Detecting Information Flows: Improving Chaff Tolerance by Joint Detection

Ting He and Lang Tong
School of Electrical and Computer Engineering
Cornell University, Ithaca, NY 14853
Email: {th255,lt35}@cornell.edu

***Abstract*— The problem of detecting encrypted information flows using timing information is considered. An information flow consists of both information-carrying packets and irrelevant packets called chaff. A relay node can perturb the timing of information-carrying packets as well as adding or removing chaff packets. The goal is to detect whether there is an information flow through certain nodes of interest by analyzing the transmission times of these nodes. Under the assumption that the relay of information-carrying packets is subject to a bounded delay constraint, fundamental limits on detection are characterized as the minimum amount of chaff needed for an information flow to mimic independent traffic. A detector based on the optimal chaff-inserting algorithms is proposed. The detector guarantees detection in the presence of an amount of chaff proportional to the total traffic size; furthermore, the proportion increases to 100% exponentially fast as the number of hops on the flow path increases.**

***Index Terms*— Information flow detection, Chaff-inserting algorithms, Chaff tolerance.**

I. Introduction

Consider a wireless ad hoc network illustrated in Fig. 1, where multiple source-destination pairs are communicating along certain routes. Suppose that we do not trust any nodes in the network, and nor do we know the routing protocol. Furthermore, assume that all the packets are reencrypted at every relay node so that the only observation we can obtain is the transmission times of the nodes. Under these constraints, we want to know how information is transmitted in the network.

Suppose we deploy eavesdroppers in the network to record node transmission times[1]. The problem is to detect information flows based on timing information. The challenges are that transmission times are subject to perturbations due to delays, reshuffling, etc. Moreover, traffic multiplexing at the relay nodes may introduce noise to the measurements. For example, in Fig. 1, if we want to detect an information flow along the path $S \rightarrow R \rightarrow D$, then the other information flows through S or R will cause noise in the detection because the measurements S_1 and S_2 will contain transmissions not belonging to the information flow of interest. Another source of noise is dummy packets actively inserted by S or R to evade detection. Both multiplexed traffic and dummy traffic are called *chaff noise*.

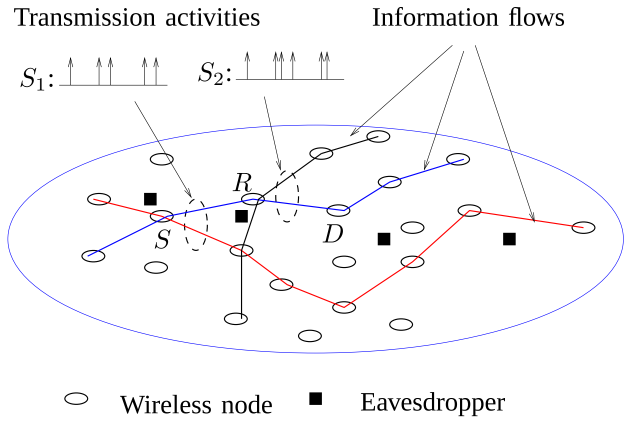

Fig. 1. Detecting information flows in a wireless ad hoc network by eavesdropping transmission activities.

A. Related Work

The problem of detecting information flows has mainly been addressed in the framework of intrusion detection. In 1995, Staniford and Heberlein [1] first considered the problem of stepping-stone detection. The key problem in stepping-stone detection is to reconstruct the intrusion path by analyzing various characteristics of the attacking traffic. Related work in the literature only considers pair-wise detection.

Early detection techniques are based on the content of the traffic; see, *e.g.*, [1], [2]. To deal with encrypted traffic, timing characteristics are used in detection, such as the On-Off detection by Zhang and Paxson [3], the deviation-based detection by Yoda and Etoh [4], and the packet interarrival-based detection by Wang *et al.* [5]. The drawback of these approaches is that they are vulnerable to active timing perturbation by the attacker.

Donoho *et al.* [6] were the first to consider bounded delay perturbation. They showed that if packet delays are bounded by a maximum amount, then it is possible to distinguish traffic

This work is supported in part by the National Science Foundation under award CCF-0635070, the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program DAAD19-01-2-0011, and TRUST (The Team for Research in Ubiquitous Secure Technology) sponsored by the National Science Foundation under award CCF-0424422. The U. S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

[1] We assume transmitter code and that the eavesdroppers know the code of the monitored nodes so that energy tests can be performed to identify transmission activities.

containing information flows from independent traffic. Their work was followed by several practical detectors, including the watermark-based detector by Wang and Reeves [7] and the counting-based detector by Blum *et al.* [8].

The problem becomes much more challenging when chaff can be inserted. In such cases, there are only incomplete solutions in the literature, *e.g.,* [6], [8]–[10]. Donoho *et al.* [6] showed that there will be notable difference between information flows and independent traffic if chaff traffic is independent of the flows of information-carrying packets. Peng *et al.* [9] and Zhang *et al.* [10] separately proposed active and passive packet-matching schemes which can detect information flows if chaff packets only appear in the outgoing traffic of the relay node. Blum *et al.* [8] modified their counting-based detector to handle a limited number of chaff packets at the cost of an increased false alarm probability.

