Studying Non-intrusive Tracing in the Internet

Alina Olteanu[1], Yang Xiao[1,*], Jing Liu[1], and Thomas M. Chen[2]

[1] Dept. of Computer Science, University of Alabama, Tuscaloosa, AL 35487 USA
aolteanu@cs.ua.edu,yangxiao@ieee.org,jliu39@crimson.ua.edu
[2] School of Engineering, Swansea University, Swansea, Wales, UK SA2 8PP
t.m.chen@swansea.ac.uk

Abstract. Intruders which log-in through a series of machines when conducting an attack are hard to trace because of the complex architecture of the Internet. The thumbprinting method provides an efficient way to tracing such intruders by determining whether two connections are part of the same connection chain. Since many connections are transient, and therefore short in length, choosing the best time interval to thumbprint over can be an issue. In this paper, we provide a way to shorten the time interval used for thumbprinting. We then study some special properties of the thumbprinting function. We also study another mechanism for tracing intruders in the Internet, based on a timestamping approach of passively monitoring flows between source and destination pairs. Given a potentially suspicious source, we identify the true destination of this source. We compute the error probability of our algorithm and show that its value decreases exponentially as the observation time increases. Our simulation results show that our approach performs well.

Keywords: Security, Tracing, Thumbprinting.

1 Introduction

Constant change is perhaps one major principle that characterizes the Internet. Recent advances in technology lead to a significant growth of the Internet by factors of 10^3 and 10^6 in the backbone speed and in the number of hosts, respectively [7]. Since the public expansion of the Internet in 1990, many new challenges have surfaced; among them, operations between un-trusted end-points, more demanding applications and less sophisticated users have posed severe stress on the Internet requirements. Furthermore, the number of attacks on networked computer systems has been growing exponentially from year to year. When considering the task of tracing intruders in the Internet, we have to take into account three main challenges. First, attackers hide their origin by making use of the Internet's architecture. By using different hosts, belonging to different countries and administrative domains, to route malicious acts, intruders' actions become extremely difficult to trace back. Second, the data collected from an Internet trace is usually incomplete or has missing values. For example, different domains of Internet service providers (ISPs) may not share

* Corresponding author.

X. Zhang and D. Qiao (Eds.): QShine 2010, LNICST 74, pp. 58–74, 2011.

data due to access issues, such as in different counties. Finally, routes change frequently, packets are lost and the network latency and time to convergence can be significantly increased due to routing instability.

To deal with such problems, two tracing mechanisms exist [4]: 1) methods of keeping track of all individuals and accounting all activities, and 2) reactive tracing, in which no global accounting is attempted until a problem arises and then tracing back its source is attempted. In own view, the first mechanism is much related to network accountability and the second mechanism is much related to network forensics. Network-based tracing and host-based tracing are two main approaches for reactive tracing in connection chains. Host-based tracing involves one tracing system per network host [4], and 1) a chain of connection hosts can be known via host communications [3] or 2) revering the attack chain by breaking the hosts in the reversed order [5]. Host-based tracing schemes suffer when an extended connection crosses a host not running the system [4]. Network-based tracing has the advantage that it does not rely on hosts which can be untrusty and it does not require host participation. Instead, network-based tracing uses the invariance of connections at higher protocol layers (such as the transport layer) and based on this observation can establish whether two connections are part of the same connection chain. We study two approaches for network-based tracing. The first approach is based on the idea of a thumbprint of a connection. A thumbprint is very similar to a checksum or the computed summary of the content of a connection [2], [4]. The thumbprint summarizes the content of a connection using only a small amount of data while at the same time preserving the uniqueness of the connection. Therefore, thumbprints of related connections are similar and can lead to constructing a connection chain. However, the thumbprinting method is dependent on the duration of the connection so the time period used for thumbprinting is very important especially in the case of transient flows. In this paper, we provide a way to shorten the time interval used for thumbprinting. We study the tradeoff introduced by using such a smaller time interval and how it affects basic thumbprint properties such as sensitivity and robustness.

Since thumbprinting relies on the content of the packages and therefore can be counterattacked by encryption, we study a second mechanism for tracing intruders in the Internet, involving passively monitoring flows between source and destination pairs in the Internet, similar to [1]. This approach is based on monitoring transmission activities of nodes and does not interfere with network operations. A one-hop communication graph can be constructed by matching transmission timestamps and acknowledgements. Based on this graph, the nodes that are part of a connection chain are those who communicate at a *sufficiently high rate*.

Our approach is different from the approach in [1] in that we make fewer statistical assumptions and we use clearer, simpler derivations. In addition, by working in the Internet, we face other challenges, like the availability of only partial information and route instability mentioned above. To account for this, we assume that the information on every link is available with a certain probability. There are many related research papers in security [12-111].

The remainder of the paper is organized as follows. Section 2 presents significant work related to our problem. In Section 3 we present our results concerning minimizing the thumbprinting interval. Section 4 contains a detailed introduction to

the tracing algorithm followed by an evaluation of its consistency in terms of the error probability. We conclude the paper in Section 5.

2 Related Work

The paper [4] presents an IP traceback method based on the idea of a thumbprint. Often attacks are conducted by logging through a chain of host machines. In this way, intruders make use of the Internet architecture to hide their true origin. The thumbprint technology, which is a summary of a connection, is used to compare connections and therefore trace the source of such an attack. A thumbprint is computed for each time interval, typically a minute, of each connection [4]. Thumbprinting has the advantage that it preserves the characteristics of a connection while at the same time being cheap to compute and requiring little storage. Similar methods like checksum and message digest have two main disadvantages. Firstly, an error in the content leads to a different value being computed, and thus, these methods are not robust. Secondly, they are not additive, i.e., two successive values cannot be combined to provide a new value for a longer interval. Other compression schemes are by far costier than thumbprinting in terms of storage space.

As the thumbprinting method is dependent on the duration of the connection, it is of importance to shorten the time interval used for thumbprinting, especially in the case of transient flows. This is the purpose of our derivation from section 3.

