Optimal Payoff for Selective Traceable Anonymity of a Network System

Extended Abstract

Md Rasel Al Mamun
University of North Texas
1307 W. Highland, Denton, TX
mdrasel.mamun@unt.edu

Bin Mai
University of North Texas
1307 W. Highland, Denton, TX
Bin.Mai@unt.edu

Bongsik Shin
San Diego State University
San Diego, CA 92182
bshin@mail.sdsu.edu

Shailesh Kulkarni
University of North Texas
1307 W. Highland, Denton, TX
Shailesh.Kulkarni@unt.edu

Dan J. Kim
University of North Texas
1307 W. Highland, Denton, TX
Dan.Kim@unt.edu

Keywords: Payoff, Traceable Anonymity, Degree of Anonymity, Cybersecurity

Optimal Payoff for Selective Traceable Anonymity of a Network System

Introduction:

One key solution for addressing the cybersecurity from the Bright Internet perspective is to find a way to trace aggressors without affecting the general spirits of the Internet, especially maintaining the privacy of benign users. The selective tracing of those who abuse the Internet is not a trivial task although it holds a key to the ultimate realization of BI. *Selective traceability* (or *traceable anonymity*) allows tracking of adversaries should the need arises (e.g., satisfaction of a policy), while protecting the anonymity of ordinary users As bright internet initiative, in the editorial article of MIS Quarterly, Lee (2015, 2016), has described "digital search warrant" that is based on efficient use of selective traceable anonymity (tracing in formal manner) as the deterrence mechanism of cybercrime.

Selective traceability (or *traceable anonymity*) is intended to discourage crimes or misbehaviors committed under the shadow of anonymity, while guaranteeing freedom of expressions. There is no questions that *traceable anonymity* is the most powerful psychological deterrence mechanism. Granted, attribution in cyberspace is difficult as there is a multitude of obfuscation techniques for adversaries to shield the true origin. However, some research paper, for example (Slamanig & Rass, 2010; Von Ahn, Bortz, Hopper, & O Neill, 2006), have provided technological solution for achieving selective traceable anonymity of users. Some contemporary cases of successful tracing the anonymous users (Wright & Kakalik, 2006) suggest the practical implication of tracing protocols and achievement of traceability.

This successful traceability arises the need for measuring the trade-off between anonymity and traceability of the network system. However, no research paper has yet been published measuring the trade-off between anonymity and traceability of the network system. Therefore, the purpose of this study is to understand the payoffs from traceable anonymity in a network under different circumstances, and the optimal configuration of the traceability/anonymity of the network to maximize the expected payoffs. In this study we investigate following research questions: what is the optimal trade-offs between traceability and anonymity in a communication network?

Background Information:

Motivation and technological solution for anonymity:

Since the inception of internet, effort was made to protect security and privacy of users. The rapid growth of internet applications has made the privacy protection more important. Encryption technology is one of the ways that carry on protection to the correspondence data content. However, in many special application fields, such as e-mail, e-voting, e-health e-commerce, e-cash, the protection degree of users' information, like users' identity, geographical location and so forth is important attributes for the overall system security. So anonymous communication was considered one of the most effective ways to protect privacy of users. It aims to preserve communication privacy and integrity within the shared public network environment. The research on anonymous communication was initiated in 1981 on electronic mail return address (D. L. Chaum, 1981) and successfully extended in many areas. The existing anonymous communications systems can be divided into four categories: cryptosystem-based schemes, routing-based schemes, broadcasting-based systems, and peer-to-peer communication systems and each of them provides strong anonymity guarantee (Ren & Wu, 2010).

Cryptosystem-based schemes: D. Chaum and Van Heyst (1991) introduced group signature that allows any member of a group to digitally sign a document anonymously without being individually identifiable. Rivest, Shamir, and Tauman (2001) invented the concept of ring signature that is a type of digital signature can be performed by any member of a group of users. I Ring signature specifies a set of possible signers instead of revealing the identity of a individual signer.

