TIMING-BASED DETECTION OF PACKET FORWARDING IN MANETS

Jinsub Kim and Lang Tong

School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14853
Email: {jk752, lt35}@cornell.edu

ABSTRACT

In mobile ad hoc networks (MANETs), timing information is easily available due to the use of a shared medium, even when the traffic is encrypted. This paper addresses how such timing information can be used for detecting packet forwarding activities in MANETs.

Our results depend in part on the previous results on unidirectional flow detection. We first provide further analysis for the unidirectional flow detector proposed in [1], under the independent Poisson chaff assumption. Regardless of the fraction of chaff, it is shown that flows can be detected consistently, and the false alarm probability decays exponentially fast as the sample size grows.

Then, we consider the detection of packet forwarding. Our approach is based on the duality between packet forwarding and unidirectional flows. We propose a threshold-based detector and conclude that its performance characteristic is the same with that of the unidirectional flow detector.

1. INTRODUCTION

Timing information of a node in a mobile ad hoc network (MANET) is easily available to other nodes in its transmission range, even in the case of encrypted traffic. Both detection systems and network intruders can acquire the timing information and make use of it as needed. Especially, this paper addresses how timing information can be used for detecting packet forwarding between a pair of nodes.

Our objective is to detect whether there exists packet forwarding between a pair of nodes R_1 and R_2. We assume that end-to-end delays are uniformly bounded above by a positive real number Δ. This assumption is valid if the MANET is carrying packets of a real time application (*e.g.*, audio/video streaming or Voice over IP (VoIP) application). Our detector is supposed to observe only the transmission epochs of each node, so that it is applicable to encrypted traffic. In practice, a node can multiplex different traffic in its transmissions, and it can also introduce dummy transmissions to confuse a detection system. Hence, even when there exists packet forwarding between R_1 and R_2, some transmission epochs of the nodes might not belong to the packet forwarding, and such epochs are referred to as *chaff*.

As illustrated in Fig. 1, adversary nodes may compromise some nodes in a MANET and use them to acquire useful information or spread harmful information to innocent nodes. Then, our detection algorithm can single out the compromised nodes by detecting packet forwarding between them and adversaries. On the other hand, the algorithm can be employed by adversaries to gather preliminary information before launching attacks.

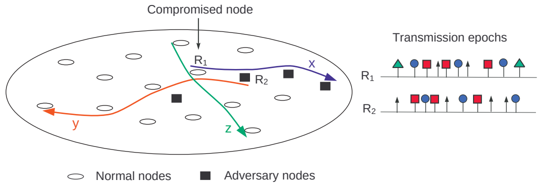

Fig. 1: Epochs with circles, rectangles, triangles, and arrows are epochs of the flow x, y, z, and chaff, respectively. Adversaries acquire information thourgh the flow x, and spread harmful packets via the flow y.

1.1. Related Work

This work was motivated by a series of papers about the detection of unidirectional information flows, which has been studied in the context of the stepping-stone detection [2]. Especially, to deal with encrypted traffic, timing characteristics are used in detection. Donoho *et al.* [3] employed a flow model with a maximum delay constraint, and proposed a multiscale analysis for detection. Chaff noise was briefly mentioned with the claim that flows can be detected if the chaff noise is independent of flows. Zhang *et al.* [4] also proposed a timing-based detection of flows with bounded delay and dealt with the insertion of independent chaff, but they assumed that only one node can insert chaff transmissions.

The problem becomes more challenging if the nodes are allowed to insert chaff in an arbitrary way to hide flows. Blum *et al.* [5] proposed a counting-based detector and modified their detector to deal with arbitrary chaff insertion, but it can handle only a limited number of chaff epochs. For arbitrary chaff insertion, [6] first presented a timing-based detector that can perform consistent detection even if the amount of chaff grows linearly with the traffic size, and every node can insert chaff epochs. Moreover, it is shown in [1] that there exists a threshold on the fraction of chaff below which consistent detection is guaranteed by a single detector and beyond which the flows can be completely hidden.