However, fingerprinting techniques are vulnerable and may not be of interest when the attacker uses encryption at every hop in the chain. To deal with such kind of problems, techniques based on packet timing information are more suitable.

The paper [1] presents a mechanism for tracing intruders in anonymous MANETs, based on passively monitoring flows between source and destination pairs. The algorithm is concerned with tracing the destination of a certain source, considered suspicious according to a higher layer intrusion detection protocol. Because anonymity of nodes in the MANET is assumed, and the monitoring is done in a non-intrusive way, this research only considers the timestamps of packets on adjacent links, and based on this, establishes causal relationships between packets. A graph is used to model the communications among nodes and based on traffic analysis and information carried in the packets, the graph is partitioned into two parts, one containing the set of possible destinations, and one with which the source does not communicate. The assumptions that are made are related to the distribution of traffic: the transmission activities on each link are assumed to follow a Poisson process. In addition, the rate of the flow to be traced must be sufficiently high, and the duration of the observation must be long enough. Therefore, the method will not work for low-rate flows, or for transient flows.

Much like [1], we focus on tracing flows between pairs (source, destination), in the Internet this time. Unlike [1], we assume differences in data due to propagation delays, skew of clocks during observation at multiple nodes at the same time and data missing from observations, or observed erroneously. We account for this by using a certain probability with which information is available on every link. In addition, we make fewer assumptions about the rate of the Poisson process and the calculations are significantly simplified.

3 Thumbprinting

The thumbprinting approach is based on the fact that, at higher protocol layers, the content of a connection is invariant at all points of the chain. The thumbprint summarizes the content of the connection using only a small amount of data while at the same time preserving the uniqueness of the connection. We first define the terminology and then present a method for shortening the time interval used for thumbprinting and some interesting properties of the thumbprint function.

3.1 Algorithm

A thumbprint is a function of a connection which preserves the unique characteristics of the connection. We use the notations and definition of a thumbprint from [4]. Consider a sequence of transmitted characters $a_1, a_2, \ldots, a_L$ to thumbprint. Consider also the function $\alpha : \mathcal{A} \to \mathbf{R}^K$, which takes a character and returns a vector of K real numbers. Let $\alpha_k(\bullet)$ denote the *k*-th component of the function. Here K is a short fixed number representing the number of thumbprint components. If we consider L to be the period of a connection, we can associate frequencies $\overline{f} = (f_1, f_2, ..., f_L)$ to our character sequence. Then the thumbprint is defined as [4]:

$$T_k = \sum_{i=1}^{L} \alpha_k(a_i) f_i, \qquad k \in \{1,2,...,K\}. \tag{1}$$

The thumbprint is thus a linear combination of the frequencies of characters and their corresponding weights. T_k represents the k th component of the K-dimensional thumbprint vector.

Each thumbprint component $T_k(C,t)$, is a function of a specific connection *C* and the time interval t, in which the thumbprints have been computed. From [4], we also know that the comparison of two sets of thumbprints, $T_k(C,t)$ and $T_k(C',t)$, $k \in \{1,2,...,K\}$, for two different connections C and C', is given by the following formula:

$$\delta_t(C,C') = \log\left(\prod_{k=1}^{K} |T_k(C',t) - T_k(C,t)|\right). \tag{2}$$

δ_t represents the logarithm of the product of component differences for two thumbprints in a specific time interval t. A large absolute value of δ_t implies that the two connections are related, while a small absolute value suggests independent connections.

3.2 Minimizing the Thumbprinting Interval

In this section, based on the results in [4], we try to find the best period of time, T, to thumbprint over. The length of time divisions for the experiments in [4] is 1 time

unit. However, many connections in the Internet are transient, and therefore short in length; in these cases a shorted thumbprinting interval is needed.

We start with the thumbprint function given by (1) and in addition, we account for the time in which the thumbprint has been computed. This gives us the following function:

$$\sum_{a,t} \alpha_k(a,t) f(a,t) . \tag{3}$$

We will use the function given by (3) above as our thumbprinting function.

Following, we do the changes of variable $a = Ly$ and $t = T\tau$. This transforms our time interval from $[0,T]$ to $[0,1]$ and the samples from every time unit to every $1/T$ time units. It can be seen that the thumbprinting function in (3) can be approximated be the following integral:

$$\iint_{[0,L]\times[0,T]} f(a,t)\alpha_k(a,t)\,da\,dt . \tag{4}$$

We have:

$$\begin{aligned}
\iint_{[0,L]\times[0,T]} f(a,t)\alpha_k(a,t)\,da\,dt &\approx LT \sum_{a,t} \alpha_k(a,t) f(a,t) \Big/ (LT) \\
&\overset{\substack{a=Ly \\ t=T\tau}}{=} LT \sum_{y,\tau} \alpha_k(Ly,T\tau) f(Ly,T\tau) \Big/ (LT) \\
&= LT \iint_{[0,1]\times[0,1]} f(Ly,T\tau)\alpha_k(Ly,T\tau)\,dy\,d\tau
\end{aligned}$$

The time period has become interval $[0,1]$.

Since thumbprinting over a one unit time interval may not provide the best results, we further provide a way to transform interval $[0,1]$ into an arbitrary time interval $[p,q]$. In the following calculus, we use $y = (u-m)/(n-m)$ and $\tau = (v-p)/(q-p)$. We have:

$$\begin{aligned}
&LT \iint_{[0,1]\times[0,1]} f(Ly,T\tau)\alpha_k(Ly,T\tau)\,dy\,d\tau \\
&= LT \iint_{[m,n]\times[p,q]} f(L(u-m)/(n-m), T(v-p)/(q-p)) \cdot \\
&\alpha_k(L(u-m)/(n-m), T(v-p)/(q-p)) \left|\frac{\partial(y,\tau)}{\partial(u,v)}\right| du\,dv \\
&= LT \iint_{[m,n]\times[p,q]} \frac{f(L(u-m)/(n-m), T(v-p)/(q-p))}{(n-m)(q-p)} \cdot \\
&\frac{\alpha_k(L(u-m)/(n-m), T(v-p)/(q-p))}{(n-m)(q-p)} du\,dv .
\end{aligned} \tag{5}$$

The time period has become interval $[p,q]$. This interval can be suitably chosen to accommodate connections with low/high data rates and transient connections in order to give the best performance possible under different scenarios.

