A Sequential Distinguisher for Covert Channel Identification

K. P. Subbalakshmi, Rajarathnam Chandramouli, and Nagarajan Ranganathan
(Corresponding author: K. P. Subbalakshmi)
B 315, Department of Electrical and Computer Engineering
Institute of Technology, Hoboken, NJ 07030, USA
(Email: ksubbala@stevens.edu)

(Received Dec. 9, 2005; revised and accepted Feb. 20, 2006)

Abstract

Covert channels are of two types: (a) timing channel and (b) storage channel. Most previous works have studied these channels from the encoder's perspective, namely, information theoretic capacity, algorithms and protocols for hiding information etc. This paper investigates the covert channel problem from an passive adversary's perspective. A sequential distinguisher for storage channel identification by an adversary is proposed and its properties are derived analytically. The impact of correlation in the observations received by the adversary is studied analytically as well as numerically.

Keywords: Covert channel, error probability, hypothesis testing, passive adversary, random walk

1 Introduction

A covert channel is defined as: *any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy* [5]. They can be broadly classified into two categories: (a) timing channels and (b) storage channels.

A covert timing channel (e.g., [1, 8, 9, 10]) encodes a message by modulating the time interval between successive responses of a system. For example, an user of a time-shared computing server can transmit covertly by varying the rate at which it sends jobs for processing. Since the response time of the computing server depends on its instantaneous load, other users can get a *noisy* version of the covert information by measuring the response time to their own jobs.

A storage channel (e.g., [2, 4, 11, 13]) embeds a covert message into the available system resources. An example of storage channels include data hiding in digital images for watermarking and fingerprinting applications. An abstract model, shown in Figure 1, of such a channel is the Prisoner's problem [12]. Here, Alice and Bob are prisoners in two different cells. They hatch a plan to escape

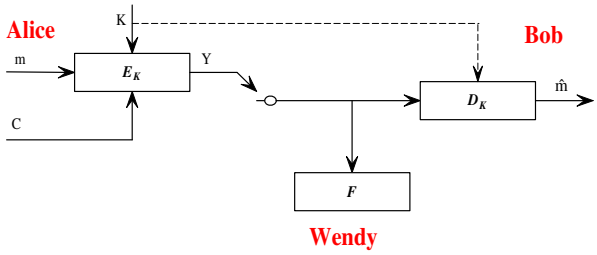

Figure 1: Prisoner's problem model for covert communication

by covertly communicating with each other using a storage channel (e.g., embedding a covert message in a plain looking digital image). It is assumed that Alice and Bob share a secret key (K) *a priori* that they use for encoding (E_K) and decoding (D_K) a covert message (m) in a cover/host message C. Each output from Alice's encoder is first examined by a passive adversary/warden, Wendy. Wendy runs an algorithm (F) on the encoder's outputs ($Y \in \Re$) to determine if it contains a covert message. Throughout this paper the generic variable Y represents either a random variable or a random vector that will be obvious from the context. If $F(Y) = 1$ then Wendy detects a covert channel and therefore punishes Alice and Bob. However, if $F(Y) = -1$ she decides that there is no covert message and allows Y to be received by Bob. Then Bob decodes a message ($\hat{m}$) from Y.

In this paper we consider a twist to the Prisoner's problem and investigate a sequential distinguisher for Wendy to identify covert channels. We first note that in the traditional Prisoner's problem described previously, Wendy punishes Alice and Bob if her algorithm $F(\cdot)$ evaluates to 1, i.e., it detects a covert message. Since $F(\cdot)$ is a statistical algorithm there are two types of possible errors—*false alarm* (α): $F(Y) = 1$ when it should really evaluate to -1 and *miss* probability (β): $F(Y) = -1$ when the true value is 1. Typically, there is a trade-off between these

two error probabilities. Keeping this in mind we introduce the twist in the following ways:

- Wendy fixes her ultimate desired false alarm and miss probabilities.
- She is allowed to examine a sequence of encoder outputs $\{Y_n\}$ and observe the corresponding decisions $\{Z_n = F(Y_n, Y_{n-1}, \ldots, Y_1)\}$. Note that $Z_n = \pm 1$, $\forall n$. A sequential distinguisher is then employed that attempts to minimize the expected number of observations for the final decision by fixing the desired detection error probabilities.

Since Wendy could make errors in making a decision, the new formulation allows her to pool her sequence of decisions until she is sufficiently confident of giving the final verdict. This modified problem raises several interesting questions. Since the error probabilities are fixed (unlike the previous model) and the number of observations is a random variable, will the sequential distinguisher converge to a final decision about the covert channel? What is the effect of the error probabilities on the expected number of observations? How does the sequential distinguisher reduce the total cost for Wendy? What is the effect of correlation? We investigate answers to some of these questions in this paper.

The paper is organized as follows. Section 2 describes the mathematical model for the covert channel identification problem of an adversary. Section 3 presents the proposed sequential distinguisher as a solution to the adversary's problem. Numerical results are presented in Section 4 with major conclusions in Section 5.

2 Mathematical Model

We first present an abstract mathematical model for the covert channel identification problem. Initially, Alice chooses either to embed a message or not in the *covertext* C where the probability distribution of C is P_C. If she embeds a message in C then the output of the encoder is the *stegotext* S (with probability distribution P_S).

Wendy performs a two-stage binary hypothesis test. In the first stage the problem is to design a distinguisher F to test the following:

$$\begin{aligned} H_0 : Y_n &\sim P_C, \quad n = 1, 2, \ldots \quad \text{(no covert message)} \\ H_1 : Y_n &\sim P_S, \quad n = 1, 2, \ldots \quad \text{(covert message embedded)} \end{aligned}$$

The statistical test is described by the function $F : Y \to \mathcal{Z}$ where $\mathcal{Z} = \{-1, 1\}$. Note that we are not concerned with the choice of F. Clearly, F induces false alarms and misses as discussed in Section 1.