Although there have been successful studies about detection of unidirectional flows, most of them excluded the possibility of bidirectional communication which is quite common in MANETs. Hence, those results are not directly applicable to the detection of packet forwarding. To our best knowledge, this is the first attempt to detect packet forwarding in MANETs based on timing information.

1.2. Summary of Results and Organization

First, we show that the unidirectional flow detector proposed in [1] is consistent regardless of the fraction of chaff if the chaff portion of two nodes are independent Poisson processes. Furthermore, the false alarm probability decays exponentially fast as the sample size grows. Donoho *et al.* [3] also claimed the detectability of flows under the

Work in this paper was sponsored by National Science Foundation under Contract CCF-0728872 and Army Research Office MURI Program under award W911NF-08-1-0238. The first author was partially supported by Samsung Scholarship.

independent chaff assumption. However, their multiscale analysis is difficult to be applied on a real-time basis. In contrast, our detector can operate on a real-time basis, and the behavior of error probabilities is well analyzed under the Poisson assumption.

Secondly, we present a threshold-based detection algorithm for packet forwarding detection. There exists a duality between packet forwarding and unidirectional flows. Based on the duality, we conclude that the packet forwarding detector has the same performance characteristics with the unidirectional flow detector. For arbitrary chaff insertion, there exists a phase transition in detectability with respect to the fraction of chaff. And, if the chaff portions of two nodes are independent Poisson processes, then packet forwarding can be detected consistently regardless of the fraction of chaff.

The rest of the paper is organized as follows. Section 2 introduces the notations and mathematical models employed in this paper. In section 3, we study the unidirectional flow detection under independent chaff assumption, and present numerical results. Section 4 introduces the packet forwarding detection problem and proposes a detection scheme and its performance analysis. Finally, section 5 concludes the paper with remarks on its contributions.

2. MATHEMATICAL MODELS

We model the transmission epochs of each node as a point process. Uppercase bold letters (*e.g.*, $\mathbf{S}$) denote point processes, and lowercase bold letters (*e.g.*, $\mathbf{s}$) denote their realizations. For a point process $\mathbf{S}$, $S(i)$ denotes the ith transmission epoch and $s(i)$ denotes its realization. Given realizations of two point processes, $(a_1,\, a_2, \ldots)$ and $(b_1,\, b_2, \ldots)$, $\bigoplus$ is the *superposition operator* defined as $(a_k)_{k=1}^{\infty} \oplus (b_k)_{k=1}^{\infty} = (c_k)_{k=1}^{\infty}$, where $c_1 \leq c_2 \leq \ldots$ and $\{a_k\}_{k=1}^{\infty} \cup \{b_k\}_{k=1}^{\infty} = \{c_k\}_{k=1}^{\infty}$. And, given a realization $\mathbf{s}$, we use $\mathcal{S}$ to denote a set of all epochs in $\mathbf{s}$. An *information flow* with a maximum delay constraint Δ can be formally defined as follows [1].

Definition 2.1 *An ordered pair of processes* $(\mathbf{F}_1,\, \mathbf{F}_2)$ *forms an* information flow *if for every realization* $(\mathbf{f}_1,\, \mathbf{f}_2)$*, there exists a bijection* $g : \mathcal{F}_1 \rightarrow \mathcal{F}_2$ *such that* $0 \leq g(s) - s \leq \Delta$ *for all* $s \in \mathcal{F}_1$*.*

The bijection condition means *packet conservation*, and $g(s) - s \in [0,\, \Delta]$ implies *causality* and *the delay bound* Δ.

