic and find inbound and outbound using statistics. This attack does not change traffic. In this article we are working on active traffic analysis technique. In active traffic analysis technique the attacker embeds a signal into current floe and now attacker can find the relationship between the users. We show a new cell counting based attack against Tor which allows the attacker to confirm anonymous communication relationship among users very quickly. In this attack by marginally varying the number of cells in the target traffic at the malicious exit onion router the attacker can embed a secret signal into the variation of cell counter of the target traffic.

Here the attacker can embedded signal into stream and make variation for short period of time. How at entry level onion router detects and excluder control cells record the number of relay cells in circuit queue and recovers embedded signal. We have implemented this system in our internet application and tested the feasibility and efficiency of attacks against TOR. This type of attackers are highly efficient can be used to find anonymity for short range communication. These attacks are very efficient and detection rate is 98% and short signal added into traffic "n" different to detect by user.

2. Related Work

A) The Onion Router (TOR):

The onion router is very popular anonymity network. It is open source project and provides anonymity of TCP application following components. The basic idea of this overlay network is to construct a circuit, which consists of onion routers (OR) that know only its predecessor and successor. Users use circuit to pass data through the TOR network anonymously. Data is wrapped in layers using symmetric cryptography and in each onion router as the data goes through a layer is unwrapped by using a symmetric key and relayed forward. At the end of the circuit onion router relays data to the intended destination.

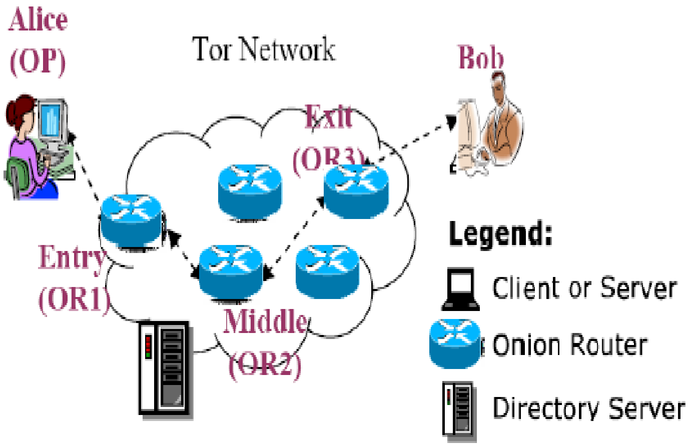


Fig 2.1 **TOR Network.**

i) Client

Here one local software i.e. onion proxy is working for hiding client data.

ISSN: 2320-1363

ii) Server

Here normally TCP applications are running.

iii) Online Routers

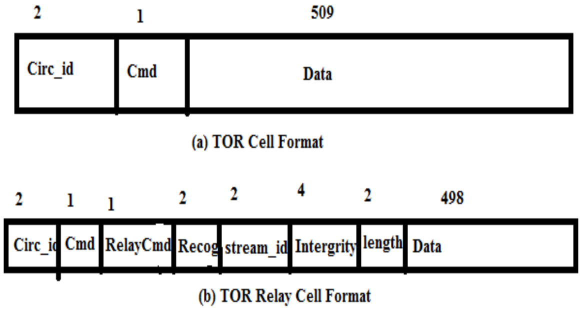
These are the special routers which allow connectivity between server and client. There is highly encrypted data that traverse in these routers.

iv) Directory Server

Directory server contains information of onion router as symmetric keys. It is authorized to handle all information. They are hard coded and build by using circuit network.

B) Transmission

Tor work on transmission control protocol. Data traverse on onion router maintain transmission layer security.



(a) TOR Cell Format

(b) TOR Relay Cell Format

Fig 2.2 Cell Format by TOR

C) Onion Routers Processing:

All onion routers receive data from selective port. After receiving data, data is forwarded to TLS protocols and TSL 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 stage 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 which circuit ID so that allows transmission of data. The respective symmetric key is used to encrypt and decrypt the transmission.