B. Summary of Results and Organization

We consider the problem of detecting information flows in a wireless ad hoc network by measuring transmission times of the nodes of interest. Assuming that the relay of information-carrying packets is subject to bounded delay perturbation, we make detection based on the difference between the transmission patterns of information flows and independent traffic. The main challenge is that our measurements may contain chaff packets. Our goal is to investigate the limits of timing-based detection in the presence of arbitrarily inserted chaff noise[2], and develop detectors which can tolerate a significant amount of chaff.

The main contribution of this paper is a general form of detector which is designed specifically to provide guaranteed detection in the presence of chaff noise. Although previous work (*e.g.,* [6]) has claimed that detection is always possible if chaff noise and the information-carrying packets are independent, we have shown in [11] that with arbitrarily inserted chaff, there are limits on the amount of chaff noise beyond which no timing-based detector can work well. In this paper, we develop a threshold detector based on the optimal chaff-inserting algorithms. The detector guarantees detection of all the information flows with fractions of chaff bounded by the detection threshold. We prove that the detector has vanishing false alarm probability as long as its threshold is smaller than the minimum fraction of chaff needed to mimic independent traffic. The proposed detector is shown to be optimal in dealing with chaff noise; in particular, as the length of the flow path increases, the tolerable fraction of chaff noise increases to one exponentially.

The rest of the paper is organized as follows. Section II formulates the problem. Section III characterizes the fundamental limits on timing-based detection. Section IV presents an information flow detector together with its performance analysis. Then Section V concludes the paper with a few comments.

II. Problem Formulation

Suppose that we are interested in detecting information flows through n nodes, as illustrated in Fig. 2. Let S_i ($i = 1, \ldots, n$) be the process of transmission times of node R_i, *i.e.,*

$$S_i = (S_i(1),\ S_i(2),\ S_i(3), \ldots), \quad i = 1,\ 2, \ldots,\ n,$$

where $S_i(k)$ ($k \geq 1$) is the kth transmission time[3] of node R_i.

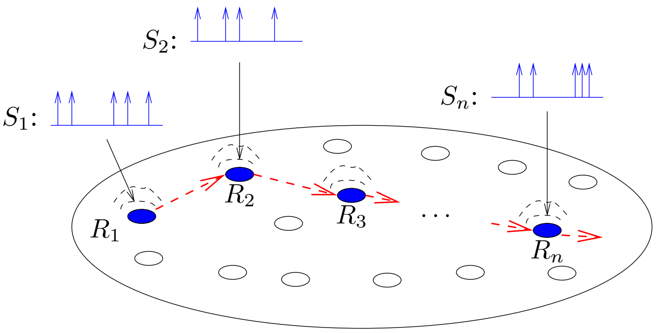

Fig. 2. Detecting information flows through nodes $R_1,\ R_2, \ldots,\ R_n$ by measuring transmission activities of these nodes.

If none of S_i ($i = 1, \ldots, n$) belongs to the same information flow, they should be jointly independent. Otherwise, if $(S_i)_{i=1}^n$ is an information flow, then it can be decomposed into an information-carrying part $(X_i)_{i=1}^n$ and a chaff part $(W_i)_{i=1}^n$. That is, $(S_i)_{i=1}^n$ is *an information flow* if[4] $S_i = X_i \bigoplus W_i$ for $i = 1, \ldots,\ n$, and $(X_i)_{i=1}^n$ satisfies the following definition.

Definition 2.1: A sequence of processes $(X_1, \ldots,\ X_n)$ is *a pure information flow* if there exist bijections $g_i : \mathcal{X}_i \rightarrow \mathcal{X}_{i+1}$ ($i = 1, \ldots,\ n-1$)[5] such that $g_i(s) - s \in [0,\ \Delta]$ for all $s \in \mathcal{X}_i$.

The bijection g_i is a mapping between the transmission times of the same packets at nodes R_{i-1} and R_i. The condition that g_i is a bijection imposes a *packet-conservation* constraint, *i.e.,* every information-carrying packet generates one and only one relay packet at each relay node. The condition $g_i(s) - s \geq 0$ is the *causality* constraint, which means that a packet cannot leave a node before it arrives. In addition, $g_i(s) - s \leq \Delta$ imposes a *bounded delay* constraint, meaning that no packet can be held at a relay node for longer than Δ.

Suppose that the detector starts at t_0 and takes observations for a duration t. We are interested in testing the following hypotheses:

$$\begin{aligned} \mathcal{H}_0 : & \quad S_1,\ S_2, \ldots,\ S_n \text{ are jointly independent,} \\ \mathcal{H}_1 : & \quad (S_i)_{i=1}^n \text{ contains an information flow,} \end{aligned}$$

by analyzing $S_i \cap [t_0,\ t_0 + t]$ ($i = 1, \ldots,\ n$)[6]. We say that

[2] We consider arbitrarily inserted chaff noise because it is the most difficult to handle. If (part of) the chaff noise is from multiplexed traffic on different paths, then it may be subject to certain constraints, and our analysis will provide lower bounds on the detection performance.