We consider the following two cases: (a) $\{Z_n\}$ is a Markov chain and (b) $\{Z_n\}$ is independent and identically distributed (iid). Clearly, the choice of F leads to these two cases (as well as many others). We can also observe that Case (b) is a special case of Case (a). The problem posed to Wendy in the second stage of the hypothesis test, for Case (a), is the following:

$$\begin{aligned} &\text{(no covert channel)} \quad H_0 : \mathcal{P}^{H_0} = \begin{pmatrix} p_{11}^{H_0} & p_{12}^{H_0} \\ p_{21}^{H_0} & p_{22}^{H_0} \end{pmatrix} \text{ vs.} \\ &\text{(covert channel present)} \quad H_1 : \mathcal{P}^{H_1} = \begin{pmatrix} p_{11}^{H_1} & p_{12}^{H_1} \\ p_{21}^{H_1} & p_{22}^{H_1} \end{pmatrix} \end{aligned} \tag{1}$$

where, $p_{11} = P(Z_{n+1} = -1 | Z_n = -1)$ and $p_{22} = P(Z_{n+1} = 1 | Z_n = 1)$,$n \geq 1$ (superscripts have been dropped here for notational convenience). This is a test between the two possible transition probability matrices for the Markov chain $\{Z_n\}$. The transition probabilities are functions of α, β and other parameters of F.

2.1 Sequential Decisions

A sequential distinguisher is based on sequential decision theory pioneered by Wald [14]. Let the observations $\{Y_n;\ n = 1, 2, \ldots\}$ be iid and let the binary hypothesis test be described by:

$$\begin{aligned} H_0 &: Y_n \sim P_0, \quad n = 1, 2, \ldots \\ H_1 &: Y_n \sim P_1, \quad n = 1, 2, \ldots \end{aligned}$$

where P_0 and P_1 are two possibilities for the distribution of the observations on $(\Re, \mathcal{B})$, where $\mathcal{B}$ denotes the Borel σ-algebra on $\Re$. A *sequential decision rule* is a pair of sequences $\{(\varphi_j, \chi_j)\}$ where $\varphi_j : \Re^j \to \{0, 1\}$ is called a *stopping rule* and χ_j on $(\Re^j, \mathcal{B}^j)$[1] is called a *terminal decision rule* for each $j \geq 0$. The two steps that are involved in the sequential decision rule are: If N is the *stopping time* defined as $N = \inf\{n : \varphi_n(Y_1, Y_2, \ldots, Y_n) = 1\}$ then the decision rule is $\chi_N(Y_1, Y_2, \ldots, Y_N)$. That is, in the first step $\{\varphi_j\}$ computes the instant to stop taking further observations and χ_N produces the final decision about the true hypothesis at that instant. If $P(N < \infty) = 1$ then the sequential test terminates after only a finite number of observations.

Sequential Probability Ratio Test: Let the probability density functions of $\{Y_n\}$ conditioned on H_1 and H_0 be denoted by $f_1(y_1, y_2, \ldots, y_n)$ and $f_0(y_1, y_2, \ldots, y_n)$; $n \geq 1$, respectively. Then for two decision thresholds T_1 and $T_2 (-\infty < T_1 < T_2 < \infty)$ the sequential probability ratio test (SPRT) is defined as [14],

$$\begin{aligned} \mathcal{L}(y_1, y_2, \ldots, y_n) &= ln \frac{f_1(y_1, y_2, \ldots, y_n)}{f_0(y_1, y_2, \ldots, y_n)} \\ &\begin{cases} \geq & T_2 \ \text{ decide } \ H_1 \\ \leq & T_1 \ \text{ decide } \ H_0 \\ \text{else} & n = n + 1 \end{cases} \end{aligned}$$

The stopping and the decision rules for the SPRT are given as follows:

stopping rule:

$$\begin{aligned} N &= \inf\{n : \mathcal{L}(y_1, y_2, \ldots, y_n) \geq T_2 \ \text{ or } \\ &\qquad \mathcal{L}(y_1, y_2, \ldots, y_n) \leq T_1\} \\ \varphi_n &= \begin{cases} 1 & \text{if } \ n = N \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

decision rule:

$$\chi_N(y_1, y_2, \ldots, y_N) = \begin{cases} H_1 & \text{if } \ \mathcal{L}(y_1, y_2, \ldots, y_n) \geq T_2 \\ H_0 & \text{if } \ \mathcal{L}(y_1, y_2, \ldots, y_n) \leq T_1 \end{cases}$$

[1] $\mathcal{B}^j$ is the class of Borel sets in $\Re^j$

The thresholds T_1 and T_2 are computed as a function of the false alarm and miss probability constraints [14].

The optimality of the SPRT for iid observations is as classical theorem [7].

This theorem tells us that for iid observations SPRT is the optimum test in that it takes the minimum average sample number to detect the hypothesis among all sequential and fixed sample size tests.

3 Sequential Distinguisher for Covert Channel Detection

In this section we present the details of a sequential hypothesis test for Markov chains (e.g., [3]) based sequential distinguisher for identifying covert channels. We first consider Case (a) discussed in Section 2 and the corresponding problem is described by Equation (1). Let the adversary's observations $Z = \{Z_n\}$, $n \geq 1$ be a stationary, time-homogeneous, positive regular discrete-time Markov chain in steady state.

Define $p_n = P(Z_n = 1)$ and $q_n = 1 - p_n$, for $n \geq 1$. It is only known that SPRT is optimal for iid observations. Since Z is as Markov chain, we consider a linear, sub-optimal (computationally simple) sequential distinguisher given by:

$$S_n = S_0 + \sum_{i=1}^{n} Z_i$$
$$\begin{cases} \geq & A \text{ decide } H_1 \text{ (covert channel detected)} \\ \leq & -B \text{ decide } H_0 \text{ (no covert channel)} \\ \text{else} & n = n + 1. \end{cases} \quad (2)$$

$-B$ and A denote two decision thresholds where $B, A \geq 0$. It is easy to show that $\{S_n\}$ is not a Markov chain in general; however, if $p_{12} = p_{21} = \frac{1}{2}$ then $\{S_n\}$ is the classical simple random walk and $\{S_n\}$ becomes a Markov chain.

