MODELING AND PREVENTION OF CELL COUNTING BASED ATTACKS ON TOR

Mamatha.Ch[1], Manoj Kumar.G[2]

[1]Student, [2]Asst.Professor, Department of CSE, MRCET, Andhra Pradesh, India
mamathachakilela@gmail.com, manojvarma9@gmail.com

Abstract

Many anonymous networks came into existence. For instance Tor allows its users to gain access to services anonymously. This network causes most of the attacks as the adversaries can hide their identity and make attacks successfully from a remote place. By making a new attack on Tor can find the vulnerability of the Tor. Ling et al. presented a new cell counting mechanism for making an attack on Tor. In this paper we implemented a custom simulator that models a Tor and demonstrates the cell counting attack by simulating nodes like sender, receiver, onion router and attacker. The experimental results revealed that the proposed attack mechanism is effective.

Keywords: *Anonymous network, Tor, attacker model, cell counting*

----------***----------

1. INTRODUCTION

Privacy and integrity have received great attention in all kinds of networks. With popularity of Internet various kinds of networks came into existence. One such network is known as Tor. This is an anonymous network where the users of the network can gain access to services of network without disclosing or proving identity. However, this kind of network is vulnerable to security attacks. The attacks are made by adversaries from a remote place through intermediary nodes. In anonymous networks encryption along can't make the network secure [1],[2]. Researchers worked on various models to protect such networks from malicious networks. Many anonymous applications were investigated in [3]. The anonymous applications can also be sued for file sharing and also web browsing [4], [5]. The remainder of this paper is structured as follows. Section 2 reviews literature. Section 3 provides information about the proposed model. Section 4 presents experimental results while section 5 concludes the paper.

2. RELATED WORK

Networks of all kinds are vulnerable unless certain security measures are considered. A good security review of network systems is found in [4], [3]. With respect to asynchronous communication much research went on earlier on mix networks. Traffic analysis techniques are used to detect and prevent attacks in mix systems. The existing techniques are categorized into two types namely active watermarking techniques and passive traffic analysis. Passive traffic analysis is used to find attacks where attackers record traffic and then reuse it as explored in [6] and [7]. By analyzing patterns of encrypted content also, the attackers are able to extract sensitive information as the recent study explores [8], [9], [10], and [11]. HTTP traffic with packets is explored in [10] for identifying web pages satisfactorily. The distribution of packet sizes in encrypted VoIP content is investigated in [9]. Spoken phases can be intercepted by eavesdropper or adversary when it is of VoIP kind as explored in [12].

Active watermarking on the other hand embeds signals into traffic as discussed widely in [13], [14], [15], and [16]. These techniques also are capable of reducing false positives by using passive traffic analysis. Flow-watermarking scheme was proposed by Yu et al. [15] to identify secret communication in mix networks. In [2] compromised mix router is studied using a security scheme. In [13] timing – based attacks pertaining to watermarking and the trace back. The feasibility of timing based attacks is also explored by Wang et al. [14]. The secrecy of timing – based attacks and the watermarking for making trace back are explored in [13] and [17]. In [18] a multi-flow approach is proposed to watermark that is interval – based [19], [20]. Other kind of water marks known as DSSS-based watermarks are explored in [15]. For observing long silence periods multi-flow-based watermarking is used.

3. PROTOTYPE IMPLEMENTATION

We have implemented a custom simulator which models a sender, receiver, router, and attacker. Our aim is to demonstrate a cell counting attack in the anonymous network. The application is built in a PC with 4 GB RAM, Core 2 Dual processor running Windows XP OS. The representations of sender node, receiver node, and router and attacker node are presented here. Fig.2 shows the UI of sender node.

Fig. 1– Typical sender node

As can be seen in fig. 2, the GUI shows the typical sender node behavior. The sender node sends data to a receiver which is sent through various router nodes. The router node forwards the data to destination node through one or more intermediate routers. The router node is as shown in fig. 3.

