International Journal of Communication Networks and Security

Volume 2 | Issue 1 Article 12

January 2013

ATTACK AGAINST ANONYMITY USING CELL COUNTING

S. D. HABEEBUNNISA
QCET, Nellore,India, HABEEBUNNISA@gmail.com

S. K. KARIMULLAH
QCET, Nellore,India, KARIMULLAH@gmail.com

P. BABU
QCET, Nellore,India, P.BABU@gmail.com

Recommended Citation
HABEEBUNNISA, S. D.; KARIMULLAH, S. K.; and BABU, P. (2013) "ATTACK AGAINST ANONYMITY USING CELL COUNTING," *International Journal of Communication Networks and Security*: Vol. 2 : Iss. 1 , Article 12.
DOI: 10.47893/IJCNS.2013.1069
Available at: https://www.interscience.in/ijcns/vol2/iss1/12

ATTACK AGAINST ANONYMITY USING CELL COUNTING

S. D. HABEEBUNNISA[1], S. K. KARIMULLAH[2], P.BABU[3]

[1]PG Student, [2]Assistent Professor, [3]Associate Professor, QCET, Nellor

Abstract- Various low-latency anonymous communication systems such as Tor and Anonymizer have been designed to provide anonymity service for users. In order to hide the communication of users, most of the anonymity systems pack the application data into equal-sized cells. 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. 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. 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. The embedded signal will be carried along with the target traffic and arrive at the malicious entry onion router. Then, an accomplice of the attacker at themalicious entry onion router will detect the embedded signal based on the received cells and confirm the communication relationship among users. We have implemented this attack against Tor, and our experimental data validate its feasibility and effectiveness. There are several unique features of this attack. First, this attack is highly efficient and can confirm very short communication sessions with only tens of cells. Second, this attack is effective, and its detection rate approaches 100% with a very low false positive rate. Third, it is possible to implement the attack in a way that appears to be very difficult for honest participants to detect.

EXISTING SYSTEM:

Most existing approaches are based on traffic analysis. Passive traffic analysis technique will record the traffic passively and identify the correlation between sender's outbound traffic and receiver's inbound traffic based on statistical measures. This type of technique requires a relatively long period of traffic observation for a reasonable detection rate. The idea is to actively introduce special signals into the sender's outbound traffic with the intention of recognizing the embedded signal at the receiver's inbound traffic.Encryption does not work, since packet headers still reveal a great deal about users.

Disadvantage:

- Encryption does not work, since packet headers still reveal a great deal about users.

PROPOSED SYSTEM:

In this project, we focus on the active watermarking technique, which has been active in the past few years. proposed a flow-marking scheme based on the direct sequence spread spectrum technique by utilizing a pseudo-noise code. By interfering with the rate of a suspect sender's traffic and marginally changing the traffic rate, the attacker can embed a secret spread-spectrum signal into the target traffic. The embedded signal is carried along with thetarget traffic from the sender to the receiver, so the investigator can recognize the corresponding communication relationship, tracing the messages despite the use of anonymous networks. However, in order to accurately confirm the anonymous communication relationship of users, the flow-marking scheme needs to embed a signal modulated by a relatively long length of PN code, and also the signal is embedded into the traffic flow rate variation. Houmansadret al. proposed a nonblind network flow watermarking scheme called RAINBOW for stepping stone detection.

Advantage:

- Active watermarking technique can reduce attack lasting time.
- Improve attack success rate and has recently received more attention.

IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

MODULES:

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

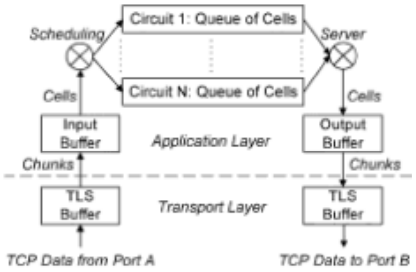
Data Transmission:

In Tor, a maintains a connection to other on demand. The uses a way of source routing and chooses several from the locally cached directory, downloaded from the directory caches. The number of the selected is referred as the path length. We use the default path length of three as an example. The iteratively

establishes circuits across the Tor network and negotiates a symmetric key with each, one hop at a time, as well as handles the streams from client applications. The side of the circuit connects to the requested destinations and relays the data. We now illustrate the procedure that theestablishes a circuit and downloads a file from the server.

Components of Tor:
Onion routers are special proxies that relay the application data. In Tor, transport-layer security connections are used for the overlay link encryption between two onion routers. The application data is packed into equal-sized cells.They hold onion router information such as public keys for onion routers. Directory authorities hold authoritative information on onion routers, and directory caches download directory information of onion routers from authorities.