Mixnet-based schemes: Many anonymous communication protocols have been developed based on Chaum's mix net (D. L. Chaum, 1981) and DC-net (D. Chaum, 1988) communication protocol. For anonymous email applications, Chaum's mix net takes a number of ciphertexts as input, encrypted using public keys of the relay servers, called mixes, decrypts and shuffles them and finally outputs a random permutation of plaintexts. Cypherpunk remailers (Parekh, 1996), also called Type I remailers are the first widespread public implementation of mixnet attempt to limit the feasibility of traffic analysis by providing an anonymous store and forward architecture. Reed, Syverson, and Goldschlag (1998) developed Onion routing that is a distributed overlay network designed to anonymize TCP-based communications over a computer network according to the principle of Chaum's mix cascades (D. L. Chaum, 1981). Tor was developed in 2004 as the second generation of onion router (Dingledine, Mathewson, & Syverson, 2005). Berthold, Federrath, and Köpsell (2001) proposed Web Mixes that was designed for anonymous and unobservable real-time Internet access that can prevent traffic analysis as well as flooding attacks.

Routing based schemes: Reiter and Rubin (1998) developed Crowds to defend against internal attackers and a corrupt receiver that provides users with a mechanism for anonymous Web browsing. The idea that Anonymous communication that can be viewed as a bus system (Bos & den Boer, 1989) was further extended by Beimel and Dolev (2003) for messages to travel on the network so that each piece of information is allocated a seat within the bus and routers are chosen and buses traverse these routes either through deterministic or randomized schedules. Since the buses traverse the network in fixed routes, the adversary cannot learn whether there is any communication between the nodes or not.

Peer-to-peer communication: Tarzan, designed by Freedman and Morris in 2002 (Freedman & Morris, 2002) is a peer-to-peer anonymous IP network overlay. In this protocol, a message initiator chooses a path of peers pseudo-randomly in a way that adversaries cannot easily influence. Anonymity is achieved with a layered onion encrypted connection, replayed through a sequence of intermediate nodes. MorphMix is another peer-to-peer system for anonymous Internet usage developed by Rennhard and Plattner also in 2002. The architecture and the threat model of MorphMix is similar to Tarzan. However, the basic difference between MorphMix and Tarzan is that in Tarzan, the route is specified by the source, while in MorphMix, the route is chosen by the intermediate nodes.

Motivation and technological solution for traceable anonymity:

Now-a-days anonymous communication has several potential applications including anonymous email, web browsing, economic transactions, electronic voting. However, recently the advantage of anonymous communication is being used for several antisocial and terrorist activities such as slander, threat, illegal and malicious content transfer. Therefore, selective traceable anonymity has become important to protect this kind of abuse of anonymous communication in cyber space. Many research papers, for example (Backes, Clark, Druschel, Kate, & Simeonovski, 2013; Dodis, Kiayias, Nicolosi, & Shoup, 2004; Golle & Juels, 2004; Kiayias, Tsiounis, & Yung, 2004; Slamanig & Rass, 2010; Von Ahn et al., 2006; Wei, Hu, & Liu, 2014), have been published describing traceable algorithm for selective traceable anonymity.

Dodis et al. (2004) introduced *Ad-hoc Anonymous Identification* schemes that can be generally and efficiently amended so that they allow the recovery of the signer's identity by an authority, if the latter is desired. Kiayias et al. (2004) have presented, implemented and applied a privacy primitive called "Traceable Signatures." They have developed the underlying mathematical and protocol tools that present the concepts and the underlying security model, and then realize the scheme and its security proof. This traceable signatures support an extended set of fairness mechanisms (mechanisms for anonymity management and revocation) when compared with the traditional group signature mechanism. This notion allows (distributed) tracing of all signatures by a single (misbehaving) party without opening signatures and revealing identities of any other user in the system. Golle and Juels (2004) presented a new DC-net constructions that simultaneously achieve non-interactivity and high-probability detection and identification of cheating players. In Von Ahn et al. (2006), they have shown that, in principal, almost any anonymity scheme can be made selectively traceable, they also transform two anonymous protocols, 'El Gamal decryption' and 'group signatures', to traceable protocol.