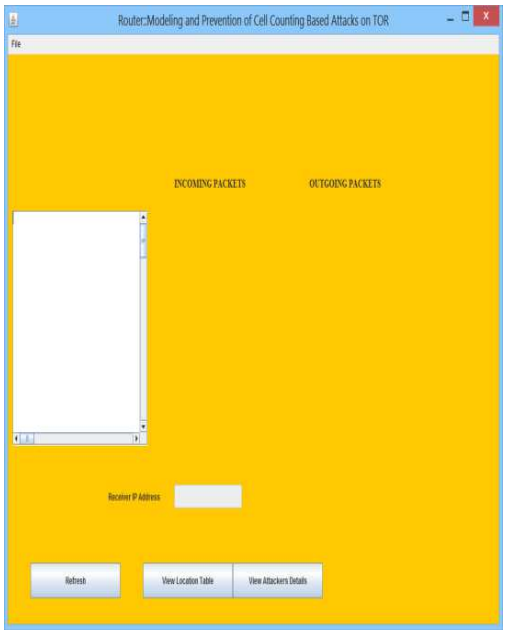

Fig. 2 – A typical router node

As can be seen in fig. 2, the router node shows the status of incoming and outgoing packets. It also shows any packets which are subjected to attacks. The router can forward data it receives to either other router or destination.

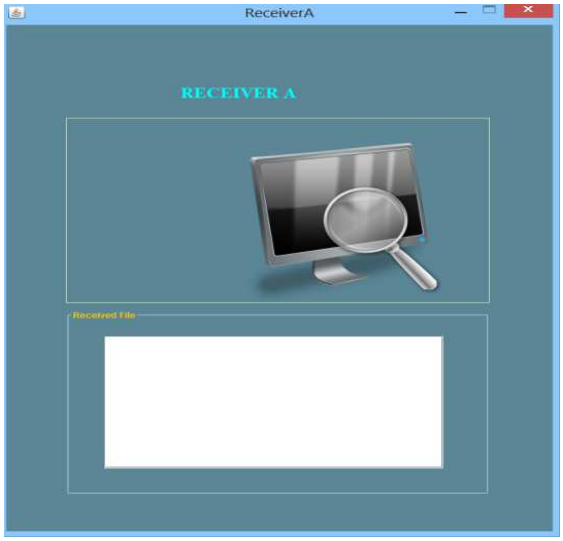

Fig.3 – A typical receiver node

As can be seen in fig. 3, the user interface of the receiver node is shown. This program simulates the receiver's behavior in the network.

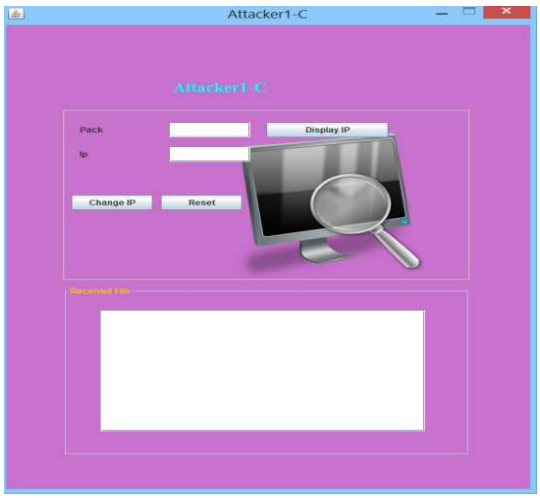

Fig.4 – A typical attacker node

As can be seen in fig. 4, the user interface of typical attacker is simulated. The attacker node is used to demonstrate to make a cell counting attack on the network.

4. EXPERIMENTAL RESULTS

Various experiments are made in the simulated network in terms of packet size, number of malicious routers, delay probability, maximal likelihood and so on. The experimental results are presented here. Fig. 1 shows the number of packets and packet size.

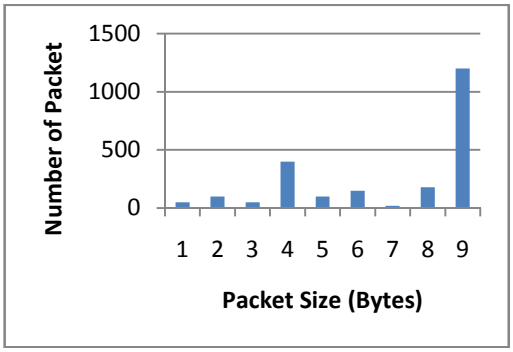

Fig. 5- Number of packets versus packet size

As shown in fig 5 the horizontal axis represents packet size while the vertical axis represents number of packets.