[3] Assume no simultaneous transmissions.

[4] The operator $\bigoplus$ is the superposition of processes $(a_1,\ a_2, \ldots)$ and $(b_1, b_2, \ldots)$, defined as $(a_i)_{i=1}^\infty \bigoplus (b_i)_{i=1}^\infty = (c_i)_{i=1}^\infty$ where $c_1 \leq c_2 \leq \ldots$ and $\{a_i\}_{i=1}^\infty \cup \{b_i\}_{i=1}^\infty = \{c_i\}_{i=1}^\infty$.

[5] We use $\mathcal{X}_i$ to denote the set of elements in X_i.

[6] Given a process $S = (s_j)_{j=1}^\infty$, $S \cap [a,\ b]$ is the truncated process defined as $(s_j)_{j=k}^l$, where $s_{k-1} < a \leq s_k$, and $s_l \leq b < s_{l+1}$.

$(S_i)_{i=1}^n$ *contains an information flow* if $\exists I \subseteq \{1, \ldots, n\}$ such that $(S_i)_{i\in I}$ is an information flow, *i.e.,* $S_i = X_i \bigoplus W_i$ for $i \in I$ and $(X_i)_{i\in I}$ is a pure information flow. Assume that the detector knows Δ but not t_0 or traffic before t_0. This is a nonparametric hypothesis testing; no statistical assumptions are made at this point (although additional assumptions under $\mathcal{H}_0$ are needed for detailed analysis).

To characterize the amount of chaff, we introduce the following definition.

Definition 2.2: If $(S_i)_{i=1}^n$ is an information flow, then its *chaff-to-traffic ratio* (CTR) in the interval $[t_0,\, t_0+t]$ is defined as[7]

$$\mathrm{CTR}(t;\, t_0) = \frac{\sum_{i=1}^{n} |\mathcal{W}_i \cap [t_0,\, t_0+t]|}{\sum_{i=1}^{n} |\mathcal{S}_i \cap [t_0,\, t_0+t]|},$$

i.e., $\mathrm{CTR}(t;\, t_0)$ is the fraction of chaff packets in the interval $[t_0,\, t_0+t]$.

Due to the nonparametricness of $\mathcal{H}_1$, we introduce a novel measure of detection performance.

Definition 2.3: An n-hop detector δ can *tolerate* r ($r \in [0,\, 1]$) fraction of chaff if[8]

1) $\lim_{t\to\infty} P_F(\delta) = 0$;
2) $\lim_{t\to\infty} \sup_{(S_i)_{i=1}^n \in \mathcal{P}} P_M(\delta) = 0$, where[9]

$$\mathcal{P} = \{(X_i \bigoplus W_i)_{i=1}^n : \limsup_{t\to\infty} \mathrm{CTR}(t;\, t_0) \le r \text{ a.s.}\}.$$

That is, δ has vanishing false alarm probability and vanishing miss probability for all n-hop information flows with asymptotic CTR bounded by r almost surely.

The *chaff tolerance* of a detector is the maximum fraction of chaff that it can tolerate.

III. Fundamental Limits on Timing-based Detection

From the detector's point of view, there is no difference between an information-carrying packet and a chaff packet. Therefore, ideally, it is possible for an information flow to mimic any transmission pattern as long as enough chaff can be inserted. It implies that there must be a fundamental limit on the chaff tolerance of any timing-based detector. In this section, we characterize this fundamental limit by CTR_n^* ($n \ge 2$)—the minimum asymptotic CTR needed for an n-hop information flow to mimic $\mathcal{H}_0$. Specifically, for $(S_i)_{i=1}^n$ under $\mathcal{H}_0$,

$$\begin{aligned} \mathrm{CTR}_n^* \quad \triangleq \quad & \inf\{r \in [0,\, 1] : \exists (X_i)_{i=1}^n,\, (W_i)_{i=1}^n \text{ satisfying:} \\ & 1)\ S_i = X_i \bigoplus W_i \text{ for } i = 1, \ldots, n; \\ & 2)\ (X_i)_{i=1}^n \text{ is a pure information flow;} \\ & 3)\ \limsup_{t\to\infty} \mathrm{CTR}(t;\, t_0) \le r \text{ a.s.}\}. \end{aligned} \qquad (1)$$

We calculate CTR_n^* by analyzing the CTR of the optimal chaff-inserting algorithms.

A. Limits on Detecting 2-hop Flows

Suppose that as illustrated in Fig. 3, we are interested in knowing whether R_2 is relaying traffic for R_1, *i.e.,* whether $(S_1,\, S_2)$ forms a 2-hop information flow. Nodes R_1 and R_2 may want to hide the information flow by inserting chaff packets to make their transmission activities independent.

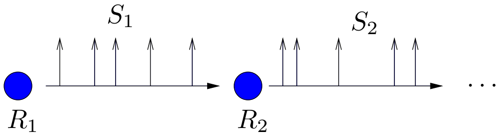

Fig. 3. $\mathcal{H}_1$: $(S_1,\, S_2)$ is a 2-hop information flow.