3.3 Properties of the Thumbprinting Function

In the following, we describe a way to easily compute the value of the integral given by (4) by the use of the mean value theorem [10]. We further study some special properties of the thumbprinting function.

Consider the right-hand side of equation (5).

Let us choose u_0 and v_0 to be the points toward which we concentrate intervals $[m,n]$ and $[p,q]$, respectively. By making $m,n \to u_0$ and $p,q \to v_0$ (i.e. $n-m \to 0$ and $q-p \to 0$), we have:

$$\iint_{[0,L]\times[0,T]} f(a,t)\alpha_k(a,t)dadt = LT \iint_{[0,1]\times[0,1]} f(Ly,T\tau)\alpha_k(Ly,T\tau)dyd\tau$$

$$= \frac{LT \iint_{[m,n]\times[p,q]} f\left(L\frac{u-m}{n-m},T\frac{v-p}{q-p}\right)\alpha_k\left(L\frac{u-m}{n-m},T\frac{v-p}{q-p}\right)dudv}{(n-m)(q-p)}$$

$$= LTf\left(L\frac{u_0-m}{n-m},T\frac{v_0-p}{q-p}\right)\alpha_k\left(L\frac{u_0-m}{n-m},T\frac{v_0-p}{q-p}\right)$$

$$= LT\,h\left(L\frac{u_0-m}{n-m},T\frac{v_0-p}{q-p}\right). \tag{6}$$

We have considered $h = f\alpha_k$ where h is a continuous function. Let $I = LT \iint_{[0,1]\times[0,1]} f(Ly,T\tau)\alpha_k(Ly,T\tau)dyd\tau$. If h is a C^n function, $n \geq 1$, then the set of points $\gamma = \{(u_0,v_0); I = LT(f\alpha_k)(u_0,v_0)\}$ represents a C^n curve which, according to the Implicit Function Theorem [6], ensures the existence of a function ϕ such that $v_0 = \phi(u_0), u_0 \in J$, where J is an interval included in $[m,n]$. This way we can express one of the variables u_0, v_0 as a function of the other.

The last equality in (6) is true for any $(u_0,v_0) \in [m,n]\times[p,q]$ on the curve γ.

We have thus shown that the value of the integral in (4) can be found by computing the value of the function $f\alpha_k$ in a certain point, in fact, in any point belonging to curve γ.

Furthermore, if we choose:

$$n = m+\varepsilon, u_0 = m+\varepsilon t, 0<t<1, q = p+\delta,$$
$$\phi(u_0) = p+\lambda(t)\delta,$$

we have:

$$I = LT(f\alpha_k)\left(L\frac{\varepsilon t}{\varepsilon}, T\frac{\lambda(t)\delta}{\delta}\right)$$
$$= LTf(Lt, T\lambda(t))\alpha_k(Lt, T\lambda(t)), t \in J.$$

We have shown that on the curve $\gamma = \{(u_0, \phi(u_0)); u_0 \in J\}$ we have:

$$\alpha_k(u_0, \phi(u_0)) = \frac{I}{LTf(u_0, \phi(u_0))} = const..$$

In order to determine the constant, it is sufficient to compute I. Therefore α_k and f are inversely proportional on curve γ.

Following we introduce an abstraction of the derivations used above by the use of a mean value operator. The use of this operator generalizes the procedure of associating the function h with its mean value. Such an operator can be defined as follows:

$$T(h)(0) = h(0) = \lim_{x\downarrow 0}\frac{\int_0^x h(t)dt}{x} = \lim_{x\downarrow 0} T(h)(x), h \in C([0,b])$$

, for one variable and

$$T(h)(0,y) = \lim_{x\downarrow 0}\frac{\iint_{[0,x]\times[0,y]} h(t_1,t_2)dt_1dt_2}{xy} = \frac{\int_0^y h(0,t_2)dt_2}{y},\ y \neq 0$$

,

$$T(h)(x,0) = \frac{\int_0^x h(t_1,0)dt_1}{x}$$

,

$T(h)(0,0) = h(0,0)$, for two variables.

Operator T associates function h with another function that is equal in every point x to the mean value of function h, on interval $[0,x]$.

4 Tracing the True Destination of a Source

Since many attackers use encryption at every hop in the chain, the same packet will have different content on every link and fingerprinting techniques are not appropriate in this case. Therefore, we present a mechanism from paper [1], for tracing intruders in anonymous MANETs, based on using timestamps of transmission to passively monitor flows between source and destination pairs. Such an approach can be implemented by using sensors equipped with energy detectors to measure transmission timestamps and distributing them on the field of interest. All measurements are fused and processed by a centralized monitor at a fusion center.

We first introduce the algorithm and its main features and then analyze the algorithm in terms of the error probability of detecting the true destination of a source. We show that the error probability decays exponentially with the observation time and also prove a similar result when the number of observed graphs goes to infinity.

4.1 Algorithm

Our derivation is based on a variation of the tracing algorithm from [1]. In [1], the approach for tracing the destination of a source is twofold. First, based on the transmission activities on adjacent links, it can be established whether these links are part of the same flow. Then, a set of possible destinations is computed. Second, the intersection method is used: using the changes in topology, some nodes are eliminated, leading to a smaller set of possible destinations.

It is assumed that the transmission activities on each link follow a Poisson process $\boldsymbol{S}$ and its realization is denoted by $\boldsymbol{s}$. Therefore a realization of the transmission timestamps of data packets on link 1 will be $\boldsymbol{s}_1 = (s_1(1), s_1(2), s_1(2), \ldots)$. Here uppercase letters denote random variables, lowercase letters realizations, boldface letters vectors and plain letters scalars.

Following, we briefly introduce the idea behind the traffic analysis method and the intersection of different topologies method from [1].