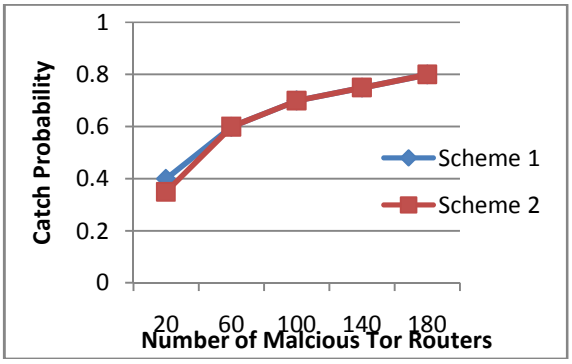

Fig6. Probability that a circuit chooses the malicious routers as entry and exit routers versus number of malicious Tor routers

As shown in fig.6 the horizontal axis is represented as number of malicious tor routers while the vertical axis represented as catch probability

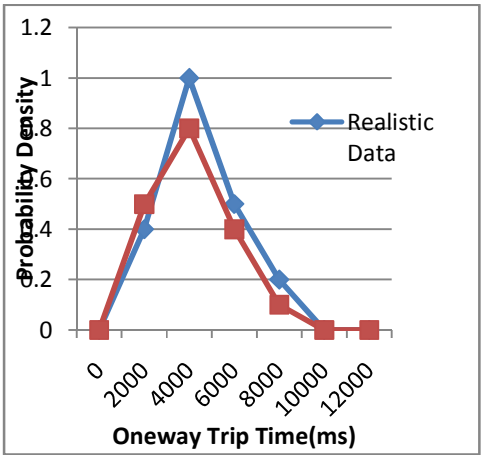

Fig7. One-way trip time probability density function

As shown in fig.7. The horizontal axis is represented as one way trip time while the vertical axis represented as probability density.

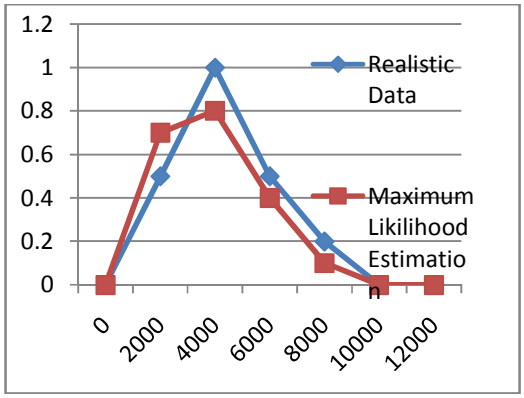

Fig8. One-way trip time probability density function in US

As shown in fig.8. The horizontal axis is represented as one way trip time while the vertical axis represented as probability density.

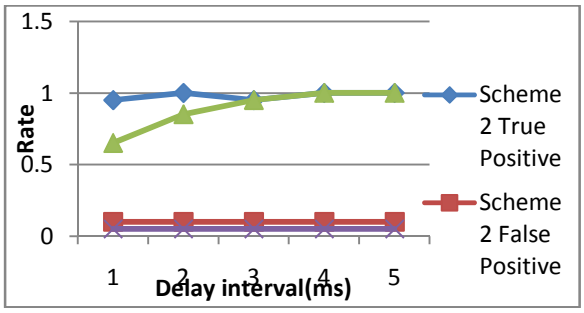

Fig9. Detection rate versus delay interval (Note: The rate is for detecting one bit).

As shown in fig.9. The horizontal axis is represented as delay interval while the vertical axis represented as rate.

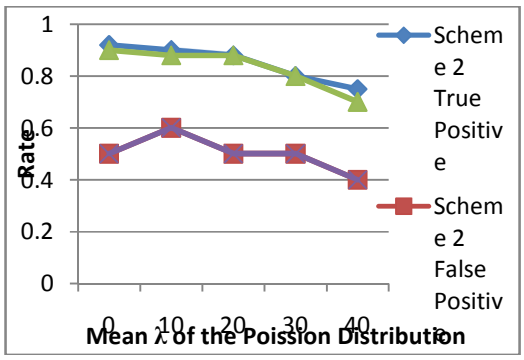

Fig10. Correlation between detection rate and mean of the Poisson distribution (Note: The rate is for detecting one bit).

As shown in fig.10. The horizontal axis is represented as Mean λ of the position distribution while the vertical axis represented as rate.