We also note that the correlation coefficient of the Markov chain $\{Z_n\}$ is given by $\rho(Z_n, Z_{n+1}) = p_{22} - p_{12}$. Therefore, the transition probability matrices in Equation (1) can be rewritten as:

$$\begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} = \begin{pmatrix} p_1\rho + q_1 & p_1(1-\rho) \\ q_1(1-\rho) & p_1 + q_1\rho \end{pmatrix},$$

The variance of S_k is then given by

$$\sigma^2 = np_1q_1 + 2p_1q_1\frac{\rho}{(1-\rho)^2}(n(1-\rho) - 1 + \rho^n)$$

which implies that $E(S_n^2) \to \infty$ as $n \to \infty$. In particular, $E(S_n^2|Z_1) \to \infty$ as $n \to \infty$ for both the possible values of Z_1.

3.1 Asymptotic Results

Let $N(\omega) = \inf\{n : S_n(\omega) = -B \text{ or } S_n(\omega) = A\}$ denote a stopping time variable. We are then interested in finding the finiteness property of N, i.e. will the sequential distinguisher Equation (2) used in the second-stage by Wendy will ever terminate? Towards this goal we use a technique similar to the one in proving Stein's lemma [6].

Theorem 1. *Let the the decision boundaries $-B$ and A be fixed. Then $P(N \geq n) = O(e^{-n\epsilon^*})$ for some $\epsilon^* > 0$ and $n^2P(N \geq n) \to 0$ as $n \to \infty$.*

Proof. Given in Appendix. □

Corollary 1. *The sequential distinguisher Equation (2) terminates with probability 1, i.e., N is finite with probability 1.*

Proof. Given in Appendix.

As a consequence of Corollary 1 we observe that all the finite moments of N exist. In particular the average and variance of the number of observations Wendy will use to detect the covert channel is finite.

Corollary 2. *For $1 \leq r < \infty$, $E(N^r) < \infty$.*

Proof. Given in Appendix. □

Lemma 1. *Let $\mu = E(Z)$ and $U_n = E(S_{n+1} - (n+1)\mu|\mathcal{F}_n)$, $n \geq 1$ where $\mathcal{F}_n = \sigma(\omega : Z_1, Z_2, \cdots, Z_n)$ is an increasing sequence of sub σ-fields. Then $\{U_n, \mathcal{F}_n\}$ is a martingale and U_0=0 a.s.*

Proof. Given in Appendix. □

Theorem 2. *$E(S_{N+1}) = (E(N) + 1)\mu$ conditioned on each hypothesis.*

Proof. Given in Appendix. □

Theorem 3. *If $\mu = 0$ then $E(S_{N+1}^2) = (E(N) + 1)var(Z)$.*

Proof. Given in Appendix. □

3.2 Finite-time Results

Here, we derive some finite-time results concerning the sequential distinguisher.

3.2.1 Finite-time Test Termination Probability:

$P(S_n = -B)$ and $P(S_n = A)$ denote the finite time termination probabilities of the sequential distinguisher. Let $S_0 = s$ for some constant integer s and $b(s, n, k) = P(S_n = k)$, $0 < k < A$. We state the following result without proof due to space constraints.

Theorem 4. *The time-dependent termination probability of the sequential distinguisher for $n \geq 2$ is given by,*

$$\begin{aligned} P(S_n = -B) &= p_1p_{11}b(s+1, n-2, -B+1) \\ &\quad + q_1p_{11}b(s-1, n-2, -B+1) \\ P(S_n = A) &= p_1p_{22}b(s+1, n-2, A-1) \\ &\quad + q_1p_{22}b(s-1, n-2, A-1) \end{aligned}$$

and

$$P(S_1 = -B) = \begin{cases} q_1 & \text{if } s = -B+1 \\ 0 & \text{otherwise} \end{cases}$$

$$P(S_1 = A) = \begin{cases} p_1 & \text{if } s = A-1 \\ 0 & \text{otherwise.} \end{cases}$$

where

$$\begin{aligned} b(s, n, k) &= \frac{2}{A+B}(M_1)^{n/2}\left(\frac{p_{11}}{p_{22}}\right)^{(s-k)/2}\sum_{l=0}^{A+B} M_2M_3M_4 \\ M_1 &= 4p_{11}p_{22} \\ M_2 &= sin(\frac{l\pi(s+B)}{A+B}) \\ M_3 &= sin\left(\frac{l\pi(k+B)}{A+B}\right) \\ M_4 &= cos^n\left(\frac{l\pi}{A+B}\right) \end{aligned} \quad (3)$$

where $-B+1 \leq s \leq A-1$, $-B+1 \leq k \leq A-1$, *and* $n \geq 2$.

We also observe that $b(s,n,-B)=0$ if $n-(s+B)$ is odd and $b(s,n,A)=0$ if $n-(A-s)$ is odd.

Note that when the false alarm and miss probabilities of the sequential distinguisher decrease to zero the decision boundaries increase unboundedly. Therefore we have the following result.

Theorem 5. *Let* $S_0 = s$ *for some fixed constant* s. *If* $min(A,B) \to \infty$ *then*

$$b(s,n,k) = 2(4p_{11}p_{22})^{n/2}\left(\frac{p_{11}}{p_{22}}\right)^{(s-k)/2}\frac{1}{\pi}\int_0^\pi sins\phi\ sink\phi\ (cos\phi)^n d\phi.$$

Proof. . Let $\phi = \frac{l\pi}{A+B}$. Then the successive difference is $\triangle\phi = \frac{\pi}{A+B}$. Therefore, if $min(A,B) \to \infty$ then the summation in Equation (3) becomes the definite integral given in the theorem. □

3.2.2 Hitting-time Probabilities:

If the random walk $\{S_n\}$ ultimately hits one of the two decision boundaries then it signals the end of the sequential test and a decision about the presence/absence of the covert channel is an output. Therefore it is interesting to study the hitting-time probabilities of the random walk.

The following theorem generalizes a result in [6] that is valid for a random walk with independent increments.