3. DETECTION OF UNIDIRECTIONAL FLOWS

3.1. Problem Statement

Let $\mathbf{S}_1$ and $\mathbf{S}_2$ denote the transmission processes of R_1 and R_2, respectively. By observing $\mathbf{S}_1$ and $\mathbf{S}_2$ for some time t $(t > 0)$, we want to test the following hypotheses:

$$\begin{array}{ll} \mathcal{H}_0: & \mathbf{S}_1 \text{ and } \mathbf{S}_2 \text{ are jointly independent} \\ \mathcal{H}_1: & (\mathbf{S}_1,\, \mathbf{S}_2) \text{ contains an information flow} \end{array} \tag{1}$$

$(\mathbf{S}_1,\, \mathbf{S}_2)$ is defined to *contain an information flow* if $(\mathbf{S}_i)_{i=1}^2$ can be partitioned into an information flow $(\mathbf{F}_i)_{i=1}^2$ and a chaff part $(\mathbf{W}_i)_{i=1}^2$. Note that this hypothesis testing is applicable only if there can exist a flow in only one direction and the direction is known priorly, and such conditions are unrealistic in MANETs. However, the analysis given in this section takes an important role in solving the packet forwarding detection problem in section 4.

3.2. Fundamental Limit of Timing-based Detection

Using timing information alone imposes a limit in detecting unidirectional flows under the presence of chaff. Because, intuitively, any realizations of independent processes $\mathbf{S}_1$ and $\mathbf{S}_2$ can be decomposed into a flow part and a chaff part if the rate of the information flow is sufficiently low. Hence, for an information flow to be detected, the strength of the flow needs to be strong enough. Under $\mathcal{H}_1$, the strength of a flow can be measured by *chaff-to-traffic ratio* (CTR) defined as follows.

Definition 3.1 *[1] Given the realizations of an information flow* $(\mathbf{f}_i)_{i=1}^2$ *and chaff noise* $(\mathbf{w}_i)_{i=1}^2$*, the* chaff-to-traffic ratio *(CTR) is defined as*

$$\mathit{CTR}(t) \triangleq \frac{\sum_{i=1}^{2} |\mathcal{W}_i \cap [0,\, t]|}{\sum_{i=1}^{2} |(\mathcal{F}_i \cup \mathcal{W}_i) \cap [0,\, t]|}, \tag{2}$$

$$\mathit{CTR} \triangleq \limsup_{t \to \infty} \mathit{CTR}(t)$$

To evaluate the performance of detection algorithms, we borrow the following notion of *Chernoff-consistent* detection [7].

Definition 3.2 *[1] Let* δ_t *be a detector that uses all timing data up to time t. The detector* δ_t *is called* r-consistent *(*$r \in [0,\, 1]$*) if it is Chernoff-consistent for all the information flows with CTR bounded almost surely by* r*. In other words, the false alarm probability* $P_F(\delta_t)$ *and the miss probability* $P_M(\delta_t)$ *satisfy the following:*

1. $\lim_{t \to \infty} P_F(\delta_t) = 0$ *for any* $(\mathbf{S}_i)_{i=1}^2$ *under* $\mathcal{H}_0$*;*
2. $\sup_{(\mathbf{S}_i)_{i=1}^2 \in \mathcal{P}} \lim_{t \to \infty} P_M(\delta_t) = 0$*, where*

$$\begin{aligned} \mathcal{P} = \{(\mathbf{S}_i)_{i=1}^2 :\ & (\mathbf{S}_i)_{i=1}^2 \textit{ contains an information flow,} \\ & \textit{and } \limsup_{t \to \infty} \mathit{CTR}(t) \leq r \textit{ a.s.}\}. \end{aligned}$$

3.3. Background: Detect-Bounded-Delay

In [1], He and Tong proposed a threshold-based detector, called Detect-Bounded-Delay (DBD), and provided its performance analysis for arbitrary chaff insertion. DBD calculates a lower bound $\widehat{\text{CTR}}(t)$ of the true CTR(t) and compares it with a predefined threshold τ. Specifically, DBD takes the following form

$$\begin{cases} \text{declare } \mathcal{H}_0 & \text{if } \widehat{\text{CTR}}(t) > \tau \\ \text{declare } \mathcal{H}_1 & \text{if } \widehat{\text{CTR}}(t) \leq \tau \end{cases} \tag{3}$$

