Cover Letter

Research Title: DSSS-Based Flow Marking Technique for Invisible Traceback
Student Name: Wei Yu
Affiliation: Ph.D. Student, Compute Science Dept., Texas A&M University
Postal Address: 4608 Dalrock Dr., Plano, TX 75024
Email: weiyu@cs.tamu.edu
Research Advisor Name: Dr. Wei Zhao, Rensselaer Polytechnic Institute (RPI)
Research Colleagues: Dr. Xinwen Fu, Dakota State University (DSU); Dr. Steve Graham (DSU); Dr. Dong Xuan, Ohio State Uiversity (OSU)
ACM Student Member Number: 9428623
Category: Graduate
Further information is available at *http://students.cs.tamu.edu/weiyu/*

Summary: Law enforcement agencies need the ability to conduct electronic surveillance to combat crime, terrorism, or other malicious activities exploiting the Internet. However, the proliferation of anonymous communication systems on the Internet has posed significant challenges to providing such traceback capability. In this project, we develop a new class of flow marking technique for invisible traceback based on Direct Sequence Spread Spectrum (DSSS), utilizing a Pseudo-Noise (PN) code. By interfering with a sender's traffic and marginally varying its rate, an investigator can embed a secret spread spectrum signal into the sender's traffic. The embedded signal is carried along with the 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. The secret PN code makes it difficult for others to detect the presence of such embedded signals, so the traceback, while available to investigators is, effectively invisible. We demonstrate a practical flow marking system which requires no training, and can achieve both high detection and low false positive rates. Using a combination of analytical modeling, simulations, and experiments on Tor (a popular Internet anonymous communication system), we demonstrate the effectiveness of the DSSS-based flow marking technique. Our ongoing studies have shown the double-edge nature of this DSSS-based technique which can be used by malicious attackers to secretly identify the deployed locations of Internet threat monitoring systems for Internet worm defense.

This project is jointed work between Texas A&M University and Dakota State University. It is partially supported by the NSF under CNS-0721766/CNS-0722856, the South Dakota Governor Individual Research Seed Grant Program, and the South Dakota Electronic Health Record Assessment (SDEHRA) project of the South Dakota Department of Health. As the result of this work, the following papers were published, including the 2007 IEEE Symposium on Security and Privacy (Oakland) (the most prominent international security conference), IEEE INFOCOM 2008, and IEEE DSN 2008.

[1] Wei Yu, Xinwen Fu, Steve Graham, Dong Xuan and Wei Zhao, "DSSS-Based Flow Marking Technique for Invisible Traceback", in *Proc. of IEEE Symposium on Security and Privacy (Oakland)*, May 2007.
[2] Xun Wang, Wei Yu, Xinwen Fu, Dong Xuan and Wei Zhao, "iLOC: An Invisible LOCalization Attack to Internet Threat Monitoring Systems", In *Proc. of IEEE International Conference on Computer Communications (INFOCOM)*, April 2008.
[3] Wei Yu, Nan Zhang, Xinwen Fu, Ricardo Bettati and Wei Zhao, "On Localization Attacks to Internet Threat Monitors: An Information-Theoretic Framework", accepted to appear in *Proc. of IEEE International Conference on Dependable Systems and Networks (DSN)*, June 2008.

DSSS-Based Flow Marking Technique for Invisible Traceback

1. Problem and Motivation

The growth of the Internet has brought convenience to our lives and created worldwide economic boom in network based businesses. However, it has also become a breeding ground for a variety of crimes. Valuable network services for anonymous communication, such as Tor [1], [2] and Anonymizer [3], can enhance privacy by supporting anonymous publishing and browsing, and can protect users from malicious eavesdroppers. Yet such anonymous communication systems can be subverted and used for crimes such as illegal file sharing or child pornography distribution. Terrorists or other conspirators can also abuse such systems.