For traffic analysis, consider two realizations $(\boldsymbol{s}_1, \boldsymbol{s}_2)$ of the transmission activities (timestamps) on two adjacent links. Let m and n be the indices of the current timestamps on links 1 and 2, respectively ($0 \le m \le \delta_1, 0 \le n \le \delta_2$). These sets of timestamps are matched against each other sequentially by assessing the difference $s_2(n) - s_1(m)$. If $s_2(n) - s_1(m) \le \Delta$, where Δ is a predefined maximum delay, and if at the same time this difference is nonnegative, then the two timestamps match. The matching timestamps from the two connections form a pair of sequences $(\boldsymbol{f}_1, \boldsymbol{f}_2)$. Given the number of matching timestamps on a link, the empirical rate on that link can be now estimated. Specifically, if $\boldsymbol{f}_i$ contains $|F_i|$ timestamps over time T, then the empirical rate is $|F_i|/T$.

Let $\tau \ge 0$ be a given rate. Given a graph sourced at j, by repeatedly applying the matching timestamps algorithm for pairs of adjacent links, and selecting only the flows which support rate at least τ, a sub-graph of the initial graph can be obtained. This new graph will contain only nodes to which node j can talk at a rate higher or equal to τ. The method, called Trace Destination (TD), is applied for the graph sourced at O and a set of possible destinations is obtained. However, node O can be only a relay node for some of these flows. In order to trace down the flows that are going through O, and did not originate in O, TD is applied for all immediate predecessors of O and the corresponding graphs sourced at these nodes. The set of obtained destinations is then subtracted from the previously obtained set of destinations of O.

To speed up the algorithm's convergence, a second feature is used, that of the changing topology. Basically, the algorithm TD is applied for every communication graph that is observed. For each observed graph, a set of destinations if obtained. The final set of possible destinations is the intersection over all sets from all observed graphs. Out of this final set, the node which appears most frequently in all topologies is selected. If there are more possible destinations with the same number of appearances across all different topologies, then one node is selected at random.

4.2 Analysis

Our tracing algorithm is a variation of the one from section 4.1. in which we account for the lack of information in the observations. We model the lack of information by considering that the information on each link is available with a certain probability. We denote this probability by $p_k, k \in \{1,2,...,K\}$, where K is the number of links in the considered path. In this modified algorithm, only flows which support rate at least $r_k / p_k \geq \tau$ are selected from the initial graph.

It is interesting now to study how well our variation of the algorithm from section 4.1 converges. We thus study the probability P_e with which the algorithm finds the destination erroneously (called error probability) and analyze its asymptotic behavior over time T. We would like to mention that even though we assume Poisson distribution of packets on a link for our specific derivation, the algorithm and analysis here can be applied to different types of traffic.

Our error probability derivation is also inspired from [1]. Assume that the transmission activities on each link follow a Poisson process of rate $R < 1$. It is well-known that the Poisson distribution of the number of events in a time interval $(t, t+t']$ is given by the following relation:

$$P[(m_{t+t'} - m_t) = n] = \frac{e^{-Rt'}(Rt')^n}{n!},\ n = 0,1,...,$$

where $m_{t+t'} - m_t$ represents the number of events in time interval $(t, t+t']$ (see for example [11]).

Let O be the source whose destination we are trying to find and let θ be the true destination of O. We denote the destination rendered by our algorithm with $\hat{\theta}$. Following, we derive the probability that $\hat{\theta}$ is not the true destination of O. Let n_k be the number of timestamps taken in time interval (m_k, m_{k+1}), corresponding to link $(k, k+1)$. We denote the total number of timestamps taken for one flow by N_1.

By definition,

$$P_e := P_e(TD) = P(\theta \neq \hat{\theta})$$
$$= P(\theta \text{ is not correctly detected by algorithm TD}).$$

According to [1], Theorem 4.4, the fact that the algorithm does not find the true destination is due to one of three possibilities:

A) θ is not detected because the empirical rate along the path from O to θ is less than τ; we will denote the probability of this event by $P(A)$;

B) θ is mistaken for a relay node because there is some node j which is a successor of θ, for which the empirical rate from O to j is greater than τ. We denote the probability of this event by $P(B)$;

C) θ is incorrectly detected as being the destination of a flow originating in some predecessor of O. We denote the probability of this event by $P(C)$;

In both *B*) and *C*) cases, all the empirical probabilities are greater or equal to τ. So

$$P_e \le P(A) + P(B) + P(C) \tag{7}$$

Following we establish an upper bound for $P(B)$. The empirical rate on the path from O to j is given by $N_1(T)/T$.

$P(B) \le Ke^{-\frac{N_1(T)}{T}T}$,

where K is a constant related to $\text{card}(G)$.

$\frac{N_1(T)}{T} \ge r_k \ge p_k\tau$, for all k

$$\Rightarrow \frac{N_1(T)}{T} \ge \tau \frac{\sum p_k}{\#\text{ of links}} = \tau\tilde{p}.$$

Using the fact that $-\frac{N_1(T)}{T} \le -\tau\tilde{p}$, we obtain:

$P(B) \le Ke^{-N_1(T)} \le Ke^{-\tau T\tilde{p}}$.

Similarly, for $P(C)$ we have: $P(C) \le Ke^{-\tau T\hat{p}}$.

For $P(A)$, the assumption is that there is at least one link along the path from O to θ with empirical rate less than τ. Suppose j_0 is the first node on the path connected to a link with rate smaller than τ. Therefore all links along the path up to j_0 have rate greater or equal to τ. Let N_1 be the total number of timestamps taken during the observation period T. We have:

We denote by λ the rate of the Poisson process defined by the recorded timestamps. Then the rate on an arbitrary interval $[m_k, m_{k+1}]$ is $\lambda(m_{k+1} - m_k)$.

$$P(A) \le \prod_{k=0}^{j_0-1} \frac{[r_k(m_{k+1}-m_k)]^{n_k}}{n_k!} e^{-r_k(m_{k+1}-m_k)} \prod_{k' \in N^+(j_0)} e^{-r_{k'}(m_{k'+1}-m_{k'})}.$$