Given the realizations $\mathbf{s}_1$ and $\mathbf{s}_2$, the test statistic $\widehat{\text{CTR}}(t)$ is calculated by the following optimization

$$\widehat{\text{CTR}}(t) \triangleq \min_{\mathbf{f}_i, \mathbf{w}_i : \mathbf{s}_i = \mathbf{f}_i \oplus \mathbf{w}_i \sim \mathcal{H}_1} \frac{\sum_{i=1}^{2} |\mathcal{W}_i \cap [0,\, t]|}{\sum_{i=1}^{2} |(\mathcal{F}_i \cup \mathcal{W}_i) \cap [0,\, t]|} \tag{4}$$

where $\mathbf{s}_i = \mathbf{f}_i \oplus \mathbf{w}_i \sim \mathcal{H}_1$ stands for the constraint that $(\mathbf{f}_1,\, \mathbf{f}_2)$ is a realization of an information flow with a delay bound Δ.

In [5], Blum *et al.* gave an algorithm, called Bounded-Greedy-Match (BGM), that achieves the above optimization. Given the measurements $(\mathbf{s}_i)_{i=1}^2$, BGM works as follows:

1. Let s be the earliest epoch in $\mathcal{S}_1$. Match s with the first unmatched epoch in $[s,\, s+\Delta]$ in $\mathcal{S}_2$.
2. Move to the next epoch t in $\mathcal{S}_1$. Match t with the first unmatched epoch in $[t,\, t+\Delta]$ in $\mathcal{S}_2$. Keep moving to the next epoch in $\mathcal{S}_1$ and finding its match based on the same rule.
3. After the trial to match the last epoch in $\mathcal{S}_1$, label all the unmatched epochs as chaff and terminate.

For the implementation of BGM, please refer to table 3 in [1]. In [1], for two independent Poisson processes $\mathbf{S}_1$ and $\mathbf{S}_2$, $\widehat{\text{CTR}}(t)$ was shown to converge almost surely to a certain value.

Theorem 3.1 *[1] If $\mathbf{S}_1$ and $\mathbf{S}_2$ are independent Poisson processes with rates λ_1 and λ_2, respectively, then $\widehat{CTR}(t)$ satisfies the following with probability one.*

$$\lim_{t\to\infty} \widehat{CTR}(t) = \begin{cases} \frac{(\lambda_2-\lambda_1)(1+(\frac{\lambda_1}{\lambda_2})e^{\Delta(\lambda_1-\lambda_2)})}{(\lambda_2+\lambda_1)(1-(\frac{\lambda_1}{\lambda_2})e^{\Delta(\lambda_1-\lambda_2)})} & \textit{if } \lambda_1 \neq \lambda_2 \\ \frac{1}{1+\lambda\Delta} & \textit{if } \lambda_1 = \lambda_2 = \lambda \end{cases}$$

Based on theorem 3.1, the following theorem states the consistency of DBD under arbitrary chaff insertion.

Theorem 3.2 *[1] Suppose that $\mathbf{S}_1$ and $\mathbf{S}_2$ under $\mathcal{H}_0$ are independent Poisson processes, and τ_0 denotes $\lim_{t\to\infty} \widehat{CTR}(t)$ under $\mathcal{H}_0$. If the threshold τ of DBD satisfies $\tau < \tau_0$, then DBD is τ-consistent. In addition, the false alarm probability decays exponenentially fast as the sample size grows.*

On the other hand, if the fraction of chaff is allowed to be greater than τ_0, then the nodes can hide flows by mimicking $\mathcal{H}_0$ based on the schedule found by BGM.

3.4. Detectability under Independent Chaff Assumption

In this section, under the assumption that chaff portions of two nodes can be modeled as independent Poisson processes, we show that DBD is able to detect flows regardless of how high the fraction of chaff is. The first step of the proof is to calculate an upper bound of $\limsup_{t\to\infty} \widehat{\text{CTR}}(t)$ under $\mathcal{H}_1$ as follows.