The problem becomes that given S_i ($i = 1,\, 2$), how to partition it into X_i and W_i such that $(X_1,\, X_2)$ is a pure information flow.

To solve this problem, Blum *et al.* in [8] proposed a greedy algorithm called "Bounded-Greedy-Match" (BGM). As illustrated in Fig. 4, BGM

1) matches every packet transmitted at time s in S_1 with the first unmatched packet transmitted in $[s,\, s+\Delta]$ in S_2;
2) labels all the unmatched packets in S_1 and S_2 as chaff.

It is easy to see that BGM has complexity $O(|\mathcal{S}_1| + |\mathcal{S}_2|)$. Interested readers can find the pseudo code implementation of BGM and all the algorithms in this paper in [12].

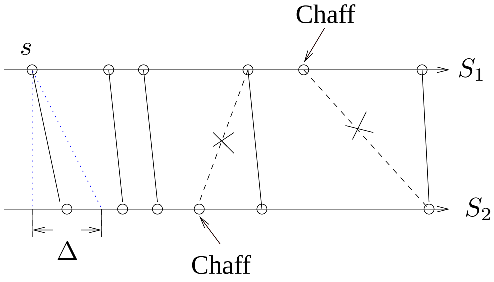

Fig. 4. BGM: a sequential greedy match algorithm.

The output of BGM is a partition of S_i ($i = 1,\, 2$) into $(X_i,\, W_i)$. The CTR of BGM in $[t_0,\, t_0+t]$ is the CTR of this partition in the given interval, denoted by $\mathrm{CTR}_{\text{BGM}}(t;\, t_0)$.

Despite being greedy, BGM has been shown in [8] to be the optimal chaff-inserting algorithm for 2-hop information flows because it minimizes the number of chaff packets for arbitrary traffic[10].

The optimality of BGM allows us to characterize CTR_2^* by analyzing the CTR of BGM. If, in particular, the traffic under $\mathcal{H}_0$ can be modelled as Poisson processes, then we have the following result.

[7] We use $\mathcal{W}_i$ and $\mathcal{S}_i$ to denote the set of elements in W_i and S_i, respectively.

[8] We denote false alarm probability by $P_F(\cdot)$, and miss probability by $P_M(\cdot)$.

[9] Here *a.s.* means "almost surely".

[10] The original proof in [8] is for independent binomial processes, but it holds for arbitrary traffic.

Theorem 3.1: If S_1 and S_2 are independent Poisson processes of rates λ_1 and λ_2, respectively, then with probability one, the CTR of BGM satisfies

$$\lim_{t\to\infty} \mathrm{CTR}_{\mathrm{BGM}}(t;\, t_0) = \begin{cases} \frac{(\lambda_2-\lambda_1)\left(1+\left(\frac{\lambda_1}{\lambda_2}\right)e^{\Delta(\lambda_1-\lambda_2)}\right)}{(\lambda_1+\lambda_2)\left(1-\left(\frac{\lambda_1}{\lambda_2}\right)e^{\Delta(\lambda_1-\lambda_2)}\right)} & \text{if } \lambda_1 \neq \lambda_2, \\ \frac{1}{1+\lambda_1\Delta} & \text{if } \lambda_1 = \lambda_2. \end{cases}$$

Proof: See Appendix. ■

Remark: Suppose that under $\mathcal{H}_0$, S_1 and S_2 are independent Poisson processes with maximum rate λ. Then from Theorem 3.1, it can be shown that $1/(1+\lambda\Delta)$ is the minimum asymptotic CTR for BGM to mimic $\mathcal{H}_0$. By the optimality of BGM, we see that $\mathrm{CTR}_2^* = 1/(1+\lambda\Delta)$.

The value of CTR_2^* establishes a fundamental limit on pairwise detection because if nodes R_1 and R_2 can insert at least CTR_2^* fraction of chaff, they can generate transmission activities according to $\mathcal{H}_0$ and use BGM to schedule the transmissions of information-carrying packets so that no timing-based detector can distinguish the two hypotheses. Hence, CTR_2^* is an upper bound on the maximum chaff tolerance. Note that as $\lambda\Delta \to \infty$, $\mathrm{CTR}_2^* \to 0$; indeed, this result shows that pairwise detection is vulnerable to chaff noise.

In [11], we characterized the asymptotic CTR of BGM for the special case $\lambda_1 = \lambda_2$. Blum *et al.* in [8] gave a different result by ignoring the causality constraint. Donoho *et al.* in [6] claimed that it is possible to detect information flows with arbitrary CTR; their claim, however, is based on the assumption that the chaff processes are independent of the processes of information-carrying packets.

B. Limits on Detecting Multi-hop Flows

In Section III-A, we have established a fundamental limit on pairwise detection. In this section, we extend the results to multi-hop information flows and show that it becomes increasingly difficult to hide an information flow as the length of the flow path increases. Our approach is parallel to that for 2-hop flows. We first develop an optimal chaff-inserting algorithm for multi-hop information flows and then analyze the CTR of that algorithm.