In Slamanig and Rass (2010), they proposed an approach which provides a means for users to anonymously conduct transactions with a service-provider such that those transactions can neither be linked to a specific user nor linked together. we provide mechanism to identify misbehaving anonymous users (*selective traceability*) behind transactions that allows revocation of the anonymity of a suspicious user along with the identification of *all* of her transactions, without violating the privacy of all remaining users. Backes et al. (2013) introduced a generic mechanism for AC networks that provides practical repudiation for the proxy nodes by tracing back the selected outbound traffic to the predecessor node (but not in the forward direction) through a cryptographically verifiable chain. This mechanism also provides an option for full (or partial) traceability back to the entry node or even to the corresponding user when all intermediate nodes are cooperating. Wei et al. (2014), in their study, propose an efficient attribute-based signcryption scheme that achieves confidentiality against chosen ciphertext attacks and unforgeability against chosen messages attacks in the selective attribute model, as well as enjoys traceability by use of non-interactive witness indistinguishable proofs; that is, the authority can break the anonymity of users if necessary.

Payoff function for anonymity/traceability:

The research question we want to investigate in this paper is: how to obtain the optimal trade-offs between the level of anonymity vs. traceability in a communication network. In this context anonymity is defined as the state of being not identifiable within a set of users, the anonymity set (Pfitzmann & Köhntopp, 2001).Traceability in this context means that a traceable authority (TA) is able to identify the sender of a message (Slamanig & Rass, 2010).

We focus on a simple scenario: consider a network system of N users. In our scenario, the only activity the users engage in the network is to send one message to an external target. All users are identical in all aspects except one: ρ portion of the users are considered normal users whose message sent to the target will generate a positive payoff (denoted as β) to the network; while the rest (1- ρ) portion of the users are considered malicious users whose message sent to the target will cause a damage of γ to the network. Comparing intangible benefit from social reward explained in (Jiang, Heng, & Choi, 2013) we can define benefit as the reputation the network system earn will increase the number of users that eventually will increase the financial benefit of service providers. On the contrary, malicious users will bring bad reputation for the network system that will be the cause of reducing users and ultimately financial loss of service provider. We assume that while it is not directly observable which user is good or malicious, the value of ρ is public knowledge. The user will decide whether or not to send the message based on the anonymity/traceability level of the network.

In this case, the anonymity of any particular user in the network can be defined as the probability of any specific user being identified as the message sender. According to definition of total anonymity, we assume that without any traceability mechanism, each user has a probability of $1/N$ as being identified as the message sender, while total traceability means with the implementation of traceability mechanism, we are able to ascertain that one user has probability 1 and all other user has probability 0 as being the message sender.

Traceable anonymity would be a more general scenario between the above two extremes, indicating that with the implementation of specific traceability mechanism each user has probability p_i (where i=1 to N) as being identified as the sender.

To integrate each user's anonymity level into the degree of anonymity for the network, we adopt the information theoretic concept of entropy (Shannon 1948). As illustrated by Diaz, Seys, Claessens, and Preneel (2002), the maximum entropy (corresponding to the scenario without any traceability mechanism) of the network systems for N number of user is defined as $H_M = log_2 N$.The entropy of the network systems with traceable anonymity (corresponding to the scenario with some specific traceability mechanism) will be $H = -\sum_{i=1}^{N} p_i log_2(p_i)$, where p_i refers to probability of each user being identified as a sender.