Theorem 6. *Let* $a_k(s) = P($*sequential distingusher terminates at* $-B, S_0 = s | Z_1 = e_k)$, $k = 1,2$. *If* $\lambda = \frac{p_{11}}{p_{22}} \neq 1$ *(non-symmetric case) then*

$$a_1(s) = \frac{p_{21}\lambda^{A+B} - p_{12}\lambda^{s+B}}{p_{21}\lambda^{A+B} - p_{12}\lambda}$$

$$a_2(s) = \frac{p_{21}\left[\lambda^{A+B} - \lambda^{s+B+1}\right]}{p_{21}\lambda^{A+B} - p_{12}\lambda}$$

If $p_{11} = p_{22} = p$ $(\lambda = 1)$ *(symmetric case) and* $q = 1-p$ *then,*

$$a_1(s) = \frac{(s-A)q - p}{[1-(A+B)]q - p}$$

$$a_2(s) = \frac{(s-A+1)q}{[1-(A+B)]q - p} \quad (4)$$

Proof. Given in Appendix. □

3.2.3 Expected Hitting Time:

From Corollary 2 we know that the expected time for the sequential distinguisher to terminate, $E(N)$, is finite. The following theorem (proof not give here) gives a formula to compute this value.

Theorem 7. *Let* $b_1(s)$ *and* $b_2(s)$ *denote the expected number of observations for the sequential test to detect the covert channel when* $S_0 = s$ *conditioned on* $Z_1 = -1$ *and* $Z_1 = 1$ *respectively,* i.e., $b_i(s) = E(N|Z_1 = e_i)$, $i = 1,2$. *Then, if* $\lambda \neq 1$,

$$b_1(s) = \frac{(p_{21}+p_{12})(s+B) - 2p_{12}}{p_{21}-p_{12}} + \frac{p_{12}[(A+B-2)(p_{21}+p_{12})+2]\lambda^{s+B} - 1}{(p_{21}-p_{12})(p_{12}-p_{21}\lambda^{A+B-1})}$$

$$b_2(s) = \frac{(p_{21}+p_{12})(s+B) + 2p_{11}}{p_{21}-p_{12}} + \frac{p_{21}[(A+B-2)(p_{21}+p_{12})+2][\lambda^{s+B} - p_{12}]}{(p_{21}-p_{12})(p_{12}-p_{21}\lambda^{A+B-1})}$$

If $p_{11} = p_{22} = p$ *and* $q = 1-p$,

$$b_1(s) = \frac{[(A+B)q+1](s+B) - [A+B+(s+B)^2]q}{p}$$

$$b_2(s) = A+B+\frac{(s+B)[(A+B)q-1] - (s+B)^2 q}{p} \quad (5)$$

(6)

4 Numerical Results

In this section provide some numerical results to further illustrate the theoretical analysis. We discuss some results when $\{Z_n\}$ is symmetric ($p_{11} = p_{22} = p$ and $p_{12} = p_{21} = q$) as well as non-symmetric. For the symmetric Markov chain the correlation coefficient is given by $\rho(Z_{n+1}, Z_n) = p - q$. Let $P(Z_1 = \pm 1) = \frac{1}{2}$. First, we observe from Equation (4) that the probability of accepting H_0 when $S_0 = s$, say, $a(s)$ is given by,

$$a(s) = \frac{1}{2}\left[1 + \frac{1 - \frac{2(s+B)}{A+B}}{1 + \frac{R}{A+B}}\right]$$

where $R = \frac{2\rho}{1-\rho}$. It is clear that as ρ varies between -1 and 1, R varies from -1 to ∞. Therefore, we see that $a(s)$ takes values between 1/2 and $1 - \frac{s+B-1/2}{A+B-1}$. Thus, $a(s) > \frac{1}{2}$ when $s < \frac{A-B}{2}$ and, $a(s) < \frac{1}{2}$ when $s > \frac{A-B}{2}$. The probability that H_1 is accepted is equal to $1 - a(s)$ because $P(N < \infty) = 1$.

We observe that as $\rho \to 1$ the probability of accepting H_0 becomes independent of the initialization and tends towards $P(Z_1 = -1) = 1/2$. Similarly, Similarly the probability of accepting H_1 tends towards $P(Z_1 = 1) = 1/2$ as $\rho \to 1$.

We first consider the non-symmetric case to compute the average sample number required by the sequential distinguisher to identify the covert channel. The choice of decision thresholds of the sequential test and the average sample number depend on the correlation co-efficient of the Markov chain $\{Z_i\}$. Let the correlation co-efficient conditioned on the hypotheses, H_i, be denoted by ρ_i, $i = 0,1$. Let $S_0 = 0$ and $\rho = \rho_0 = \rho_1$. Consider the following example transition probability matrices: $p_{11}^{H_0} = 0.55$, $p_{22}^{H_0} = 0.45$, $p_{11}^{H_1} = 0.4$, $p_{22}^{H_1} = 0.6$, $P^{H_0}(Z=1) = 0.45$, and $P^{H_1}(Z=1) = 0.6$ for $\rho = 0$. Similarly, when $p_{11}^{H_0} = 0.7$, $p_{22}^{H_0} = 0.4$, $p_{11}^{H_1} = 0.4$, $p_{22}^{H_1} = 0.7$, $P^{H_0}(Z=1) = 0.33$, and $P^{H_1}(Z=1) = 0.67$ we see that $\rho = 0.1$. We computed the optimal decision thresholds A and B that satisfy the given false alarm and miss probability constraints. These thresholds were computed using the Levenberg-Marquadt iterative method for solving non-linear equations. We note that the values of the decision thresholds decrease as the acceptable false alarm and miss probabilities increase. This is because the constraint on the sequential distinguisher is relaxed when the error probabilities are increased. An increase in the correlation co-efficient also results in a decrease in the thresholds. This is because a positive correlation co-efficient implies that the successive observations have a bias towards the true hypothesis.

Figures 2 and 3 show the average sample number required by the sequential distinguisher to detect the presence/absence of a covert channel when $\rho = 0$ and $\rho = 0.1$, respectively. The false alarm probability (α_{01}) ranges from 10^{-5} to 10^{-1}. We notice from these figures that even a small positive correlation reduces the average sample number of the sequential test by at least a factor of 5. This means that the sequential distinguisher

is able to detect the covert channel much faster by exploiting a positive correlation.