To insert chaff into an n-hop flow ($n \geq 2$), we extend BGM to a recursive greedy algorithm called "Multi-Bounded-Delay-Relay" (MBDR). Given $(S_i)_{i=1}^n$, MBDR

1) matches every packet transmitted at time s_1 in S_1 with the first unmatched packet in the interval $[s_1,\, s_1+\Delta]$ in S_2, conditioned on that this packet has a match in S_3;
2) for $i = 2, \ldots,\, n-1$, matches a packet at s_i in S_i with the first unmatched packet in the interval $[s_i,\, s_i+\Delta]$ in S_{i+1}, conditioned on that this packet has a match in S_{i+2} (assume every packet in S_n has a match);
3) after trying to match all the packets in S_1, labels all the unmatched packets as chaff.

For example, consider the 3-hop information flow illustrated in Fig. 5. To match $s_1 \in \mathbb{S}_1$, MBDR recursively looks for a match for s_2. Since s_2 can be matched with $s_3 \in \mathbb{S}_3$, s_1 is matched with s_2. If s_2 does not have a match in S_3, then MBDR will try to match s_1 with the next unmatched packet in S_2. If there is no more packet left in the interval $[s_1,\, s_1+\Delta]$ in S_2, MBDR labels s_1 as chaff.

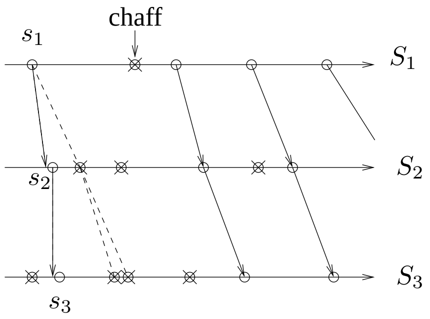

Fig. 5. MBDR: a recursive greedy match algorithm.

Note that for $n = 2$, MBDR is equivalent to BGM. A direct implementation of MBDR has complexity $O((\lambda\Delta)^n|\mathbb{S}_1|)$, where λ is the maximum rate of $S_1, \ldots,\, S_n$. The complexity can be reduced to $O(n^2|\mathbb{S}_1|)$ by expanding the recursions; see [12].

In [11], we developed a chaff-inserting algorithm called "Greedy-Relay-Embedding" (GRE). It can be shown that MBDR and GRE are equivalent except that GRE does not contain recursions. Algorithm GRE has been shown in [11] to find the largest number of matched packets, or equivalently, the minimum number of chaff packets. Therefore, MBDR is optimal.

Let $\mathrm{CTR}_{\mathrm{MBDR}}(t;\, t_0)$ be the CTR of the n-hop information flow $(S_i)_{i=1}^n = (X_i \bigoplus W_i)_{i=1}^n$ partitioned by MBDR. It is proved in [11] that if S_i ($i = 1, \ldots,\, n$) are independent Poisson processes of maximum rate[11] λ, then the asymptotic fraction of information-carrying packets found by GRE is upper bounded by $(1-e^{-\lambda\Delta})^{n-1}$, *i.e.*, with probability one,

$$\lim_{t\to\infty} \mathrm{CTR}_{\mathrm{MBDR}}(t;\, t_0) \geq 1-(1-e^{-\lambda\Delta})^{n-1}. \tag{2}$$

Suppose that under $\mathcal{H}_0$, S_i's are jointly independent Poisson processes with rate up to λ. Then by (2) and the optimality of MBDR, we see that $\mathrm{CTR}_n^* \geq 1-(1-e^{-\lambda\Delta})^{n-1}$. As $n \to \infty$, $\mathrm{CTR}_n^* \to 1$ exponentially fast. Therefore, the information flow will eventually be saturated with chaff as the length of the flow path increases, indicating that it is almost impossible to hide information flows with arbitrarily long paths.

IV. Information Flow Detector

Having established the fundamental limits on detection, we hope to develop detectors to achieve these limits. In this section, we present a general form of detector and analyze its performance.

We propose to detect information flows by a threshold detector based on the optimal chaff-inserting algorithms. Given

[11] The original proof was for equal rate Poisson processes, but it is easily generalizable to the maximum rate case.

$(S_i \cap [t_0,\ t_0+t])_{i=1}^n$ $(n \geq 2)$, the detector is defined as[12]

$$\delta((S_i \cap [t_0,\ t_0+t])_{i=1}^n;\ \tau_n) = \begin{cases} 1 & \text{if } \mathrm{CTR}'(t;\ t_0) \leq \tau_n, \\ 0 & \text{o.w.,} \end{cases}$$

where $\mathrm{CTR}'(t; t_0)$ is the CTR of MBDR on the measurements excluding chaff packets in $S_i \cap [t_0, t_0+(i-1)\Delta)$ $(i = 1, \ldots, n)$. That is, if W_i $(i = 1, \ldots, n)$ are the chaff processes found by MBDR, then

$$\mathrm{CTR}'(t;\ t_0) = \frac{\sum_{i=1}^n |\mathcal{W}_i \cap [t_0+(i-1)\Delta,\ t_0+t]|}{\sum_{i=1}^n |\mathbb{S}_i \cap [t_0,\ t_0+t]|}.$$