Because crime has spread along with the fast growing convergent technologies which comprise the Internet, network forensics has a more and more important role to play, supporting legal surveillance in a technically challenging domain. However, questionable practices have left network forensics troubled, where reliance on inaccurate data can lead to wrongful surveillance, detention, deportation, prosecution, or even conviction. A number of anonymous remailers have been shutdown because of legal troubles since 1996 [4]. In Germany, the operation and expansion of anonymous browsing networks, such as Tor, have been slowed by incidents involving the detention and arrest of innocent Tor node operators in the last two years [5]. Effective forensic approaches can boost the deployment of privacy-preserving systems on the Internet by enabling legal surveillance.

A fundamental network-based forensic technique is traceback [6], [7], [8]. Both accuracy and secrecy of traceback are essential for successful network forensics. Accurate traceback makes surveillance possible, while traceback secrecy prevents suspects from realizing they are under surveillance. Secrecy refers to the difficulty of detecting traceback activity by anyone other than the investigators. When a suspect can realize that he is being traced, he will take countermeasures to prevent further collection of evidence. Furthermore, if a suspect can determine the parameters of the traceback technique, he may introduce disinformation, such as incriminating other network users by deliberately embedding marks into their traffic. In any case, a failure of secrecy leads to the loss of forensic evidence, or worse, damaged or contaminated evidence.

2. Background and Related Work

Researchers have been developing anonymous communication systems over the past two decades. Mix networks [1], [2] are a popular tool for this purpose. Originally developed for anonymous email [9], mix networks were later adapted to provide anonymity for low latency, connection-based applications such as web browsing. Our research on traceback mechanisms focuses on such low latency applications.

To trace Internet communications despite anonymous channels, we must use traffic characteristics other than the easily modified IP headers. To this end, the traffic analysis techniques have been studied and can be classified into two categories: passive traffic analysis and active traffic analysis. For the passive traffic analysis, in order to identify or confirm a communication relationship (e.g., determine whether Alice is communicating with Bob) through a mix network, the traffic is recorded and similarities between Alice's outbound traffic and Bob's inbound traffic may be measured. Many techniques belong to this category [10], [11], [12], [13]. However, passive traffic analysis can be defeated by countermeasures such as batching, padding, or reordering [14].

For this project, we adopted an active traffic-based approach, e.g., a *flow marking* technique, initially introduced in [15]. In contrast to passive traffic analysis techniques, to determine whether a sender is communicating with a receiver, an investigator, known as the *interferer*, can embed a series of marks (signals with a specific pattern) into the sender's traffic by interfering with the sender's outbound messages. Another investigator, known as the *sniffer*, eavesdrops on the receiver's inbound traffic. If a similar pattern of embedded marks is found in the receiver's traffic, the investigators know that the sender is communicating with the receiver. By tracing the marks, investigators may reconstruct the full communication path. Since the investigator has the capability to control where and when to embed the marks, fast and robust traceback can be achieved [15].

3. Approach and Uniqueness

However, existing active traffic analysis based techniques have generally been unable to meet both of the traceback requirements (accuracy and invisibility) simultaneously [15], [16]. For example, consider marks in a periodic pattern such as the approach described in [15]. They are easy to introduce (since an investigator may just interfere with a target traffic flow periodically), and detect (a sniffer would apply a *Fourier* transform). However, period patterns may have a high false positive rate, since such traffic markings may induce a similar pattern into other traffic sharing a link. Furthermore, if a *Fourier* Transform is applied to a traffic flow containing a periodic pattern, the periodic pattern will be obvious in the frequency domain to the correspondents, who may adopt countermeasures to defeat this approach. Clearly, a flow marking technique must address these shortcomings, decreasing false positives, while increasing the difficulty of detection by anyone other than the investigators.

In this project, we develop a novel class of flow marking technique for invisible traceback based on *Direct Sequence Spread Spectrum* (DSSS). Applying this technique, the investigator introduces DSSS marks into a target traffic flow. The marks correspond to a signal modulated by a *Pseudo-noise* (PN) code, known only to the investigators. Only those with knowledge of the code can correctly recover the original signal and identify the communication relationship. The PN code modulated signal will appear as innocent noise in both the time and spectrum domains, so detection of such marks is difficult. Because the marks resemble noise (without knowledge of the PN code), correspondents cannot use the approach from [15], which relies on recognizing periodic patterns in traffic, to recognize the embedded signals studied within this research. Therefore, using a DSSS-based technique, we are able to accurately trace identify suspect senders and receivers communicating anonymously without alarming the suspects.