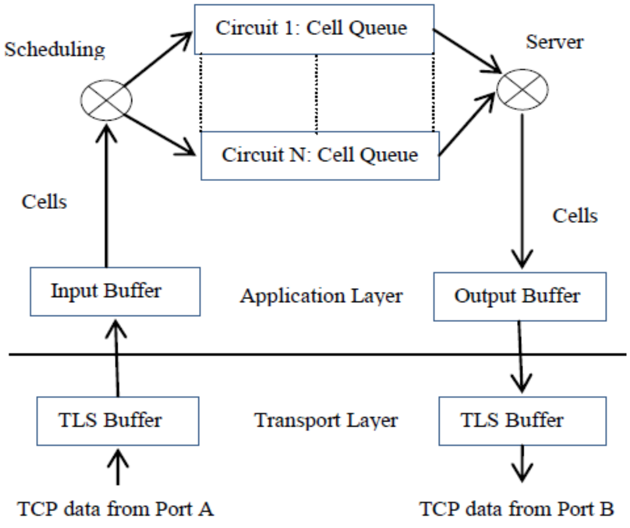


Fig.2.3. Cell processing at the Onion Router.

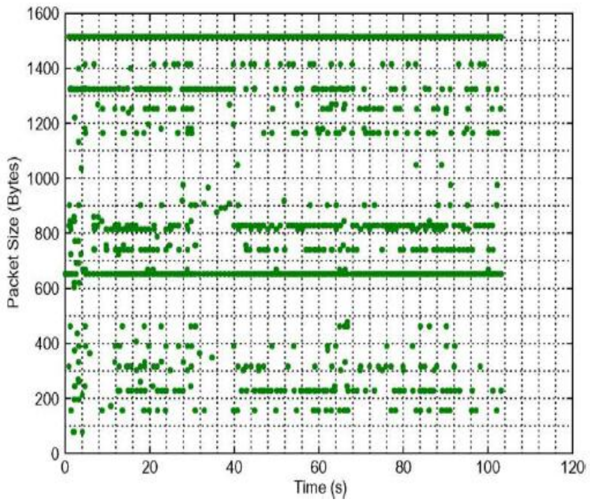


Fig.2 .4 packet sequence vs. packet size

3. Related Work

1. **Cell Counting Attacks Against Connection based TOR**

The size of IP packets is dynamic so based on some construction we need to initiate on streams.

i) Changing IP packet size

The application data packets are of size 512B in Fig.2.4 shows the size of IP packets received over time period.

ISSN: 2320-1363

ii) Core part

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 updated cell in targeted traffic depending on random signal these update packets will be carried to client through or entry or record variation of received cells and recognize embedded signal.

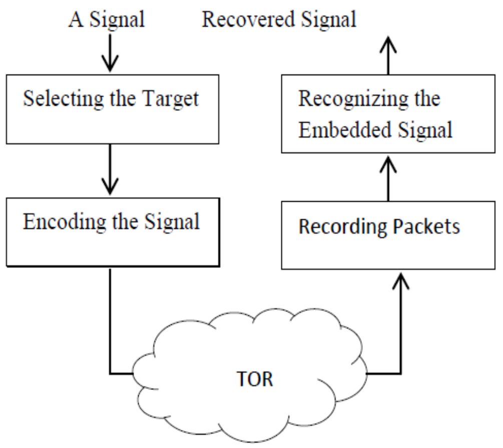


Fig.3. 1 Cell Counting based attack

a) Selecting Target

Log of all information if maintained by attacker at malicious onion router it also include IP of server with circuit ID. Here at malicious or for data collection we can use relay data in data stream.

a) Encoding signal

The relay data that is available in connection queue which will be flushed in output buffer. The attacker can send his own bits i.e. ‘10101’ in short period of time. The attacker counts number of cells in circuit queue, attacker’s calls circuit writes and all cells flushed to output buffer instantly. For two cells encoding ‘1’ bit not enough because if number if cells embed the secret signal into the variation of cell counts in short time. The attackers have two cells to encode for bit ‘1’ and will be Easley lost will be hard to recover then, when two cells available at input buffer in between OR first cell is pulled out and queue will be empty and as input buffer is empty cell available will be flushed output buffer.

b) Finding Embedded Signal

With embedded signal cells travels among the network to client. In order to recognize attacker used recovery mechanism as following to decode the signals. Arrived cells combination can be categorized into four types. 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 positive integer. The original signal is denoted as $S=\{S_0,S_1\ldots S_j\ldots S_{n-1}\}$