The idea behind this detector is to target at the information flows that are the most difficult to detect. Since $\mathrm{CTR}'(t;\ t_0)$ is based on the CTR of the optimal chaff-inserting algorithm and is adjusted (by ignoring chaff in $S_i \cap [t_0,\ t_0+(i-1)\Delta)$) to take into account the packets stored at the relay nodes initially, it is guaranteed to be no larger than the actual CTR in the measurements. Therefore, by making decisions based on $\mathrm{CTR}'(t; t_0)$, we make sure that it is possible to evade detection only if the information flow contains more than τ_n fraction of chaff packets; equivalently, the detector has no miss detection for up to τ_n fraction of chaff.

The threshold needs to be chosen to guarantee vanishing false alarm probability. For pairwise detection, we prove the following result.

Theorem 4.1: Assume that under $\mathcal{H}_0$, S_1 and S_2 are independent Poisson processes of maximum rate λ. If $\tau_2 = 1/(1+\lambda'\Delta)$, then the false alarm probability satisfies

$$\lim_{N\to\infty} \frac{1}{N} \log P_F(\delta) \leq -\Gamma(\lambda,\ \lambda',\ \Delta),$$

where $N = |\mathbb{S}_1 \cap [t_0,\ t_0+t]| + |\mathbb{S}_2 \cap [t_0,\ t_0+t]|$, and $\Gamma(\lambda,\ \lambda',\ \Delta) > 0$ for all $\lambda' > \lambda$.

Proof: See Appendix. ■

Remark: Theorem 4.1 says that the false alarm probability of pairwise detection decays exponentially as long as $\lambda' > \lambda$, or equivalently, $\tau_2 < \mathrm{CTR}_2^*$. Definition of the function $\Gamma(\lambda,\ \lambda',\ \Delta)$ can be found in the proof. A key property of $\Gamma(\lambda,\ \lambda',\ \Delta)$ is that it is an increasing function of λ'.

By similar arguments as in the proof of Theorem 4.1, it can be shown that for general n-hop joint detection, if $\tau_n = \mathrm{CTR}_n^* - \epsilon$ for any $\epsilon > 0$, then the false alarm probability satisfies

$$\lim_{N\to\infty} \frac{1}{N} \log P_F(\delta) \leq -\sigma_n(\epsilon;\ \lambda,\ \Delta),$$

where $\sigma_n(\epsilon;\ \lambda,\ \Delta)$ is positive for all $\epsilon > 0$, and it is an increasing function of ϵ.

The parameter ϵ represents a tradeoff between the chaff tolerance and the false alarm probability. A larger ϵ leads to faster decaying false alarm probability but less tolerance of chaff, whereas a smaller ϵ enables more chaff tolerance at the cost of more false alarms. In particular, as $\epsilon \to 0$, the chaff tolerance of the proposed detector converges to the fundamental limit. Therefore, the detector is optimal in the sense that it provides the maximum chaff tolerance.

Note that although CTR_n^* $(n > 2)$ is unknown, one can choose the threshold by $\tau_n = 1-(1-e^{-\lambda\Delta})^{n-1}$ to guarantee exponentially decaying false alarm probability.

V. Conclusion

This paper presents an information flow detector which has the maximum tolerance of arbitrarily inserted chaff noise. We point out that although the detailed analysis is done for independent Poisson processes, the detector also applies to other types of traffic except that the threshold may need adjustment. The proposed detector coupled with capacity constraints between neighbor nodes can capture all the long-lived information flows with positive rate and sufficiently long paths.

VI. Appendix

A. Proof of Theorem 3.1

Sequentially match packets in S_1 with those in S_2 and let Y_i be the delay of the ith packet, *i.e.*, $Y_i = S_2(i) - S_1(i)$. Define

$$Z_i \overset{\Delta}{=} Y_i - Y_{i-1} = (S_2(i) - S_2(i-1)) - (S_1(i) - S_1(i-1)).$$

We see that Z_i's are i.i.d. random variables, and each Z_i is the difference between two independent exponential random variables with mean $1/\lambda_2$ and $1/\lambda_1$, respectively. The process $\{Y_i\}_{i=1}^\infty$ is a general random walk with steps Z_i's. Define $Y_0 = 0$.