We develop a new DSSS mark generator that embeds a secret spread signal using a PN code into a target flow at the transmitter. To recover the signal at the receiver, we use digital filters to remove direct current components, which correspond to network traffic seasonal variations and high frequency noise from target traffic flow, so we can effectively recover the DSSS marks. Our DSSS-based technique has a simple and effective decision rule, compared with other threshold-based techniques that normally require lengthy and impractical training processes [10], [11]. Using a model, we derive formulas for detection and false positive rates for our traceback technique. We discuss how to determine various parameters such as an appropriate PN code length, interference strength. We also address practical issues such as PN code synchronization and tracing multiple traffic flows simultaneously.

Besides theoretical analysis, we have also conducted extensive evaluations of our DSSS approach using both simulations and real-world experiments. We used *ns-2* simulations to explore the effectiveness of our DSSS-based technique. Simulation results show that even with low traffic mark strength, our technique is robust and able to correlate sender and receiver communication relationships at a probability of 100%, so long as the PN code length is sufficiently long. We show that the false positive rate is also substantially reduced. Our data show that the DSSS-based technique is capable of effectively invisible traceback, since there is no clear difference between the traffic with marks and the traffic without marks in either the time domain or the spectrum domain. We developed a suite tools and performed a set of real-world Internet experiments on communications using *Tor*, a popular anonymous communication network for transporting TCP streams over the Internet. Our data validate the theoretical and simulation findings and demonstrate that our DSSS-based technique can track anonymous traffic flows through the *Tor* network, even when such flows exhibit wild dynamics.

4. Results and Contributions

To summarize, the DSSS-based flow marking technique uses the following mechanisms to achieve both accuracy and secrecy of traceback:

- Secrecy of the code. The DSSS marks provide secrecy based on the secrecy of the code. Since the suspect sender and receiver don't know the code, it is very difficult for them to recognize the existence of marks embedded in their traffic.
- The strength of DSSS marks can be very low in comparison with Internet background traffic as noise so that the DSSS marks are covered by the hosted traffic. The recognition process will effectively restore the spread signal to its narrow band and recover DSSS marks from the noise.
- Given a low strength of DSSS marks for traceback secrecy, we can use a PN code with reasonable length to achieve traceback accuracy as well.
- DSSS marks show a white noise-like pattern in both time and frequency domains. PN code modulated traffic appears random for those who don't know the code. In general, the greater the code length, the harder the code is to detect. The mark pattern is also designed to appear random in order to maintain the secrecy. It is not feasible to recognize PN code modulated traffic in time and frequency domains.

The results of our work have both intellectual merit and broader impacts.

Intellectual Merit: In this research, we used a formal and rigorous approach, followed by empirical investigations to study the fundamental issues involved in invisible traceback techniques with respect to anonymous Internet communication systems. Our DSSS flow marking technique is capable of tracing communications through anonymity systems while remaining effectively undetectable. The significance of this work will be as follows.

- Our research work is fundamental. We applied communication theory to carry out a thorough study of invisible traceback techniques. Based on the resulting analytical model, we derived formulas for detection and false positive rates for the DSSS traceback technique. Our theoretical analysis provides guidance to determine various design parameters such as an appropriate PN code length, and the strength of marks.
- Our research work is practical. We have conducted evaluations to our proposed approach using both *ns-2* simulations and experiments on *Tor*, a popular anonymous communication system. Our real-world experiments corroborate our theoretical results and demonstrate the utility of our technique for real-world systems.
- Our research work is extensible. This project builds a foundation for studying and evaluating invisible traffic analysis techniques. There are a number of possibilities for extending this research. For example, our ongoing studies have shown the double-edge nature of this technique which can be used by malicious adversaries to identify the deployed locations of Internet threat monitoring systems for Internet worm defense [17]. We also systematically studied countermeasures against such a threat based on an information theoretic-based framework [18]. Our technique can also be applied to trace communications in wireless networks. We can use wireless jamming techniques to interfere with the wireless traffic and effectively embed the PN coded signals into the target wireless communications flow. Using techniques similar to those developed in this project, communication paths in wireless network can be traced by tracking the embedded signal.