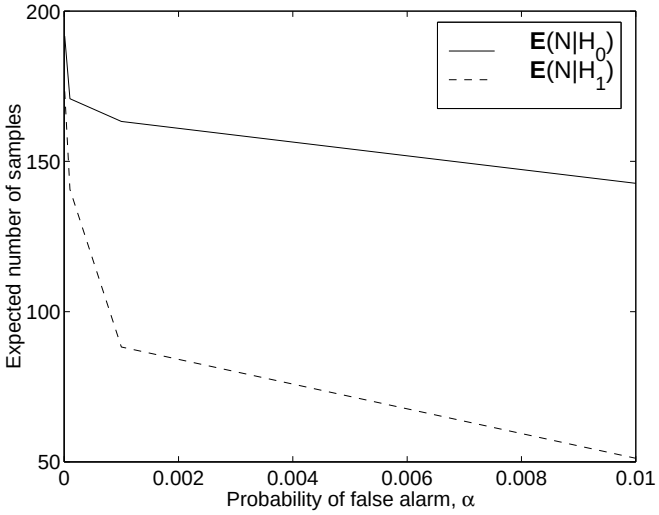

Figure 2: Average sample number for the test to identify the presence/absence of the covert channel when $\rho = 0$

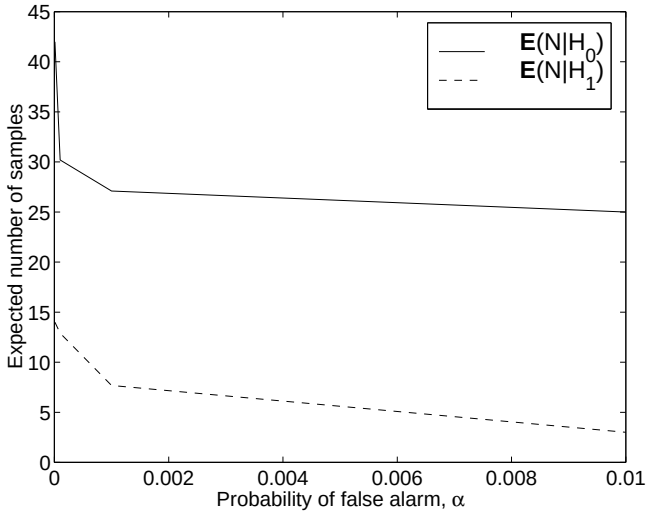

Figure 3: average sample number for the test to identify the presence/absence of the covert channel when $\rho = 0.1$

Figure 4 shows the comparison of the average sample number used by the sequential distinguisher for dependent and independent observations. The value of the parameters are $A = 10$, $B = -9$, and $s = 0$. Clearly the sequential distinguisher exploits the correlation and outperforms that case when the observations are statistically independent.

Now, consider the symmetric case. From Equation (5) the average sample number for the test to terminate for equally likely first step can be seen to be,

$$\begin{aligned}\Xi(s) &= \frac{1}{2}[b_1(s) + b_2(s)] \\ &= (s+B)(A-s) \\ &\quad -(\frac{\rho}{1+\rho})[2(s+B)(A-s) - (A+B)] \quad (7)\end{aligned}$$

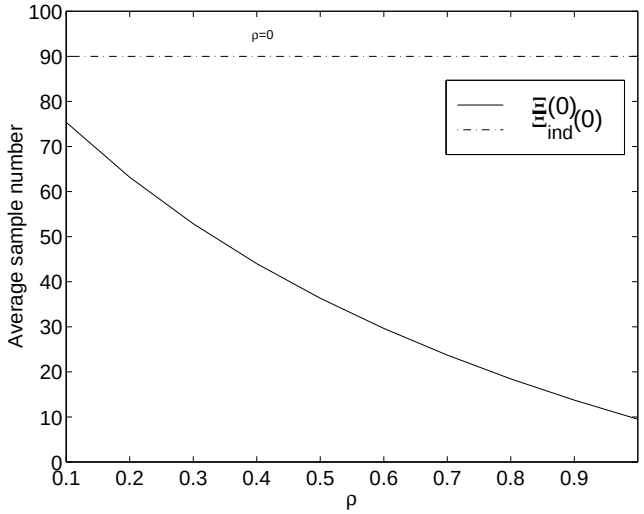

Figure 4: Comparison of average sample numbers for the cases of independent and Markov correlated observations

If $\{Z_k\}$ is assumed to be independent then $\rho = 0$. Then, from Equation (7) the average sample number, say, $\Xi_{ind}(s)$ is given by

$$\Xi_{ind}(s) = (s+B)(A-s) \quad (8)$$

which agrees with a classical result [6]. Now,

$$\begin{aligned}(s+B)(A-s) &= (s+B)[(A+B) - (s+B)] \\ &= (s+B)(A+B) - (s+B)^2\end{aligned}$$

The right hand side of the above equation attains it minimum value when $s = -B+1$ or $s = A-1$ (note that $-B+1 \le s \le A-1$). Therefore we have $(s+B)(A-s) \ge (A+B) - 1 \ge \frac{A+B}{2}$ if $(A+B) \ge 2$. This implies that $2(s+B)(A-s) - (A+B) \ge 0$. Using this in Equation (7) we observe that there is a reduction in the average sample number when the correlation coefficient, $\rho > 0$. Thus, the sequential distinguisher exploits the correlation in the observations and results in faster detection, *i.e.*, $\Xi(s) \le \Xi_{ind}(s)$. In fact, $\Xi(s) \to (A+B)/2$ when $\rho \to 1$. The following theorem shows that the sequential distinguisher is asymptotically efficient for positively correlated observations.