Therefore, the degree of anonymity for the network can thus be defined as $= H/H_M$

For the implementation of traceability, the network system incurs some costs. We define this cost function $C(d)$ as the cost of implementation of selective traceability of the network system. It is assumed that $\partial C/\partial d < 0$, i.e., the higher the degree of anonymity d the network has, the lower the cost C the network system would incur.

- For certain level of anonymity d, the potential benefit to the network system caused by users' behavior can be defined as $U(d)$. It is assumed that $\partial U/\partial d > 0$, i.e., the higher the degree of anonymity d the network has, the higher the potential benefits the network system would obtain from user behaviors.
- For certain level of anonymity d, the potential damage of the network system caused by the users' behavior can be defined as (d) . It is assumed that $\partial V/\partial d > 0$, i.e., the higher the degree of anonymity d the network has, the higher the potential damages the network system would sustain from user behaviors.

We can thus define the overall payoff function for specific level of traceable anonymity as

$Q = U(d) - C(d) - V(d)$..... (1)

Equation 1 will be our objective functions to be optimized.

We now propose the actual functional forms for U, C, and V.

Cost function $C(d)$ is the cost of implementation of selective traceability to the network system. In our setting, at initial stage, the network system is totally anonymous. As (Huang, Hu, & Behara, 2008), it is reasonable to assume that the cost of implementation of selective traceability increases linearly with the increase of traceability; or conversely, the cost decreases with the decrease of anonymity level. We define α as the cost for implementation of total traceability (i.e., 0 anonymity level), therefore for implementing selective traceability, cost function $C(d) = \alpha(1 - d)$.

For the ρ portion of the users who are normal users, the payoffs generated to the network system can be defined as, $U(d) = \beta\rho N f(d)$. Following (Huang et al., 2008) and (Gordon & Loeb, 2002), it is reasonable to assume that the likelihood a normal user will send out a message is increasing with the increase of anonymity level; in addition, as the anonymity level increases, the rate of increase of this likelihood decrease. That is, the likelihood a normal user will send out a message is increasing in a concave fashion with increase of the anonymity level. We define $\theta 1$ as the

probability of normal user sending messages when network system is totally traceable (i.e., d=0), and $(1-\theta_2)$ is the probability of normal user sending messages when network system is totally anonymous (i.e., d=1). Therefore, we have $f(d) = (1-\theta_1-\theta_2)d^r + \theta_1$. Where, θ_1, θ_2 and r, all are between 0 and 1, and r is the parameter that defines the shape of the concave function. So, the benefit can be defined as $U(d) = \beta\rho N[(1-\theta_1-\theta_2)d^r + \theta_1]$.

For the $(1-\rho)$ portion of the user who are malicious users, the damage caused to the network system is defined as $V(d) = \gamma\,(1-\rho)Ng(d)$. We assume that when network system is totally traceable, no user will send malicious messages and the higher the degree of anonymity d, more likely the malicious user will send the message. We further assume that the likelihood of malicious user sending out message is increasing at an increasing rate with the increase of d (i.e., the likelihood of malicious user sending out message is an increasing convex function of d as explained by (Gordon & Loeb, 2002; Huang et al., 2008)). So, we define $g(d) = \delta d^w$, where δ is the probability of sending malicious messages when network system is totally anonymous and w>1, is the parameter that defines the shape of the convex function. So, the damage, $V(d) = \gamma\,(1-\rho)N\,\delta d^w$ .So, total payoff of the network system , $Q = \beta\rho N[(1-\theta_1-\theta_2)d^r + \theta_1] - \alpha(1-d) - \gamma\,(1-\rho)N\,\delta d^w$.....(2)

Research Methodology:

We will maximize the total expected pay off Q for different circumstances such as different parameters associated with degree of anonymity. We will validate our model implementing it on a simulated system through numerical analysis and on an existing system through empirical analysis.

Contribution:

This research will provide a guideline to design and development of traceability mechanisms. It will be helpful to create optimal tracing mechanisms to maximize the overall welfare of the network systems.