Lemma 3.1 *Suppose that $\mathbf{S}_1$ and $\mathbf{S}_2$ have the rates λ_1 and λ_2, respectively, and $(\mathbf{S}_1,\, \mathbf{S}_2)$ contains an information flow with the rate λ_f. If the chaff portions of R_1 and R_2 can be modeled as independent Poisson processes, then $\limsup_{t\to\infty} \widehat{CTR}(t)$ satisfies the following inequality with probability one.*

$$\limsup_{t\to\infty} \widehat{CTR}(t) \leq \begin{cases} \frac{(\lambda_2-\lambda_1)(1+(\frac{\lambda_1-\lambda_f}{\lambda_2-\lambda_f})e^{\Delta(\lambda_1-\lambda_2)})}{(\lambda_2+\lambda_1)(1-(\frac{\lambda_1-\lambda_f}{\lambda_2-\lambda_f})e^{\Delta(\lambda_1-\lambda_2)})} & \textit{if } \lambda_1 \neq \lambda_2 \\ \frac{\lambda-\lambda_f}{\lambda(1+(\lambda-\lambda_f)\Delta)} & \textit{if } \lambda_1 = \lambda_2 = \lambda \end{cases}$$

Proof: $N(t)$, $N_f(t)$, and $N_c(t)$ are random variables denoting the true number of total epochs, information flow epochs, and chaff epochs in $(\mathbf{S}_i)_{i=1}^2$ until time t. In addition, $C(t)$ is a random variable denoting the number of chaff epochs found by running BGM over $(\mathbf{S}_i)_{i=1}^2$ until time t. Because $(\mathbf{S}_i)_{i=1}^2$ contains an information flow, it is a superposition of the flow part $(\mathbf{F}_i)_{i=1}^2$ and the chaff part $(\mathbf{W}_i)_{i=1}^2$. By the assumptions of the theorem, $\mathbf{W}_1$ and $\mathbf{W}_2$ are independent Poisson processes with the rates $\lambda_1 - \lambda_f$ and $\lambda_2 - \lambda_f$, respectively.

Consider running BGM on $(\mathbf{F}_i)_{i=1}^2$ and $(\mathbf{W}_i)_{i=1}^2$ separately until time t, and denote the total number of the chaff epochs found in this way by $\hat{C}(t)$. Let $\text{CTR}_W(t)$ denote the resulting chaff-to-traffic ratio when we run BGM over $(\mathbf{W}_i)_{i=1}^2$ until time t. Because running BGM over the whole measurements is the optimal partitioning to minimize the chaff portion, running BGM separately over the flow part and the chaff part will result more number of chaff epochs. In other words, the optimality of BGM implies that $\hat{C}(t)$ is greater than or equal to $C(t)$. In addition, since running BGM on $(\mathbf{F}_i)_{i=1}^2$ results no chaff, $\hat{C}(t)$ is the number of chaff epochs resulting from running BGM over $(\mathbf{W}_i)_{i=1}^2$ until time t. Hence,

$$C(t) \leq \hat{C}(t) = N_c(t)(\text{CTR}_W(t)).$$

Dividing both sides by $N(t)$ leads to

$$\frac{C(t)}{N(t)} \leq \frac{N_c(t)}{N(t)}(\text{CTR}_W(t)) = \frac{N_c(t)/t}{N(t)/t}(\text{CTR}_W(t)). \qquad (5)$$

We have

$$\frac{C(t)}{N(t)} = \widehat{\text{CTR}}(t),\ \lim_{t\to\infty} \frac{N_c(t)/t}{N(t)/t} = \frac{\lambda_1+\lambda_2-2\lambda_f}{\lambda_1+\lambda_2} \text{ a.s.,}$$
$$\lim_{t\to\infty} \text{CTR}_W(t) = \text{CTR}_{H0}[\lambda_1-\lambda_f,\, \lambda_2-\lambda_f] \text{ a.s..}$$

where $\text{CTR}_{H0}[x_1,\, x_2]$ stands for the value of $\lim_{t\to\infty} \widehat{\text{CTR}}(t)$ when $\mathbf{S}_1$ and $\mathbf{S}_2$ are independent Poisson processes with the rates x_1 and x_2, respectively. Hence, taking the supremum limit of both sides in (5) results in

$$\limsup_{t\to\infty} \widehat{\text{CTR}}(t) \leq \frac{\lambda_1+\lambda_2-2\lambda_f}{\lambda_1+\lambda_2} \text{CTR}_{H0}[\lambda_1-\lambda_f,\, \lambda_2-\lambda_f] \text{ a.s.}$$