$N^+(j_0)$ denotes all successors of node j_0 on links with rate at least R. Notice that in the first product $r_k \ge p_k\tau$ for all k, while all $r_{k'}$ from the second product are less than $p_k\tau$. On the other hand, $r_{k'} \ge (N_1(T) - N(j_0))/(T - m(j_0))$. We thus have:

$$P(A) \le C_{j_0} \exp[-\tau(\sum_{k=0}^{j_0-1} p_k(m_{k+1}-m_k)]\exp[-\frac{N_1(T)-N(j_0)}{T-m(j_0)}$$

$$(T-m(j_0))] = C_{j_0} \exp(N(j_0)\exp[-\tau(\sum_{k=0}^{j_0-1} p_k(m_{k+1}-m_k)]$$

$$\exp(-N_1(T)) = K_1(j_0,\tau)\exp(-N_1(T))$$

$$= K_1(j_0,\tau)\exp(-T\rho(T)),$$

where

$$C(j_0) = \prod_{k=0}^{j_0-1} \frac{r_k (m_{k+1} - m_k)^{n_k}}{n_k!} \text{ and } K'(j_0, \tau) = C(j_0) e^{N(j_0) - \tau m_{j_0}}.$$

Here we let $\rho = \lim_{T \to \infty} N_1(T)/T > 0$.

Therefore $P(A)$ decreases exponentially with the observation time.

Using equation (7), we now have:

$$\begin{aligned} P_e &\le K'(j_0, \tau) e^{-\rho T} + \text{card}(\text{G}) e^{-\tau \tilde{p}} + \text{card}(\text{G}) e^{-\tau \hat{p}} \\ &= e^{-T\tau \min\{\tilde{p}, \hat{p}\}} (K'(j_0, \tau) + 2K). \end{aligned}$$

We can now investigate the convergence rate of our algorithm by showing the asymptotic decay rate of the error probability as time increases.

By logarithming the above inequality we obtain:

$$\lim_{T \to \infty} (-\ln P_e / T) \ge \tau \min(\tilde{p}, \hat{p}) > 0.$$

Compared to the upper bound for the error of algorithm TD, which is τ (corresponding to the case $p_k = 1$ for all k), the modified algorithm has upper bound: $\tau \min(\tilde{p}, \hat{p})$.

The minimum is strictly positive as the minimum of a finite number of strictly positive values.

We can see that the algorithm has an exponential convergence rate.

5 Conclusion

We provided a way to shorten the time interval used for thumbprinting and tune it suitably depending on network conditions. We have found interesting properties of the thumbprinting function using the mean value and provided a general method to compute the value of the function. The method works for any function that satisfies certain properties. We have also studied another mechanism for tracing intruders in the Internet, based on an approach of passively monitoring flows between source and destination pairs. We computed the error probability of our algorithm and show that its value decreases exponentially as the observation time increases.

Acknowledgments. This work is supported in part by the US National Science Foundation (NSF) under the grant numbers CCF-0829827, CNS-0716211, and CNS-0737325.

References

1. He, T., Wong, H.Y., Lee, K.-W.: Traffic Analysis in Anonymous MANETs. In: Proc. IEEE MILCOM, San Diego, pp. 1–7 (2008)
2. Heberlein, L.T., Levitt, K., Mukherjee, B.: Internetwork Security Monitor: An Intrusion-Detection System for Large Scale Networks. In: Proc. 15th National Computer Security Conference, pp. 262–271 (1992)

3. Tae, H., Kim, H.L., Seo, Y.M., Choe, G., Min, S.L., Kim, C.S.: Caller Identification System in the Internet Environment. In: Proc. of 4th USENIX Security Symposium, pp. 69–78 (1993)
4. Staniford-Chen, S., Heberlein, L.T.: Holding Intruders Accountable on the Internet. In: Proc. the 1995 IEEE Symposium on Security and Privacy, Oakland, CA, pp. 39–49 (1995)
5. Wadell, S.: Private Communication (1994)
6. Implicit Function Theorem, http://en.wikipedia.org/wiki/Implicit_function_theorem
7. Internet, http://en.wikipedia.org/wiki/Internet
8. Jensen's Inequality, http://en.wikipedia.org/wiki/Jensen'sinequality
9. Least Squares, http://en.wikipedia.org/wiki/Least_squares
10. Mean Value Theorem, http://en.wikipedia.org/wiki/Mean_value_theorem
11. Poisson Process, http://en.wikipedia.org/wiki/Poisson_proce
12. Xiao, Y.: Editorial. International Journal of Security and Networks 1(1/2), 1 (2006)
13. Shehab, M., Bertino, E., Ghafoor, A.: Workflow Authorization in Mediator-free Environments. International Journal of Security and Networks 1(1/2), 2–12 (2006)
14. Jung, E., Gouda, M.G.: Vulnerability Analysis of Certificate Graphs. International Journal of Security and Networks 1(1/2), 13–23 (2006)
15. Kiayias, A., Yung, M.: Secure Scalable Group Signature with Dynamic Joins and Separable Authorities. International Journal of Security and Networks 1(1/2), 24–45 (2006)
16. Franklin, M.: A Survey of Key Evolving Cryptosystems. International Journal of Security and Networks 1(1/2), 46–53 (2006)
17. Hamadeh, I., Kesidis, G.: A Taxonomy of Internet Traceback. International Journal of Security and Networks 1(1/2), 54–61 (2006)
18. Jhumka, A., Freiling, F., Fetzer, C., Suri, N.: An Approach to Synthesize Safe Systems. International Journal of Security and Networks 1(1/2), 62–74 (2006)
19. Evans, J.B., Wang, W., Ewy, B.J.: Wireless Networking Security: Open Issues in Trust, Management, Interoperation and Measurement. International Journal of Security and Networks 1(1/2), 84–94 (2006)
20. Englund, H., Johansson, T.: Three Ways to Mount Distinguishing Attacks on Irregularly Clocked Stream Ciphers. International Journal of Security and Networks 1(1/2), 95–102 (2006)
21. Zhu, B., Jajodia, S., Kankanhalli, M.S.: Building Trust in Peer-to-Peer Systems: A Review. International Journal of Security and Networks 1(1/2), 103–112 (2006)
22. Ramkumar, M., Memon, N.: Secure Collaborations Over Message Boards. International Journal of Security and Networks 1(1/2), 113–124 (2006)
23. Xiao, Y., Jia, X., Sun, B., Du, X.: Editorial: Security Issues on Sensor Networks. International Journal of Security and Networks 1(3/4), 125–126 (2006)
24. Wang, H., Sheng, B., Li, Q.: Elliptic Curve Cryptography-based Access Control. International Journal of Security and Networks 1(3/4), 127–137 (2006)
25. Zheng, J., Li, J., Lee, M.J., Anshel, M.: A Lightweight Encryption and Authentication Scheme for Wireless Sensor Networks. International Journal of Security and Networks 2006 1(3/4), 138–146 (2006)
26. Al-Karaki, J.N.: Analysis of Routing Security-Energy Trade-offs in Wireless Sensor Networks. International Journal of Security and Networks 1(3/4), 147–157 (2006)