Now for every chaff packet inserted at t in S_2, we insert a virtual packet at t in S_1; for every chaff packet at s in S_1, we insert a virtual packet at $s+\Delta$ in S_2, as illustrated in Fig. 6. Let the new delays after the insertion of virtual packets be $\{Y'_j\}_{j=1}^\infty$. It can be shown that $\{Y'_j\}_{j=1}^\infty$ is also a random walk with steps Z_i's, but it has two reflecting barriers at 0 and Δ, *i.e.*,

$$Y'_j = \min(\max(Y'_{j-1} + Z_j,\ 0),\ \Delta).$$

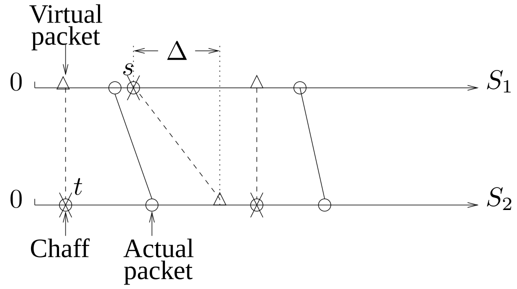

Fig. 6. Inserting virtual packets to calculate the delays of chaff packets.

Since it is almost surely impossible for $Y'_{j-1} + Z_j$ to be exactly equal to 0 or Δ, each time $Y'_j = 0$ or Δ corresponds to an escape across the barriers which results in a chaff packet. Specifically, $Y'_j = 0$ corresponds to a chaff packet in S_2,

[12] Here $\delta(\cdot) = 1$ denotes $\mathcal{H}_1$, and $\delta(\cdot) = 0$ denotes $\mathcal{H}_0$.

and $Y'_j = \Delta$ corresponds to a chaff packet in S_1. Thus, asymptotically, the probability for a packet to be chaff is $h_\Delta/(1-h_0)$ in S_1, and $h_0/(1-h_\Delta)$ in S_2, where $h_0 = \lim_{j\to\infty} \Pr\{Y'_j = 0\}$, and $h_\Delta = \lim_{j\to\infty} \Pr\{Y'_j = \Delta\}$. The overall probability for a packet in $S_1 \bigoplus S_2$ to be chaff is

$$\frac{\lambda_1 h_\Delta}{(\lambda_1+\lambda_2)(1-h_0)} + \frac{\lambda_2 h_0}{(\lambda_1+\lambda_2)(1-h_\Delta)}. \tag{3}$$

To calculate h_0 and h_Δ, let the equilibrium distribution function of Y'_j be $H(x)$, *i.e.*, $H(x) = \lim_{j\to\infty} \Pr\{Y'_j \leq x\}$. It is shown in Example 2.16 in [13] that

$$h_0 = H(0) = \begin{cases} \frac{1-\frac{\lambda_1}{\lambda_2}}{1-\left(\frac{\lambda_1}{\lambda_2}\right)^2 e^{\Delta(\lambda_1-\lambda_2)}} & \text{if } \lambda_1 \neq \lambda_2, \\ \frac{1}{2+\lambda_1\Delta} & \text{o.w.} \end{cases}$$

and

$$h_\Delta = 1-H(\Delta-) = \begin{cases} \frac{\left(\frac{\lambda_1}{\lambda_2}\right) e^{\Delta(\lambda_1-\lambda_2)}\left(1-\frac{\lambda_1}{\lambda_2}\right)}{1-\left(\frac{\lambda_1}{\lambda_2}\right)^2 e^{\Delta(\lambda_1-\lambda_2)}} & \text{if } \lambda_1 \neq \lambda_2, \\ \frac{1}{2+\lambda_1\Delta} & \text{o.w.} \end{cases}$$

By ergodicity of $\{Y'_j\}_{j=1}^{\infty}$, we see that $\text{CTR}_{\text{BGM}}(t;\ t_0)$ converges to (3) almost surely. Therefore, we have that with probability one,

$$\begin{aligned} &\lim_{t\to\infty} \text{CTR}_{\text{BGM}}(t;\ t_0) \\ &= \begin{cases} \frac{(\lambda_2-\lambda_1)\left(1+\left(\frac{\lambda_1}{\lambda_2}\right)e^{\Delta(\lambda_1-\lambda_2)}\right)}{(\lambda_1+\lambda_2)\left(1-\left(\frac{\lambda_1}{\lambda_2}\right)e^{\Delta(\lambda_1-\lambda_2)}\right)} & \text{if } \lambda_1 \neq \lambda_2, \\ \frac{1}{1+\lambda_1\Delta} & \text{if } \lambda_1 = \lambda_2. \end{cases} \end{aligned}$$

■

B. *Proof of Theorem 4.1*

Define T_1 to be the number of packets in $S_1 \bigoplus S_2$ until the first chaff packet, including the first chaff packet, and T_i ($i > 1$) the number of packets between the $(i-1)$th and ith chaff packets, excluding the $(i-1)$th chaff packet but including the ith. Then the false alarm probability can be written as

$$P_F(\delta) = \Pr\{\frac{1}{N'}\sum_{i=1}^{N'} T_i \geq 1 + \lambda'\Delta\}, \tag{4}$$

where $N' = N/(1+\lambda'\Delta)$.