Above, replacing $\text{CTR}_{H0}[\lambda_1-\lambda_f,\, \lambda_2-\lambda_f]$ with the closed-form expression given in theorem 3.1 finishes the proof. ∎

Based on lemma 3.1, the following theorem guarantees the consistency of DBD under independent Poisson chaff assumption.

Theorem 3.3 *Suppose that (i) under $\mathcal{H}_0$, $\mathbf{S}_1$ and $\mathbf{S}_2$ are Poisson processes, and (ii) under $\mathcal{H}_1$, the chaff portions of R_1 and R_2 are independent Poisson processes. In addition, the transmission rates of R_1 and R_2 are λ_1 and λ_2, respectively. Then, for any $\rho \in (\frac{|\lambda_1-\lambda_2|}{\lambda_1+\lambda_2},\, 1)$, there exists a proper threshold τ for DBD, such that DBD is ρ-consistent. Especially, the following τ can be used.*

$$\tau = \begin{cases} \frac{(\lambda_2-\lambda_1)(1+(\frac{\lambda_1(3+\rho)-\lambda_2(1-\rho)}{\lambda_2(3+\rho)-\lambda_1(1-\rho)})e^{\Delta(\lambda_1-\lambda_2)})}{(\lambda_2+\lambda_1)(1-(\frac{\lambda_1(3+\rho)-\lambda_2(1-\rho)}{\lambda_2(3+\rho)-\lambda_1(1-\rho)})e^{\Delta(\lambda_1-\lambda_2)})} & \textit{if } \lambda_1 \neq \lambda_2 \\ \frac{1+\rho}{2+\lambda(1+\rho)\Delta} & \textit{if } \lambda_1 = \lambda_2 = \lambda \end{cases}$$

Moreover, the false alarm probability decays exponentially fast as the sample size grows.

Proof: Fix $\rho \in (\frac{|\lambda_1-\lambda_2|}{\lambda_1+\lambda_2},\, 1)$, and define τ as given in the theorem's statement. Then, $\rho < \frac{\rho+1}{2} < 1$. In addition, define $\hat{\lambda}_f$ to be the value satisfying $\frac{\rho+1}{2} = \frac{\lambda_1+\lambda_2-2\hat{\lambda}_f}{\lambda_1+\lambda_2}$ or equivalently $\hat{\lambda}_f = \frac{(\lambda_1+\lambda_2)(1-\rho)}{4}$. In other words, $\hat{\lambda}_f$ is the rate of the information flow when the fraction of chaff is $\frac{\rho+1}{2}$, and $\frac{\rho+1}{2} < 1$ implies that $\hat{\lambda}_f > 0$. Now, let $h(x) \triangleq \frac{\lambda_1+\lambda_2-2x}{\lambda_1+\lambda_2}\text{CTR}_{H0}[\lambda_1-x,\, \lambda_2-x]$. We can easily

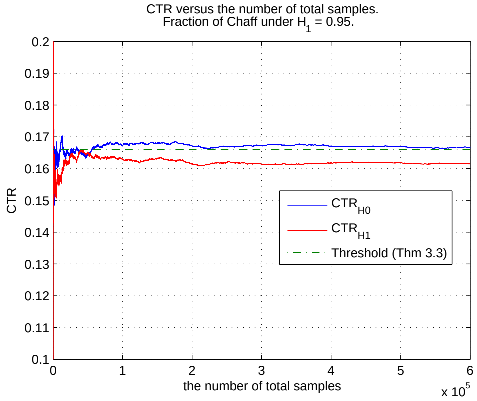

Fig. 2: $\widehat{\mathrm{CTR}}$ versus the number of total samples. $\lambda_1 = \lambda_2 = 10$. Fraction of chaff under $\mathcal{H}_1$ = 0.95. $\Delta = 0.5$.

check that $h(x)$ is strictly decreasing in $[0,\ \min(\lambda_1, \lambda_2)]$, and τ is equal to $h(\hat{\lambda}_f)$.