27. Araz, O., Qi, H.: Load-balanced Key Establishment Methodologies in Wireless Sensor Networks. International Journal of Security and Networks 1(3/4), 158–166 (2006)
28. Deng, J., Han, R., Mishra, S.: Limiting DoS Attacks During Multihop Data Delivery in Wireless Sensor Networks. International Journal of Security and Networks 1(3/4), 167–178 (2006)
29. Hwu, J., Hsu, S., Lin, Y.-B., Chen, R.: End-to-End Security Mechanisms for SMS. International Journal of Security and Networks 1(3/4), 177–183 (2006)
30. Wang, X.: The Loop Fallacy and Deterministic Serialisation in Tracing Intrusion Connections through Stepping Stones. International Journal of Security and Networks 1(3/4), 184–197 (2006)
31. Jiang, Y., Lin, C., Shi, M., Shen, X.: A Self-Encryption Authentication Protocol for Teleconference Services. International Journal of Security and Networks 1(3/4), 198–205 (2006)
32. Owens, S.F., Levary, R.R.: An Adaptive Expert System Approach for Intrusion Detection. International Journal of Security and Networks 1(3/4), 206–217 (2006)
33. Chen, Y., Susilo, W., Mu, Y.: Convertible Identity-based Anonymous Designated Ring Signatures. International Journal of Security and Networks 1(3/4), 218–225 (2006)
34. Teo, J., Tan, C., Ng, J.: Low-power Authenticated Group Key Agreement for Heterogeneous Wireless Networks. International Journal of Security and Networks 1(3/4), 226–236 (2006)
35. Tan, C.: A New Signature Scheme without Random Oracles. International Journal of Security and Networks 1(3/4), 237–242 (2006)
36. Liu, Y., Comaniciu, C., Man, H.: Modelling Misbehaviour in Ad Hoc Networks: A Game Theoretic Approach for Intrusion Detection. International Journal of Security and Networks 1(3/4), 243–254 (2006)
37. Karyotis, V., Papavassiliou, S., Grammatikou, M., Maglaris, V.: A Novel Framework for Mobile Attack Strategy Modelling and Vulnerability Analysis in Wireless Ad Hoc Networks. International Journal of Security and Networks 1(3/4), 255–265 (2006)
38. Chen, H., Guizani, M.: Editorial. International Journal of Security and Networks 2(1/2), 1–2 (2007)
39. Li, R., Li, J., Chen, H.: DKMS: Distributed Hierarchical Access Control for Multimedia Networks. International Journal of Security and Networks 2(1/2), 3–10 (2007)
40. Sakarindr, P., Ansari, N.: Adaptive trust-based anonymous network. International Journal of Security and Networks 2(1/2), 11–26 (2007)
41. Malaney, R.A.: Securing Wi-Fi Networks with Position Verification: Extended Version. International Journal of Security and Networks 2(1/2), 27–36 (2007)
42. Sun, F., Shayman, M.A.: On Pairwise Connectivity of Wireless Multihop Networks. International Journal of Security and Networks 2(1/2), 37–49 (2007)
43. Erdogan, O., Cao, P.: Hash-AV: Fast Virus Signature Scanning by Cache-Resident Filters. International Journal of Security and Networks 2(1/2), 50–59 (2007)
44. Rabinovich, P., Simon, R.: Secure Message Delivery in Publish/Subscribe Networks using Overlay Multicast. International Journal of Security and Networks 2(1/2), 60–70 (2007)
45. Chen, Z., Ji, C.: Optimal worm-scanning method using vulnerable-host distributions. International Journal of Security and Networks 2(1/2), 71–80 (2007)
46. Pan, J., Cai, L., Shen, X.: Vulnerabilities in Distance-indexed IP Traceback Schemes. International Journal of Security and Networks 2(1/2), 81–94 (2007)