Theorem 8. *(*Asymptotic Efficiency*) Let $\rho \ge 0$. Then for each hypothesis*

$$\limsup_{min(A,B)\to\infty} \frac{\Xi(s)}{\Xi_{ind}(s)} \le 1$$

Proof. From Equations (8) and (7) we get

$$\begin{aligned}\frac{\Xi(s)}{\Xi_{ind}(s)} &= 1 - 2\left(\frac{\rho}{1+\rho}\right) + \frac{A+B}{(s+B)(A-s)} \\ &\le 1 + \frac{A+B}{(s+B)(A-s)}\end{aligned}$$

As $min(A,B) \to \infty$ the second term on the RHS of the above term goes to zero and the result follows. □

5 Conclusions

The major conclusions that we draw about the proposed sequential distinguisher for covert channel identification are the following:

- The proposed sequential distinguisher uses finite number of observations w.p. 1 to detect the covert channel.
- As the correlation coefficient of Wendy's Markov-dependent observations tend towards 1 the probability of identifying the channel correctly tends to their prior probabilities and asymptotically becomes independent of the initialization of the sequential distinguisher.
- As the values of the decision thresholds decrease the acceptable false alarm and miss probabilities increase. An increase in the correlation co-efficient also results in a decrease in the thresholds.
- Even a small positive correlation in the observations received by the adversary reduces the required average sample number of the sequential distinguisher by at least a factor of 5. This means that the sequential distinguisher is able to detect the covert channel much faster by exploiting a positive correlation.
- The sequential distinguisher is asymptotically efficient for Markov-dependent observations when compared to iid observations.

Acknowledgements

R. Chandramouli was supported by an U.S. AFRL grant and K.P. Subbalakshmi was supported by a NSF grant.

References

[1] V. Anantharam and S. Verdu, "Bits through queues," *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 4-18, Jan. 1996.

[2] C.Cachin, "An information-theoretic model for steganography," *Information and Computation*, vol. 192, no. 1, pp. 41-56, July 2004.

[3] R. Chandramouli and N. Ranganathan, "A generalized sequential sign detector for binary hypothesis testing," *IEEE Signal Processing Letters*, vol. 5, no. 11, pp. 295-297, Nov. 1998.

[4] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*, Academic Press, 2002.

[5] U. S. D. O. Defense, *Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, 1985.

[6] W. Feller, *An introduction to probability theory and its applications*, vol. 1, Wiley and Sons, 1950.

[7] B. Ghosh, *Sequential tests of statistical hypotheses*, Addison-Wessley, 1970.

[8] J. Giles and B. Hajek, "An information-theoretic and game-theoretic study of timing channels," *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2455-2477, Sept. 2002.

[9] S. J. Greenwald, I. S. Moskowitz, and M. H. Kang, "An analysis of the timed z-channel," *Proceedings of IEEE Symposium on Security and Privacy*, pp. 2-11, May 1996.

[10] S. Lipner, "A comment on the confinement problem," *Fifth symposium on Operating systems principles*, pp. 192-197, Nov. 1975.

[11] I. S. Moskowitz and M. H. Kang, "Covert channels - here to stay?" *Proceedings of COMPASS*, pp. 235-243, Jun. 1994.

[12] G. Simmons, "The prisoners problem and the subliminal channel," *Advances in Cryptology: Proceedings of Crypto*, pp. 51-67, 1984.

[13] C. R. Tsai and V. D. Gligor, "A bandwidth computation model for covert storage channels and applications," *Proceedings of Computer Security Foundations Workshop IV*, pp. 22-33, Jun. 1991.

[14] A. Wald, *Sequential analysis*, Dover Publications, 1973.

Appendix

Proof of Theorem 1:

Proof. Let $C = A + B$. Since $E(S_n^2|Z_1 = e_i) \to \infty$ as $n \to \infty$, for $i = 1, 2$, where $e_1 = -1$ and $e_2 = 1$, there exists a k such that

$$P(S_k^2 < C^2|Z_1 = e_i) < 1, \quad i = 1, 2$$

Let us denote this probability by $1 - \epsilon_i$, $\epsilon_i > 0$ and, let $\epsilon^* = min(\epsilon_1, \epsilon_2)$. Then,

$$P(S_k^2 < C^2|Z_1) < 1 - \epsilon^*$$

and by choosing $n = jk$ we get

$$P\left([S_{k(r+1)} - S_{kr}]^2 < C^2,\ r = 0, 1, \cdots, j-1\right) \leq (1 - \epsilon^*)^{n/k}$$

Hence, we see that

$$P(N \geq n) \leq (1-\epsilon^*)^{n/k} = O(e^{-n\epsilon^*}) = o(n^{-2}) \text{ as } n \to \infty. \quad (9)$$

□

Proof of Corollary 1:

Proof. Let $\mathcal{A} = \{N = \infty\}$, *i.e.*, $\mathcal{A}$ is the event that $-B < S_n < A$, $\forall\ n \geq 1$. Let $\mathcal{A}_n = \{-B < S_r < A,\ 0 < r \leq n\}$. Therefore, $\mathcal{A} = \bigcap_n \mathcal{A}_n$ and $P(\mathcal{A}) \leq P(\mathcal{A}_n)$, $\forall\ n \geq 1$. Now,

$$\begin{aligned} P(\mathcal{A}_{nk}) &= P\left(\bigcap_{r=1}^{nk}\{-B < S_r < A\}\right) \\ &= P\left(\bigcap_{r=1}^{n}\{-B < S_{rk} < A\}\right) \\ &= P(N \geq n) \leq (1 - \epsilon^*)^{n/k} \quad \text{(from Equation (9))} \end{aligned}$$

Hence we have $0 \leq P(\mathcal{A}) \leq P(\mathcal{A}_n) \leq (1 - \epsilon^*)^{n/k}$ which completes the proof.