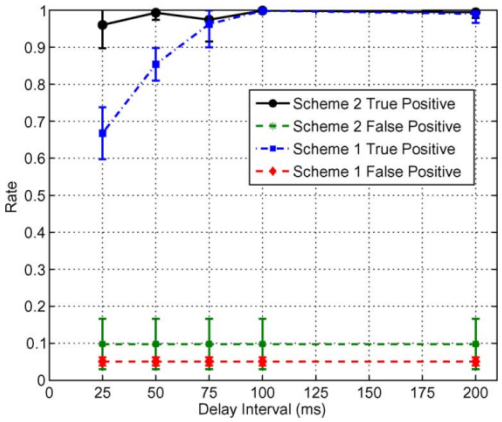
Cells at Onion Routers:
To begin with, the onion router receives the data from the connection on the given port A. After the data is processed by protocols, the data will be delivered into the buffer of the connection. When there is pending data in the buffer, the read event of this connection will be called to read and process the data. The connection read event will pull the data from the buffer into the connection input buffer. Each connection input buffer is implemented as a linked list with small chunks. The data is fetched from the head of the list and added to the tail. After the data in the TLS buffer is pulled into the connection input buffer, the connection read event will process the cells from the connection input buffer one by one.



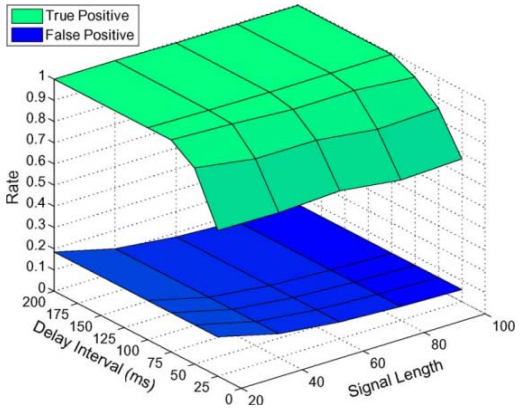
3. Processing the cells at onion routers.

EXPERIMENTAL RESULTS

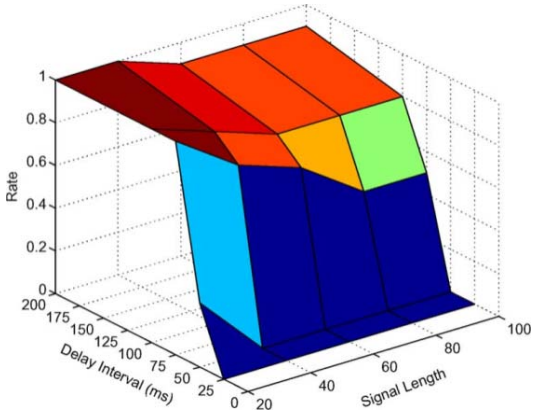
To obtain the empirical property of IP packet size for the traffic within the Tor network, we downloaded a file with the size of20M using the Tornetwork. Fig.15shows the empirical cumulative probability function (CDF) of the IP packet size in the traffic. As shown in Fig. 5, we know that the packets with non-MTU size are around 50%. This validates that the size of packets transmitted over the Tor is dynamic. Consequently, it also indicates that our embedded signal will be hidden in the normal traffic and hard to be detected by victims. Tovalidatetheaccuracyofthecell-counting-basedattack,we let the client download 30 files in our experiments. The size of each file is around 10 MB. At the exit onion router, we generate a random signal with 100 b. When the target traffic from server Bobarrivesattheexitonionrouter,wevarythenumberofcells in the circuit and embed the signal into the variation of the cell count during a short period in the target traffic. At the entry onionrouter,the cellsinthecircuitqueuearerecordedinthelog, and the recovery mechanisms will be applied to recognize the embeddedsignal.Inaddition,wechosedifferentthresholdsand types in our recovery mechanism.



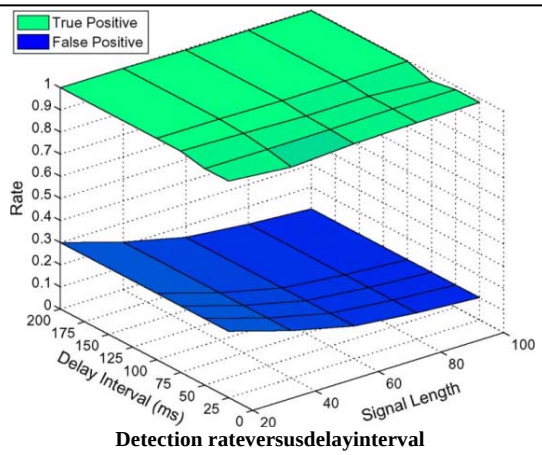
Detection rateversusdelayinterval (Note: Therateisfordetecting onebit).



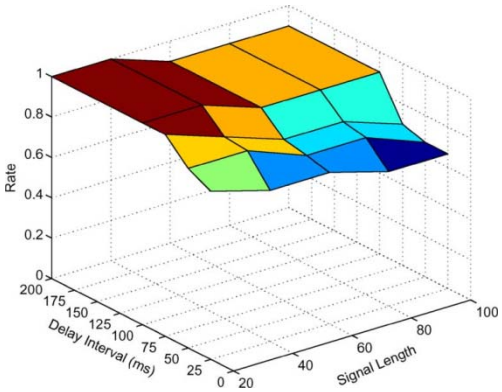
Detection rateversusdelayinterval andsignallengthwithdetection scheme1(Note: Therateisfor detectingonebit).