47. Korkmaz, T., Gong, C., Sarac, K., Dykes, S.G.: 8 Single Packet IP Traceback in AS-Level Partial Deployment Scenario. International Journal of Security and Networks 2(1/2), 95–108 (2007)
48. Ling, H., Znati, T.: End-to-end Pairwise Key Establishment using Node Disjoint Secure Paths in Wireless Sensor Networks. International Journal of Security and Networks 2(1/2), 109–121 (2007)
49. Artan, N.S., Chao, H.J.: Design and Analysis of A Multipacket Signature Detection System. International Journal of Security and Networks 2(1/2), 122–136 (2007)
50. Zhu, Y., Fu, X., Bettati, R., Zhao, W.: Analysis of Flow-correlation Attacks in Anonymity Network. International Journal of Security and Networks 2(1/2), 137–153 (2007)
51. Gu, Q., Liu, P., Chu, C., Zhu, S.: Defence Against Packet Injection in Ad Hoc Networks. International Journal of Security and Networks 2(1/2), 154–169 (2007)
52. Mu, Y., Chen, L., Chen, X., Gong, G., Lee, P., Miyaji, A., Pieprzyk, J., Pointcheval, D., Takagi, T., Traore, J., Seberry, J., Susilo, W., Wang, H., Zhang, F.: Editorial. International Journal of Security and Networks 2(3/4), 171–174 (2007)
53. Tartary, C., Wang, H.: Efficient Multicast Stream Authentication for the Fully Adversarial Network Model. International Journal of Security and Networks 2(3/4), 175–191 (2007)
54. Bhaskar, R., Herranz, J., Laguillaumie, F.: Aggregate Designated Verifier Signatures and Application to Secure Routing. International Journal of Security and Networks 2(3/4), 192–201 (2007)
55. Hsu, H., Zhu, S., Hurson, A.R.: LIP: A Lightweight Interlayer protocol for Preventing Packet Injection Attacks in Mobile Ad Hoc Network. International Journal of Security and Networks 2(3/4), 202–215 (2007)
56. Oliveira, L.B., Wong, H., Loureiro, A.A.F., Dahab, R.: On the Design of Secure Protocols for Hierarchical Sensor Networks. International Journal of Security and Networks 2(3/4), 216–227 (2007)
57. Michail, H.E., Panagiotakopoulos, G.A., Thanasoulis, V.N., Kakarountas, A.P., Goutis, C.E.: Server Side Hashing Core Exceeding 3 Gbps of Throughput. International Journal of Security and Networks 2(3/4), 228–238 (2007)
58. Hoeper, K., Gong, G.: Preventing or Utilizing Key Escrow in Identity-based Schemes Employed in Mobile Ad Hoc Networks. International Journal of Security and Networks 2(3/4), 239–250 (2007)
59. Cheng, Z., Chen, L.: On Security Proof of McCullagh–Barreto's Key Agreement Protocol and Its Variants. International Journal of Security and Networks 2(3/4), 251–259 (2007)
60. Finnigin, K.M., Mullins, B.E., Raines, R.A., Potoczny, H.B.: Cryptanalysis of An Elliptic Curve Cryptosystem for Wireless Sensor Networks. International Journal of Security and Networks 2(3/4), 260–271 (2007)
61. Huang, D.: Pseudonym-based Cryptography for Anonymous Communications in Mobile Ad Hoc Networks. International Journal of Security and Networks 2(3/4), 272–283 (2007)
62. Abdalla, M., Bresson, E., Chevassut, O., Moller, B., Pointcheval, D.: Strong Password-based Authentication in TLS Using the Three-party Group Diffie–Hellman Protocol. International Journal of Security and Networks 2(3/4), 284–296 (2007)
63. Kotzanikolaou, P., Vergados, D.D., Stergiou, G., Magkos, E.: Multilayer Key Establishment for Large-scale Sensor Networks. International Journal of Security and Networks 3(1), 1–9 (2008)

64. Wang, W., Kong, J., Bhargava, B., Gerla, M.: Visualization of Wormholes in Underwater Sensor Networks: A Distributed Approach. International Journal of Security and Networks 3(1), 10–23 (2008)
65. Scheirer, W., Chuah, M.: Syntax vs. Semantics: Competing Approaches to Dynamic Network Intrusion Detection. International Journal of Security and Networks 3(1), 24–35 (2008)
66. Burt, A.L., Darschewski, M., Ray, I., Thurimella, R., Wu, H.: Origins: An Approach to Trace Fast Spreading Worms to Their Roots. International Journal of Security and Networks 3(1), 36–46 (2008)
67. Zou, X., Karandikar, Y.: A Novel Conference Key Management Solution for Secure Dynamic Conferencing. International Journal of Security and Networks 3(1), 47–53 (2008)
68. Asadpour, M., Sattarzadeh, B., Movaghar, A.: Anonymous Authentication Protocol for GSM Networks. International Journal of Security and Networks 3(1), 54–62 (2008)
69. Hu, F., Rughoonundon, A., Celentano, L.: Towards a Realistic Testbed for Wireless Network Reliability and Security Performance Studies. International Journal of Security and Networks 3(1), 63–77 (2008)
70. Memon, N., Goel, R.: Editorial. International Journal of Security and Networks 3(2), 79 (2008)
71. Ray, I., Poolsappasit, N.: Using Mobile Ad Hoc Networks to Acquire Digital Evidence from Remote Autonomous Agents. International Journal of Security and Networks 3(2), 80–94 (2008)
72. Kilpatrick, T., Gonzalez, J., Chandia, R., Papa, M., Shenoi, S.: Forensic Analysis of SCADA Systems and Networks. International Journal of Security and Networks 3(2), 95–102 (2008)
73. Cronin, E., Sherr, M., Blaze, M.: On the (Un)reliability of Eavesdropping. International Journal of Security and Networks 3(2), 103–113 (2008)
74. Okolica, J.S., Peterson, G.L., Mills, R.F.: Using PLSI-U to Detect Insider Threats by Datamining E-mail. International Journal of Security and Networks 3(2), 114–121 (2008)
75. Lin, X., Ling, X., Zhu, H., Ho, P., Shen, X.: A Novel Localised Authentication Scheme in IEEE 802.11 based Wireless Mesh Networks. International Journal of Security and Networks 3(2), 122–132 (2008)
76. Challal, Y., Gharout, S., Bouabdallah, A., Bettahar, H.: Adaptive Clustering for Scalable Key Management in Dynamic Group Communications. International Journal of Security and Networks 3(2), 133–146 (2008)
77. Xu, H., Ayachit, M., Reddyreddy, A.: Formal Modelling and Analysis of XML Firewall for Service-oriented Systems. International Journal of Security and Networks 3(3), 147–160 (2008)
78. Bouhoula, A., Trabelsi, Z., Barka, E., Benelbahri, M.: Firewall Filtering Rules Analysis for Anomalies Detection. International Journal of Security and Networks 3(3), 161–172 (2008)
79. Li, F., Srinivasan, A., Wu, J.: PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks. International Journal of Security and Networks 3(3), 173–182 (2008)
80. Ma, X., Cheng, X.: Verifying Security Protocols by Knowledge Analysis. International Journal of Security and Networks 3(3), 183–192 (2008)