Broader Impacts: There are immediate and obvious impacts of this research work for the security and privacy of both wired and wireless networks. Both the security and the privacy of information networks are widely acknowledged as important and timely topics among computer science researchers and educators. The research conducted on this project will advance the theories and understanding needed for defending the security and privacy of individuals as well as our national information infrastructure. Our work on this project provides both strong theoretical foundations and practical test beds that network systems designers and practitioners can use to improve the designs and services of deployed systems. We also expect this research to have an impact on security related education across a broad range of subjects and at a wide range of academic levels. In particular, my research colleagues in Dakota State University (DSU) and Ohio-State University (OSU) have integrated research material directly into relevant security courses. This work demands and applies a deeper knowledge of signal processing and communications theory that is an innovative component of security courses. Additionally, colleagues have encouraged highly motivated students to conduct research or honors projects on topics relevant to this work.

REFERENCES

[1] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The second-generation onion router,” in *Proceedings of the 13th USENIX Security Symposium*, August 2004.
[2] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” *Communications of the ACM*, vol. 4, no. 2, February 1981.
[3] Anonymizer, Inc., “Anonymizer,” http://ww.anonymizer.com/, 2007.
[4] Wikipedia, “Penet remailer,” http://en.wikipedia.org/wiki/Penet_remailer, 2007.
[5] R. Dingledine and N. Mathewson, “Tor: An anonymous internet communication system,” http://archives.seul.org/or/talk/, 2006.
[6] Y. Zhang and V. Pasxon, “*Detecting stepping stones*,” in *Proceedings of the 9th USENIX Security Symposium*, August 2000.
[7] X. Wang and D. S. Reeves, “Robust correlation of encrypted attack traffic through stepping stones by manipulation of inter-packet delays,” in *Proceedings of the 2003 ACM Conference on Computer and Communications Security (CCS)*, November 2003.
[8] X. Wang, S. Chen, and S. Jajodia, “Tracking anonymous peer-to-peer voip calls on the internet,” in *Proceedings of the 12th ACM Conference on Computer Communications Security (CCS)*, November 2005.
[9] G. Danezis, R. Dingledine, and N. Mathewson, “Mixminion: design of a type III anonymous remailer protocol,” in *Proceedings of the 2003 IEEE Symposium on Security and Privacy (S&P)*, May 2003.
[10] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, “On flow correlation attacks and countermeasures in mix networks,” in *Proceedings of Workshop on Privacy Enhancing Technologies (PET)*, May 2004.
[11] B. N. Levine, M. K. Reiter, C. Wang, and M. Wright, “Timing attacks in low-latency mix-based systems,” in *Proceedings of Financial Cryptography (FC)*, February 2004.
[12] S. J. Murdoch and G. Danezis, “Low-cost traffic analysis of tor,” in *Proceedings of the IEEE Security and Privacy Symposium (S&P)*, May 2006.
[13] L. Overlier, “Locating hidder servers,” in *Proceedings of the IEEE Security and Privacy Symposium (S&P)*, May 2006.
[14] A. Serjantov, R. Dingledine, and P. Syverson, “From a trickle to a flood: active attacks on several mix types,” in *Proceedings of Information Hiding Workshop (IH)*, February 2002.
[15] X. Fu, Y. Zhu, B. Graham, R. Bettati, and W. Zhao, “On flow marking attacks in wireless anonymous communication networks,” in *Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS)*, April 2005.
[16] P. Peng, P. Ning, and D. S. Reeves, “On the secrecy of timing-based active watermarking trace-back techniques,” in *Proceedings of the IEEE Security and Privacy Symposium (S&P)*, May 2006.
[17] X. Wang, W. Yu, X. Fu, D. Xuan and W. Zhao, “iLOC: an invisible LOCalization attack to internet threat monitoring systems”, In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, April 2008.
[18] W. Yu, N. Zhang, X. Fu, R. Bettati and W. Zhao, “ On localization attacks to internet threat monitors: an information-theoretic framework”, accepted to appear in *Proceedings of IEEE International Conference on Dependable Systems and Networks (DSN)*, June 2008.