□

Proof of Corollary 2:

Proof. We know that

$$\begin{aligned} E(N^r) &= \sum_{n=1}^{\infty} n^r P(N = n) \\ &= \sum_{n=1}^{\infty} n^r \left[P(N \geq n) - P(N \geq n+1)\right] \\ &\leq \text{constant.} \sum_{n=1}^{\infty} n^r \left[e^{-n\epsilon^*} - e^{-(n+1)\epsilon^*}\right] < \infty \\ &\quad \text{(from Corollary 1)} \end{aligned}$$

□

Proof of Lemma 1:

Proof. Since,

$$\begin{aligned} E(U_n|\mathcal{F}_{n-1}) &= E(S_{n+1} - (n+1)\mu|\mathcal{F}_{n-1}) \\ &= U_{n-1} + E(Z_{n+1} - \mu|\mathcal{F}_{n-1}) \\ &= U_{n-1} \text{ a.s.} \end{aligned}$$

□

Proof of Theorem 2:

Proof. Let $N \wedge n = min(N, n)$. Then, from Lemma 1 and the optional stopping theorem we have

$$\begin{aligned} E(S_{N\wedge n+1} - (N \wedge n + 1)\mu) &= E(U_{N\wedge n}) \\ &= E(U_0) \\ &= 0. \end{aligned}$$

Therefore,

$$E(S_{N\wedge n+1}) = E(N \wedge n + 1)\mu \tag{10}$$

Now, let $Z_n^+ = max(0, Z_n)$ and $Z_n^- = -min(0, Z_n)$. Then we can write $Z_n = Z_n^+ - Z_n^-$. Therefore,

$$\begin{aligned} S_{N\wedge n+1} &= \sum_{i=1}^{N\wedge n+1} Z_n \\ &= \sum_{i=1}^{N\wedge n+1} Z_n^+ - \sum_{i=1}^{N\wedge n+1} Z_n^- \\ &= S_{N\wedge n+1}^+ - S_{N\wedge n+1}^- \end{aligned}$$

which gives $E(S_{N\wedge n+1}) = E(S_{N\wedge n+1}^+) - E(S_{N\wedge n+1}^-)$. Taking limits,

$$\begin{aligned} \lim_{n\to\infty} E(S_{N\wedge n+1}) &= \lim_{n\to\infty} E(S_{N\wedge n+1}^+) - \lim_{n\to\infty} E(S_{N\wedge n+1}^-) \\ &= E(\lim_{n\to\infty} S_{N\wedge n+1}^+) - E(\lim_{n\to\infty} S_{N\wedge n+1}^-) \\ &\quad \text{(by monotone convergence theorem)} \\ &= E(S_{N+1}^+) - E(S_{N+1}^-) \\ &= E(S_{N+1}) \end{aligned} \tag{11}$$

But from Equation (10),

$$\begin{aligned} \lim_{N\to\infty} E(S_{N\wedge n+1}) &= \lim_{N\to\infty} (E(N \wedge n) + 1)\mu \\ &= (E(\lim_{N\to\infty} N \wedge n) + 1)\mu \\ &\quad \text{(due to monotone convergence theorem)} \\ &= (E(N) + 1)\mu \end{aligned} \tag{12}$$

From Equations (11) and (12) the result follows. □

Proof of Theorem 3:

Proof. We know that,

$$\begin{aligned} E(S_{N+1}^2) &= E\left(\sum_{i=1}^{N+1} Z_i\right)^2 \\ &= E(\sum_{i=1}^{N+1} Z_i \sum_{j=1}^{N+1} Z_j) \\ &= E(\sum_{i=1}^{N+1} Z_i^2 + \sum_{i=1}^{N+1} \sum_{j=1}^{N+1,*} Z_i Z_j) \\ &= E(\sum_{i=1}^{N+1} Z_i^2 + E(\sum_{i=1}^{N+1} \sum_{j=1}^{N+1,*} Z_i Z_j) \\ &= (E(N) + 1)E(Z^2) + E(\sum_{i=1}^{N+1} \sum_{j=1}^{N+1,*} Z_i Z_j) \\ &\quad \text{(since } \{Z_i^2\} \text{ is also a Markov chain)} \\ &= (E(N) + 1)var(Z) \\ &\quad \text{(by optional stopping theorem} \\ &\quad E(W_N) = E(W_0) = 0) \end{aligned}$$

□

Proof of Theorem 6:

Proof. Let $a_{k,n}(s) = P(S_n = -B, S_0 = s|Z_1 = e_k)$, $k = 1, 2$. Then, for $-B + 1 < s < A - 1$ we get the following system of homogeneous, linear difference equations,

$$\begin{aligned} a_{1,n+1}(s + 1) &= p_{12}a_{2,n}(s) + p_{11}a_{1,n}(s) \\ a_{2,n+1}(s) &= p_{22}a_{2,n}(s + 1) + p_{21}a_{1,n}(s + 1) \end{aligned} \tag{13}$$

with boundary conditions, $a_{2,1}(A-1) = 0$ and $a_{1,1}(-B+1) = 1$. Let the generating function be $A_{k,s}(r) = \sum_{n=0}^{\infty} a_{k,n}(s)r^n$, $k = 1, 2$. Then using Equation (13) to compute the generating functions we get the following system of difference equations in the s-variable:

$$\begin{aligned} A_{1,s+1}(r) &= p_{12}rA_{2,s}(r) + p_{11}rA_{1,s}(r) \\ A_{2,s}(r) &= p_{22}rA_{2,s+1}(r) + p_{21}rA_{1,s+1}(r) \end{aligned} \tag{14}$$

Eliminating $A_{2,s}(r)$ from Equation (14) we get

$$\left[\mathcal{T}^2 - \frac{1 - r^2(1 - p_{11} - p_{22})}{rp_{22}}\mathcal{T} + \frac{p_{11}}{p_{22}}\right] A_{1,s}(r) = 0$$

where the operator $\mathcal{T}$ is defined as $\mathcal{T}^j A_{k,s}(r) = A_{k,s+j}(r)$, and j is a non-negative integer. We need to compute $a_k(s) = A_{k,s}(1)$, the conditional probability of the test statistic ultimately reaching $-B$. When $\lambda \neq 1$ (non-symmetric case) putting $r = 1$ in Equation (14),

$$\left[\mathcal{T}^2 - \frac{p_{11} + p_{22}}{p_{22}}\mathcal{T} + \frac{p_{11}}{p_{22}}\right] A_{1,s}(1) = 0$$

The solutions to this equation are given by the roots of the characteristic equation, namely,

$$\begin{aligned} \left[\mathcal{T}^2 - \frac{p_{11} + p_{22}}{p_{22}}\mathcal{T} + \frac{p_{11}}{p_{22}}\right] &= 0 \\ \implies [\mathcal{T} - 1]\left[\mathcal{T} - \frac{p_{11}}{p_{22}}\right] &= 0 \end{aligned}$$