(i) Miss detection probability: Under $\mathcal{H}_1$, consider the case that CTR is no greater than ρ. If λ_f is the rate of the information flow, then $\lambda_f = \frac{(\lambda_1+\lambda_2)(1-\mathrm{CTR})}{2} > \bar{\lambda}_f \triangleq \frac{(\lambda_1+\lambda_2)(1-(3\rho+1)/4)}{2} > \hat{\lambda}_f$, because CTR $\leq \rho < \frac{3\rho+1}{4} < \frac{\rho+1}{2}$. Then, lemma 3.1 and the monotonicity of h give, under $\mathcal{H}_1$ when CTR $\leq \rho$,

$$\limsup_{t\to\infty} \widehat{\mathrm{CTR}}(t) \leq h(\lambda_f) < h(\bar{\lambda}_f) < h(\hat{\lambda}_f) = \tau \ \text{ a.s.}$$

Hence, if CTR $\leq \rho$, $\lim_{t\to\infty} \Pr(\widehat{\mathrm{CTR}}(t) > \tau) = 0$, meaning the vanishing miss detection probability.

(ii) False alarm probability: Under $\mathcal{H}_0$,

$$\lim_{t\to\infty} \widehat{\mathrm{CTR}}(t) = \mathrm{CTR}_{H0}[\lambda_1,\ \lambda_2] = h(0) > h(\hat{\lambda}_f) = \tau \ \text{ a.s.}$$

and theorem 6.4 in [1] imply the exponential decay of the false alarm probability. Thus, DBD with the threshold τ is ρ-consistent. ■

For any ρ less than 1, theorem 3.3 can give us a ρ-consistent detector if the chaff portions are independent Poisson processes.

3.5. Numerical Results: Independent Chaff Processes

This section presents a numerical result for the detectability under independent Poisson chaff assumption. $(\mathbf{S}_i)_{i=1}^2$ under $\mathcal{H}_0$ and $(\mathbf{F}_i)_{i=1}^2$, $(\mathbf{W}_i)_{i=1}^2$ under $\mathcal{H}_1$ are all modeled as Poisson processes. Delays are i.i.d. and uniformly distributed in $[0,\ \Delta]$. Fig. 2 shows the plots of $\widehat{\mathrm{CTR}}(t)$ with respect to the number of total epochs observed. Under $\mathcal{H}_1$, the fraction of chaff was set to be 0.95, meaning that 95 percent of epochs are chaff noise. Neverthless, we can see that $\widehat{\mathrm{CTR}}$ values of two hypotheses become completely separable, as the sample size grows. The dashed straight line between two $\widehat{\mathrm{CTR}}$ plots is the threshold τ given in theorem 3.3.

4. DETECTION OF PACKET FORWARDING

4.1. Problem Statement

This section deals with timing-based detection of packet forwarding. By observing $\mathbf{S}_1$ and $\mathbf{S}_2$ for some time t ($t > 0$), we want to test the following hypotheses.

$\mathcal{H}_0$: $\mathbf{S}_1$ and $\mathbf{S}_2$ are jointly independent
$\mathcal{H}_1$: $(\mathbf{S}_1,\ \mathbf{S}_2)$, $(\mathbf{S}_2,\ \mathbf{S}_1)$, or both contain an information flow

The above is different from the problem in section 3.1 in that R_1 and R_2 are allowed to have flows in either or both directions under $\mathcal{H}_1$.