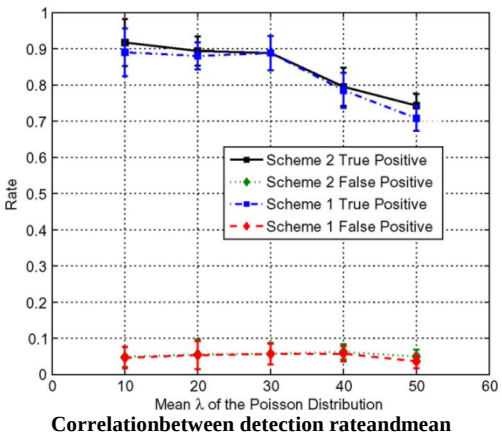
Detection rateversusdelay interval andsignallengthwithdetection scheme1.



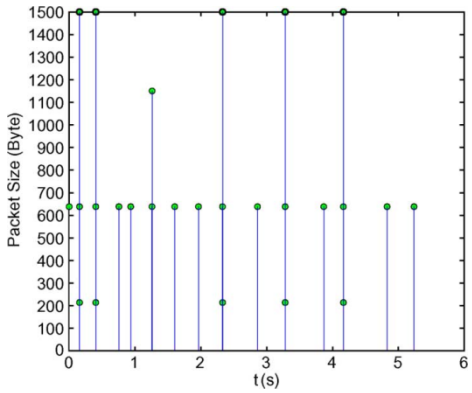
Detection rateversusdelayinterval andsignallengthwithdetection scheme2(Note: Therateisfor detectingonebit).



Detection rateversusdelay interval andsignallengthwithdetection scheme2.



Correlationbetween detection rateandmean ofthePoissondistri- bution(Note: Therate isfordetecting onebit).



Variance ofIPpacket size.

CONCLUSIONS

In this project, we introduced a novel cell-counting-based attack against Tor. This attack is ifficult to detect and is able to quickly and accurately confirm the anonymous communication relationship among users on Tor. An attacker at the malicious exit onion router slightly manipulates the transmission of cells from a target TCP stream and embeds a secret signal (a series of binary bits) into the cell counter variation of the TCP stream. 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. Our theoretical analysis shows that the detection rate is a monotonously increasing function with respect to the delay interval and is a monotonously decreasing function of the variance of one way transmission delay along a circuit. Via extensive real-world experiments on Tor, the effectiveness and feasibility of the attack is validated. Our data showed that this attack could drastically and quickly degrade the anonymity service that Tor provides. Due to Tor's fundamental design, defending against this attack remains a very challenging task that we will investigate in ourfuture research.

REFERENCES:

[1] Q.X.Sun, D.R.Simon, Y.Wang, W.Russell, V.N.Padmanabhan, and L.L.Qiu, "Statistical identification of encrypted Webbrowsing traffic,"inProc.IEEE S&P,May2002,pp.19–30.

[2] X.Fu,Y.Zhu, B.Graham, R.Bettati, and W.Zhao, "On flowmarking attacksinwirelessanonymous communication networks,"inProc. IEEEICDCS,Apr.2005,pp. 493–503.

[3] L.Øverlier and P.Syverson, "Locating hidden servers," in Proc. IEEE S&P, May2006,pp.100–114.

[4] G.Danezis,R.Dingledine, andN.Mathewson, "Mixminion: Design of a type III anonymousremailer protocol,"inProc. IEEES & P, May2003,pp.2–15.

[5] R.Dingledine, N.Mathewson, and P.Syverson, "Tor: The second- generationonionrouter,"inProc.13th USENIXSecuritySymp.,Aug.2004,p.21.

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

[7] A.Serjantov and P.Sewell, "Passive attack analysis for connection based anonymity systems,"inProc.ESORICS,Oct.2003, pp.116–131.

[8] B. N.Levine, M.K. Reiter, C.Wang, and M.Wright,"Timingattacks 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 Mixnetworks," inProc.PET, May2004, pp.735–742.

[10] S.J.MurdochandG.Danezis,"Low-costtrafficanalysisofTor,"inProc. IEEES&P, May 2006,pp. 183–195.

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

[12] X.Wang, S.Chen, and S.Jajodia, "Network flow water marking attack onlow-latencyanonymouscommunication systems,"inProc.IEEE S&P, May2007,pp.116–130.

[13] W.Yu,X. Fu, S.Graham, D.Xuan, and W.Zhao, "DSSS-based flow marking technique for invisible traceback,"inProc.IEEES&P,May2007, pp.18–32.

[14] N.B.Amir Houmansadr and N.Kiyavash, "RAINBOW: Arobust and invisiblenon-blind water mark for network flows," in Proc.16thNDSS, Feb.2009,pp.1–13.

[15] V. Shmatikovand M.-H. Wang,"Timinganalysisin low-latency MIX networks: Attacks and defenses,"in Proc.ESORICS,2006, pp. 18–31.

[16] V.Fusenig, E.Staab, U.Sorger, and T.Engel, "Slotted packet counting attacks on anonymity protocols," in Proc. AISC, 2009, pp.53–60.