References:

Backes, M., Clark, J., Druschel, P., Kate, A., & Simeonovski, M. (2013). Introducing Accountability to Anonymity Networks. *arXiv preprint arXiv:1311.3151*.

Beimel, A., & Dolev, S. (2003). Buses for Anonymous Message Delivery. *Journal of cryptology, 16*(1).

Berthold, O., Federrath, H., & Köpsell, S. (2001). *Web MIXes: A system for anonymous and unobservable Internet access.* Paper presented at the Designing privacy enhancing technologies.

Bos, J., & den Boer, B. (1989). *Detection of disrupters in the DC protocol.* Paper presented at the Workshop on the Theory and Application of of Cryptographic Techniques.

Chaum, D. (1988). The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of cryptology, 1*(1), 65-75.

Chaum, D., & Van Heyst, E. (1991). *Group signatures.* Paper presented at the Advances in Cryptology—EUROCRYPT'91.

Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM, 24*(2), 84-90.

Diaz, C., Seys, S., Claessens, J., & Preneel, B. (2002). *Towards measuring anonymity.* Paper presented at the International Workshop on Privacy Enhancing Technologies.

Dingledine, R., Mathewson, N., & Syverson, P. (2005). Challenges in deploying low-latency anonymity (DRAFT). *Unpublished Manuscript. http://tor.eff.org/cvs/tor/doc/design-paper/challenges. pdf.*

Dodis, Y., Kiayias, A., Nicolosi, A., & Shoup, V. (2004). *Anonymous identification in ad hoc groups.* Paper presented at the Eurocrypt.

Freedman, M. J., & Morris, R. (2002). *Tarzan: A peer-to-peer anonymizing network layer.* Paper presented at the Proceedings of the 9th ACM conference on Computer and communications security.

Golle, P., & Juels, A. (2004). *Dining cryptographers revisited.* Paper presented at the Eurocrypt.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM transactions on information and system security (TISSEC), 5*(4), 438-457.

Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics, 114*(2), 793-804.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research, 24*(3), 579-595.

Kiayias, A., Tsiounis, Y., & Yung, M. (2004). *Traceable signatures.* Paper presented at the Eurocrypt.

Lee, J. K. (2015). Guest editorial: research framework for AIS grand vision of the bright ICT initiative. *MIS Quarterly, 39*(2), iii-xii.

Lee, J. K. (2016). Invited Commentary—Reflections on ICT-enabled Bright Society Research. *Information Systems Research, 27*(1), 1-5.

Parekh, S. (1996). Prospects for remailers. *First Monday, 1*(2).

Pfitzmann, A., & Köhntopp, M. (2001). *Anonymity, unobservability, and pseudonymity—a proposal for terminology.* Paper presented at the Designing privacy enhancing technologies.

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected areas in Communications, 16*(4), 482-494.

Reiter, M. K., & Rubin, A. D. (1998). Crowds: Anonymity for web transactions. *ACM transactions on information and system security (TISSEC), 1*(1), 66-92.

Ren, J., & Wu, J. (2010). Survey on anonymous communications in computer networks. *Computer Communications, 33*(4), 420-431.

Rivest, R., Shamir, A., & Tauman, Y. (2001). How to leak a secret. *Advances in Cryptology—ASIACRYPT 2001*, 552-565.

Slamanig, D., & Rass, S. (2010). *Anonymous but authorized transactions supporting selective traceability.* Paper presented at the Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on.

Von Ahn, L., Bortz, A., Hopper, N. J., & O Neill, K. (2006). *Selectively traceable anonymity.* Paper presented at the Privacy Enhancing Technologies.

Wei, J., Hu, X., & Liu, W. (2014). Traceable attribute-based signcryption. *Security and Communication Networks, 7*(12), 2302-2317.

Wright, M. A., & Kakalik, J. S. (2006). *Information security: Contemporary cases*: Jones and Bartlett Publishers, Inc.