Define Y_i the same as in the proof of Theorem 3.1. For $i \geq 2$, T_i's are *i.i.d.* with the distribution

$$\inf\{n : Y_n < 0 \text{ or } Y_n > \Delta \mid Y_0 = 0\}. \tag{5}$$

Now that $\max(\lambda_1,\ \lambda_2) \leq \lambda$, by Theorem 3.1, we know that the asymptotic CTR of BGM is no smaller than $1/(1+\lambda\Delta)$ almost surely, *i.e.*, $\lim_{c\to\infty} \frac{1}{c}\sum_{i=1}^{c} T_i \leq 1 + \lambda\Delta$ almost surely, which implies that $\mathbb{E}[T_2] \leq 1 + \lambda\Delta$. By Sanov's Theorem [14], we have that

$$\begin{aligned} \lim_{N'\to\infty} \frac{1}{N'} \log \Pr\{\frac{1}{N'}\sum_{i=1}^{N'} T_i \geq 1 + \lambda'\Delta\} = \\ -\min_{W:\, \mathbb{E}[W]\geq 1+\lambda'\Delta} D(W||T_2). \end{aligned}$$

Plugging in (4) yields that

$$\begin{aligned} \lim_{N\to\infty} \frac{1}{N} \log P_F(\delta) &= -\frac{1}{1+\lambda'\Delta} \min_{\mathbb{E}[W]\geq 1+\lambda'\Delta} D(W||T_2) \\ &\leq -\Gamma(\lambda,\ \lambda',\ \Delta), \end{aligned}$$

where

$$\Gamma(\lambda,\ \lambda',\ \Delta) \stackrel{\Delta}{=} \frac{1}{1+\lambda'\Delta} \min_{\mathbb{E}[W]\geq 1+\lambda'\Delta} D(W||\tilde{T}_2),$$

and $\tilde{T}_2$ is defined in (5) but for the special case $\lambda_1 = \lambda_2 = \lambda$. For $\lambda' > \lambda$ (assume $\Delta > 0$), we have $\mathbb{E}[W] > \mathbb{E}[\tilde{T}_2]$, and therefore $\Gamma(\lambda,\ \lambda',\ \Delta) > 0$.

■

References

[1] S. Staniford-Chen and L. Heberlein, "Holding intruders accountable on the internet," in *Proc. the 1995 IEEE Symposium on Security and Privacy*, (Oakland, CA), pp. 39–49, May 1995.

[2] X. Wang, D. Reeves, S. Wu, and J. Yuill, "Sleepy watermark tracing: An active network-based intrusion response framework," in *Proc. of the 16th International Information Security Conference*, pp. 369–384, 2001.

[3] Y. Zhang and V. Paxson, "Detecting stepping stones," in *Proc. the 9th USENIX Security Symposium*, pp. 171–184, August 2000.

[4] K. Yoda and H. Etoh, "Finding a connection chain for tracing intruders," in *6th European Symposium on Research in Computer Security, Lecture Notes in Computer Science 1895*, (Toulouse, France), October 2000.

[5] X. Wang, D. Reeves, and S. Wu, "Inter-packet delay-based correlation for tracing encrypted connections through stepping stones," in *7th European Symposium on Research in Computer Security, Lecture Notes in Computer Science 2502*, pp. 244–263, 2002.

[6] D. Donoho, A. Flesia, U. Shankar, V. Paxson, J. Coit, and S. Staniford, "Multiscale stepping-stone detection: Detecting pairs of jittered interactive streams by exploiting maximum tolerable delay," in *5th International Symposium on Recent Advances in Intrusion Detection, Lecture Notes in Computer Science 2516*, 2002.

[7] X. Wang and D. Reeves, "Robust correlation of encrypted attack traffic through stepping stones by manipulation of inter-packet delays," in *Proc. of the 2003 ACM Conference on Computer and Communications Security*, pp. 20–29, 2003.

[8] A. Blum, D. Song, and S. Venkataraman, "Detection of Interactive Stepping Stones: Algorithms and Confidence Bounds," in *Conference of Recent Advance in Intrusion Detection (RAID)*, (Sophia Antipolis, French Riviera, France), September 2004.

[9] P. Peng, P. Ning, D. Reeves, and X. Wang, "Active Timing-Based Correlation of Perturbed Traffic Flows with Chaff Packets," in *Proc. 25th IEEE International Conference on Distributed Computing Systems Workshops*, (Columbus, OH), pp. 107–113, June 2005.

[10] L. Zhang, A. Persaud, A. Johson, and Y. Guan, "Detection of Stepping Stone Attack under Delay and Chaff Perturbations," in *Proc. of the 25th IEEE International Performance Computing and Communications Conference (IPCCC 2006)*, (Phoenix, AZ), April 2006.

[11] T. He, P. Venkitasubramaniam, and L. Tong, "Packet scheduling against stepping-stone attacks with chaff," in *Proc. IEEE Military Communications Conference*, (Washington,DC), October 2006.

[12] T. He and L. Tong, "Chaff-inserting Algorithms and Robust Detection Algorithms for Information Flows," Tech. Rep. ACSP-TR-02-07-01, Cornell University, February 2007. `http://acsp.ece.cornell.edu/pubR.html`.

[13] D. Cox and H. Miller, *The Theory of Stochastic Processes*. New York: John Wiley & Sons Inc., 1965.

[14] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley & Sons, Inc., 1991.