CONCLUSIONS

In this paper we develop a custom simulator Tor network which demonstrates a new cell counting based attack. Ling et al. [22] presented a mechanism where an attacker can make a new cell counting based attack on Tor network. We implemented this network using custom Java simulator which demonstrates the typical behavior of sender node, receiver node, router node and attacker node. We performed various experiments on the proposed network with regard to cell counting attack. The experimental results revealed that the attack mechanism is successful.

REFERENCES

[1] X. Fu,Y. Zhu, B.Graham, R. Bettati, andW. Zhao, "On flow marking attacks in wireless anonymous communication networks," in Proc.IEEE ICDCS, Apr. 2005, pp. 493–503
[2] L. Øverlier and P. Syverson, "Locating hidden servers," in Proc. IEEE S&P, May 2006, pp. 100–114
[3] G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: Design of a type III anonymous remailer protocol," in Proc. IEEE S&P, May 2003, pp. 2–15.
[4] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The secondgeneration onion router," in Proc. 13th USENIX Security Symp., Aug. 2004, p. 21.
[5] "Anonymizer, Inc.," 2009 [Online]. Available: http://www.anonymizer.com/
[6] 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
[7] 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
[8] Q. X. Sun, D. R. Simon, Y. Wang, W. Russell, V. N. Padmanabhan, and L. L. Qiu, "Statistical identification of encrypted Web browsing traffic," in Proc. IEEE S&P, May 2002, pp. 19–30.
[9] C. V.Wright, L. Ballard, F. Monrose, and G.M.Masson, "Language identification of encrypted VoIP traffic: Alejandra y Roberto or Alice and Bob?," in Proc. 16th Annu. USENIX Security Symp., Aug. 2007, pp. 43–54.
[10] M. Liberatore and B. N. Levine, "Inferring the source of encrypted HTTP connections," in Proc. ACM CCS, Oct. 2006, pp. 255–263.
[11] D. X. Song, D. Wagner, and X. Tian, "Timing analysis of keystrokes and timing attacks on SSH," in Proc. 10th USENIX Security Symp., Aug. 2001, p. 25.
[12] C. V.Wright, L. Ballard, S. E. Coull, F.Monrose, and G. M. Masson, "Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversation," in Proc. IEEE S&P, May 2008, pp. 35–49.
[13] X. Wang and D. S. Reeves, "Robust correlation of encrypted attack traffic through stepping stones by manipulation of inter-packet delays," in Proc. ACM CCS, Nov. 2003, pp. 20–29
[14] X. Wang, S. Chen, and S. Jajodia, "Tracking anonymous peer-to-peer VoIP calls on the internet," in Proc. 12th ACM CCS, Nov. 2005, pp. 81–91.
[15] 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.
[16] S. J. Murdoch and G. Danezis, "Low-cost traffic analysis of Tor," in Proc. IEEE S&P, May 2006, pp. 183–195.
[17] P. Peng, P. Ning, and D. S. Reeves, "On the secrecy of timing-based active watermarking trace-back techniques," in Proc. IEEE S&P, May 2006, pp. 335–349
[18] N. Kiyavash, A. Houmansadr, and N. Borisov, "Multi-flow attacks against network flow watermarking schemes," in Proc. USENIX SecuritySymp., 2008, pp. 307–320 LING et al.: NEW CELL-COUNTING-BASED ATTACK AGAINST TOR 1261
[19] Y. J. Pyun, Y. H. Park, X. Wang, D. S. Reeves, and P. Ning, "Tracing traffic through intermediate hosts that repacketize flows," in Proc.IEEE INFOCOM, May 2007, pp. 634–642
[20] X.Wang, S. Chen, and S. Jajodia, "Network flow watermarking attack on low-latency anonymous communication systems," in Proc. IEEES&P, May 2007, pp. 116–130.
[21] Zhen Ling, Junzhou Luo, Wei Yu, Xinwen Fu, Dong Xuan, and Weijia Jia, "A New Cell-Counting-Based Attack Against Tor". IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO 4, AUGUST 2012.

BIOGRAPHIES

Mamatha.Ch, she is pursuing M.Tech (CSE) in MRCET, Hyderabad, AP, INDIA. She has received B.Tech Degree in Computer Science and Engineering. Her main research interest includes Networking.

Manoj Kumar.G, He is working as an assistant professor in MRCET. He has received MCA Degree in Computer Science and M.Tech degree in Computer Science and Engineering. His main Research interests include Networking