Since $p_{11} \neq p_{22}$ the solution to the difference equation is given by

$$A_{1,s}(1) = B_1 + B_2\lambda^s \tag{15}$$

for two arbitrary constants B_1 and B_2 and, from Equation (14),

$$A_{2,s}(1) = \frac{1}{p_{12}}\left[B_1 + B_2\lambda^{s+1} - p_{11}\left(B_1 + B_2\lambda^{s}\right)\right] \quad (16)$$

Now, using the two boundary conditions we have

$$\begin{aligned} B_1 + B_2\lambda^{-B+1} &= 1 \\ \frac{1}{p_{12}}\left(B_1 + B_2\lambda^{A} - p_{11}\left(B_1 + B_2\lambda^{A-1}\right)\right) &= 0 \end{aligned}$$

solving which gives us

$$\begin{aligned} B_1 &= \frac{\lambda^A(1-p_{22})}{\lambda^A(1-p_{22}) - (1-p_{11})\lambda^{-B+1}} \\ B_2 &= \frac{p_{11}-1}{\lambda^A(1-p_{22}) - (1-p_{11})\lambda^{-B+1}} \end{aligned} \quad (17)$$

Therefore, from Equations (15) and (16) we get the required result when $\lambda \neq 1$ as shown below. For the symmetric case (*i.e.*, $\lambda = 1$) the characteristic equation becomes

$$(\mathcal{T}-1)^2 = 0$$

whose solution is

$$A_{1,s}(1) = C_1 + C_2 s$$

for two arbitrary constants C_1 and C_2. Therefore by putting $p_{11} = p_{22} = p$ and $p_{12} = p_{21} = q$ in Equation (14) we get

$$A_{2,s}(1) = \frac{1}{q}[C_1 + C_2(s+1) - p(C_1 + C_2 s)]$$

Using the boundary conditions again, we obtain

$$\begin{aligned} C_1 + (1-B)C_2 &= 1 \\ qC_1 + (A - p(A-1))C_2 &= 0 \end{aligned}$$

which has the following solution

$$\begin{aligned} C_1 &= \frac{-(p+Aq)}{(1-A-B)q - p} \\ C_2 &= \frac{q}{(1-A-B)q - p} \end{aligned}$$

from which the proof follows. The unconditional probability of the random walk terminating at $-B$ is $P(-B) = q_1 a_1(s) + p_1 a_2(s)$. By Corollary 1 the probability of the random walk ultimately terminating at A is $P(A) = 1 - P(-B)$.
Since $a_2(s) = A_{2,s}(1)$ and Equation (16) and Equation (17) give

$$A_{2,s}(1) = \frac{1}{p_{12}}\left[B_1 + B_2\lambda^{s+1} - p_{11}\left(B_1 + B_2\lambda^{s}\right)\right]$$

where

$$\begin{aligned} B_1 &= \frac{\lambda^A(1-p_{22})}{\lambda^A(1-p_{22}) - (1-p_{11})\lambda^{-B+1}} \\ B_2 &= \frac{p_{11}-1}{\lambda^A(1-p_{22}) - (1-p_{11})\lambda^{-B+1}} \end{aligned}$$

Using the fact that $1 - p_{22} = p_{21}$ and $1 - p_{11} = p_{12}$,

$$\begin{aligned} a_2(s) &= \frac{1}{p_{12}}\left[\frac{\lambda^A p_{21} - \lambda^{s+1}p_{12} - p_{11}p_{21}\lambda^A + p_{11}p_{12}\lambda^s}{\lambda^A p_{12} - \lambda^{-B+1}p_{12}}\right] \\ &= \frac{1}{p_{12}}\left[\frac{p_{12}\lambda^A(1-p_{11}) + p_{12}\lambda^s\left(p_{11} - \frac{p_{11}}{p_{22}}\right)}{\lambda^A p_{21} - \lambda^{-B+1}p_{12}}\right] \\ &= \frac{p_{21}\lambda^A - p_{21}\lambda^{s+1}}{\lambda^A p_{21} - \lambda^{-B+1}p_{12}} \\ &= \frac{p_{21}\lambda^{A+B} - p_{21}\lambda^{s+B+1}}{p_{21}\lambda^{A+B} - p_{12}\lambda} \\ &= \frac{p_{21}\lambda^{A+B} - p_{21}\lambda^{s+B+1}}{p_{21}\lambda^{A+B} - p_{12}\lambda} \end{aligned}$$

To compute $a_1(s) = A_{1,s}(1)$ we use Equation (15). From Equation (15) we obtain

$$\begin{aligned} a_1(s) &= B_1 + B_2\lambda^s \\ &= \frac{p_{21}\lambda^A}{p_{21}\lambda^A - p_{12}\lambda^{-B+1}} - \frac{p_{12}\lambda^s}{p_{21}\lambda^A - p_{12}\lambda^{-B+1}} \\ &= \frac{p_{21}\lambda^{A+B} - p_{12}\lambda^{s+B}}{p_{21}\lambda^{A+B} - p_{12}\lambda} \end{aligned}$$

□

Proof of Theorem 8:

Proof. From Equations (8) and (7) we get

$$\begin{aligned} \frac{\Xi(s)}{\Xi_{ind}(s)} &= 1 - 2\left(\frac{\rho}{1+\rho}\right) + \frac{A+B}{(s+B)(A-s)} \\ &\leq 1 + \frac{A+B}{(s+B)(A-s)} \end{aligned}$$

As $min(A,B) \to \infty$ the second term on the RHS of the above term goes to zero and the result follows. □

K. P. Subbalakshmi is an Assistant Professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. Her current research interests are in the areas of wireless security, cryptography, multimedia security, and joint source-channel coding. Further details can be found in http://www.ece.stevens-tech.edu/∼suba

Rajarathnam Chandramouli is an Associate Professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. His current research interests are in the areas of wireless networking and security, media security, and applied probability theory. Further details can be found in http://www.ece.stevens-tech.edu/∼mouli

N. Ranganathan is a Professor in the Department of Computer Science and Engineering at the University of S. Florida. His current research interests are in the areas of security, VLSI, and data compression. He is a Fellow of the IEEE. Further details can be found in http://www.cse.usf.edu/∼ranganat