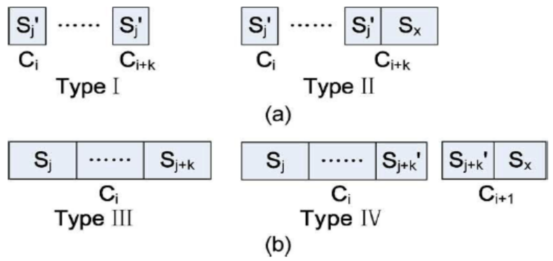
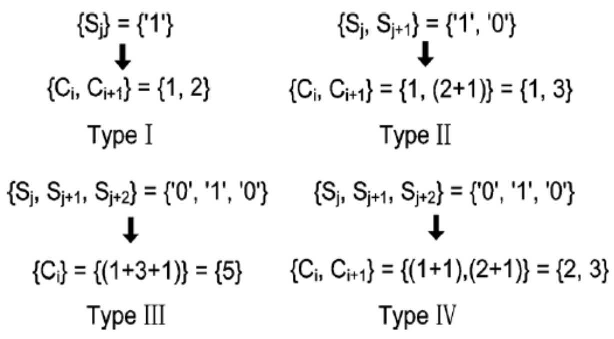


Fig. signal division and combination.

```
%%%%%%%%%%%%%%%%%%%%
Algorithm 1: Recovery Mechanism for Continuously
Embedded Bits.
%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%
i = 0; j = 0
 while i <= m do
   if C[i] = = S[j] then
 Signal S[j] is matched.
 else if C[i] < S[j] then
Signal S[j] is spitted.
 If C[i] +c[i +1] = = S[j] then
 Signal S[j] is processed as Type I with k = 1
 else if C[i] + C[i + 1] > S[j] then
 Signal S[j] and S[j + 1] are processed s Type
 with k = 1.
 else if C[i] + C[i + 1] < S[j] then
 Find the value of k
 if C[i]+....+C[i + k] = = S[j] then
Signal S[j] is processed as Type I with k>=2.
 else
 Signal S[j] and S[j + 1] is processed as Type II
with k >= 2.
 end if
 I = I + k;
 end if
 else if C[i] > S[j] then
 Two or more signals combined together.
 if C[i] == S[j] + S[j+1] then
 Signal S[j] and S[j+1] are processed as Type IV
with k = 1
 else if C[i] < S[j] + S[j+1] then
 Signal S[j] and S[j+1] are processed as Type IV
with k = 1
 else if C[i] > S[j] + S[j+1] then
 Find the value of k
 if C[i] == S[j] + … + S[j+k] then
 These combined signals are processed as Type
 with k >= 2
 else
 These combined signals are processed as Type
 with k >= 2
 end if
 j = j + k
 end if
 end if
 i = i + 1; j = j + 1
 end while
```

ISSN: 2320-1363

Type-I indicates that the original signal is divided into separate cells with K=1.


{Sj} = {'1'}
{Ci, Ci+1} = {1, 2}
Type I
{Sj, Sj+1} = {'1', '0'}
{Ci, Ci+1} = {1, (2+1)} = {1, 3}
Type II
{Sj, Sj+1, Sj+2} = {'0', '1', '0'}
{Ci} = {(1+3+1)} = {5}
Type III
{Sj, Sj+1, Sj+2} = {'0', '1', '0'}
{Ci, Ci+1} = {(1+1),(2+1)} = {2, 3}
Type IV

Suppose signal S_j is bit '1' the number of cells should be 3, as onion router records C_i is 1 and C_{i+1} is 2, will create 3 cells.

Type-II indicates last part of S_j is merged with S_x with K=1.

Type-III indicated k original signals are merged into signal packet. To deal with these types, we propose algorithm 1 for recovery mechanism. Once original signal are identified entry point onion router carry information of server client IP with port of TCP stream.

Conclusion

In this article we introduced cell counting analysis attack against connection based TOR. This attack is very hard to detect and can quickly confirm the anonymity relationship among client and server. An accomplice of the attacker at the entry onion router recognizes the embedded signal using our developed recovery algorithms and links the communication relationship among users. An attacker with malicious onion router will slightly modify target stream with TCP signal. The recovery algorithm used to recover bits at entry level onion router with show this attack will be complex and challenging task. We will keep those things for future research.

References

[1] Zhen Ling, Junzhou Luo, Wei Yu, Xinwen Fu, Dong Xuan, and Weijia Jia, ―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.