81. Uphoff, B., Wong, J.S.: An Agent-based Framework for Intrusion Detection Alert Verification and Event Correlation. International Journal of Security and Networks 3(3), 193–200 (2008)
82. Tripathy, S., Nandi, S.: Secure User-identification and Key Distribution Scheme Preserving Anonymity. International Journal of Security and Networks 3(3), 201–205 (2008)
83. Li, F., Xin, X., Hu, Y.: ID-based Threshold Proxy Signcryption Scheme from Bilinear Pairings. International Journal of Security and Networks 3(3), 206–215 (2008)
84. Ma, L., Teymorian, A.Y., Xing, K., Du, D.: An One-way Function Based Framework for Pairwise Key Establishment in Sensor Networks. International Journal of Security and Networks 3(4), 217–225 (2008)
85. Srinivasan, A., Li, F., Wu, J., Li, M.: Clique-based Group Key Assignment in Wireless Sensor Networks. International Journal of Security and Networks 3(4), 226–239 (2008)
86. Hsieh, C., Chen, J., Lin, Y.-B., Chen, K., Liao, H., Liang, C.: NTP-DownloadT: A Conformance Test Tool for Secured Mobile Download Services. International Journal of Security and Networks 3(4), 240–249 (2008)
87. Sadowitz, M., Latifi, S., Walker, D.: An Iris and Retina Multimodal Biometric System. International Journal of Security and Networks 3(4), 250–257 (2008)
88. Kandikattu, R., Jacob, L.: Secure Hybrid Routing with Micro/Macro-mobility Handoff Mechanisms for Urban Wireless Mesh Networks. International Journal of Security and Networks 3(4), 258–274 (2008)
89. Mayrhofer, R., Nyberg, K., Kindberg, T.: Foreword. International Journal of Security and Networks 4(1/2), 1–3 (2009)
90. Scannell, A., Varshavsky, A., LaMarca, A., De Lara, E.: Proximity-based Authentication of Mobile Devices. International Journal of Security and Networks 4(1/2), 4–16 (2009)
91. Soriente, C., Tsudik, G., Uzun, E.: Secure Pairing of Interface Constrained Devices. International Journal of Security and Networks 4(1/2), 17–26 (2009)
92. Buhan, I., Boom, B., Doumen, J., Hartel, P.H., Veldhuis, R.N.J.: Secure Pairing with Biometrics. International Journal of Security and Networks 4(1/2), 27–42 (2009)
93. McCune, J.M., Perrig, A., Reiter, M.K.: Seeing-Is-Believing: Using Camera Phones for Human-verifiable Authentication. International Journal of Security and Networks 4(1/2), 43–56 (2009)
94. Goodrich, M.T., Sirivianos, M., Solis, J., Soriente, C., Tsudik, G., Uzun, E.: Using Audio in Secure Device Pairing. International Journal of Security and Networks 4(1/2), 57–68 (2009)
95. Laur, S., Pasini, S.: User-aided Data Authentication. International Journal of Security and Networks 4(1/2), 69–86 (2009)
96. Suomalainen, J., Valkonen, J., Asokan, N.: Standards for Security Associations in Personal Networks: A Comparative Analysis. International Journal of Security and Networks 4(1/2), 87–100 (2009)
97. Kuo, C., Perrig, A., Walker, J.: Designing User Studies for Security Applications: A Case Study with Wireless Network Configuration. International Journal of Security and Networks 409(1/2), 101–109 (2009)
98. Berthier, R., Cukier, M.: An Evaluation of Connection Characteristics for Separating Network Attacks. International Journal of Security and Networks 4(1/2), 110–124 (2009)
99. Wu, B., Wu, J., Dong, Y.: An Efficient Group Key Management Scheme for Mobile Ad Hoc Networks. International Journal of Security and Networks 4(1/2), 125–134 (2009)
100. Chen, Z., Chen, C., Li, Y.: Deriving a Closed-form Expression for Worm-scanning Strategies. International Journal of Security and Networks 4(3), 135–144 (2009)

101. Lee, S., Sivalingam, K.M.: An Efficient One-Time Password Authentication Scheme Using a Smart Card. International Journal of Security and Networks 4(3), 145–152 (2009)
102. Watkins, L., Beyah, R., Corbett, C.: Using Link RTT to Passively Detect Unapproved Wireless Nodesd. International Journal of Security and Networks 4(3), 153–163 (2009)
103. Drakakis, K.E., Panagopoulos, A.D., Cottis, P.G.: Overview of Satellite Communication Networks Security: Introduction of EAP. International Journal of Security and Networks 4(3), 164–170 (2009)
104. Chakrabarti, S., Chandrasekhar, S., Singhal, M.: An Escrow-less Identity-based Group-key Agreement Protocol for Dynamic Peer Groups. International Journal of Security and Networks 4(3), 171–188 (2009)
105. Ehlert, S., Rebahi, Y., Magedanz, T.: Intrusion Detection System for Denial-of-Service Flooding Attacks in SIP Communication Networks. International Journal of Security and Networks 4(3), 189–200 (2009)
106. Bai, L., Zou, X.: A Proactive Secret Sharing Scheme in Matrix Projection Method. International Journal of Security and Networks 4(4), 201–209 (2009)
107. Bettahar, H., Alkubeily, M., Bouabdallah, A.: TKS: A Transition Key Management Scheme for Secure Application Level Multicast. International Journal of Security and Networks 4(4), 210–222 (2009)
108. Huang, H., Kirchner, H., Liu, S., Wu, W.: Handling Inheritance Violation for Secure Interoperation of Heterogeneous Systems. International Journal of Security and Networks 4(4), 223–233 (2009)
109. Rekhis, S., Boudriga, N.A.: Visibility: A Novel Concept for Characterizing Provable Network Digital Evidences. International Journal of Security and Networks 4(4), 234–245 (2009)
110. Djenouri, D., Bouamama, M., Mahmoudi, O.: Black-hole-resistant ENADAIR-based Routing Protocol for Mobile Ad Hoc Networks. International Journal of Security and Networks 4(4), 246–262 (2009)
111. Hu, F., Dong, D., Xiao, Y.: Attacks and Countermeasures in Multi-hop Cognitive Radio Networks. International Journal of Security and Networks 4(4), 263–271 (2009)