4.2. Packet-Forward-Detect

In this section, we propose a threshold-based detector referred to as Packet-Forward-Detect (PFD). PFD first calculates a lower bound $\widetilde{\mathrm{CTR}}(t)$ of the true $\mathrm{CTR}(t)$. Then, it compares $\widetilde{\mathrm{CTR}}(t)$ to a predefined threshold τ and makes a decision. PFD takes the following form,

$$\begin{cases} \text{declare } \mathcal{H}_0 & \text{if } \widetilde{\mathrm{CTR}}(t) > \tau \\ \text{declare } \mathcal{H}_1 & \text{if } \widetilde{\mathrm{CTR}}(t) \leq \tau \end{cases} \qquad (6)$$

Given $(\mathbf{s}_i)_{i=1}^2$, $\widetilde{\mathrm{CTR}}(t)$ is obtained by the below optimization.

$$\min_{\substack{\mathbf{f}_i^{12},\, \mathbf{f}_i^{21},\, \mathbf{w}_i\ :\\ \mathbf{s}_i = (\mathbf{f}_i^{12} \oplus \mathbf{f}_i^{21}) \oplus \mathbf{w}_i \sim \mathcal{H}_1}} \frac{\sum_{i=1}^{2} |\mathcal{W}_i \cap [0,\ t]|}{\sum_{i=1}^{2} |(\mathcal{F}_i^{12} \cup \mathcal{F}_i^{21} \cup \mathcal{W}_i) \cap [0,\ t]|}$$

where $\mathbf{s}_i = (\mathbf{f}_i^{12} \oplus \mathbf{f}_i^{21}) \oplus \mathbf{w}_i \sim \mathcal{H}_1$ stands for the constraint that $(\mathbf{f}_1^{12},\ \mathbf{f}_2^{12})$ and $(\mathbf{f}_2^{21},\ \mathbf{f}_1^{21})$ are realizations of information flows with a delay bound Δ.

The above optimization can be achieved by a matching algorithm called Bidirectional-Bounded-Greedy-Match (BiBGM). As the name stands, BiBGM can be understood as a bidirectional version of BGM. Given the measurements $(\mathbf{s}_i)_{i=1}^2$, BiBGM works as follows:

1. Let s be the earliest epoch in $\mathcal{S}_1 \cup \mathcal{S}_2$. Match s with the first unmatched epoch in $[s,\ s+\Delta]$ in the other node.
2. Move to the next unmatched epoch t in $\mathcal{S}_1 \cup \mathcal{S}_2$. Match t with the first unmatched epoch in $[t,\ t+\Delta]$ in the other node. Keep moving to the next unmatched epoch in $\mathcal{S}_1 \cup \mathcal{S}_2$ and finding its match based on the same rule.
3. After the trial to match the last unmatched epoch, label all the unmatched epochs as chaff and terminate.

The implementation of PFD is given in Table 1, and BiBGM is included in lines 1-12. Its computational complexity is $O(|\mathcal{S}_1| + |\mathcal{S}_2|)$. In addition, if an epoch is once labeled as chaff or matched to another, BiBGM no longer needs the epoch for processing newly incoming observations. Combined with the linear complexity, such characteristic makes PFD applicable on a real-time basis. To show the optimality of BiBGM, we introduce the following lemma regarding the relation between BiBGM and BGM.

Lemma 4.1 *Running BiBGM on $(\mathbf{s}_i)_{i=1}^2$ is equivalent to:*

1. *Increase all the epochs of $\mathbf{s}_2$ by Δ.*
2. *Apply BGM with the delay constraint 2Δ to the modified measurements.*

Proof: Let $\hat{\mathbf{s}}_2$ be a sequence generated by increasing every epoch in $\mathbf{s}_2$ by Δ (*i.e.*, $\hat{s}_2(i) = s_2(i) + \Delta,\ 1 \leq i \leq |\mathcal{S}_2|$). The concrete steps of BiBGM are shown in table 1. There, we can replace $s_2(n)$ with $\hat{s}_2(n) - \Delta$, and rewrite the steps as follows.

1. $m \leftarrow 1$, $n \leftarrow 1$.
2. If $s_1(m) > \hat{s}_2(n)$, $n \leftarrow n+1$; else if $s_1(m) + 2\Delta < \hat{s}_2(n)$, $m \leftarrow m+1$; else, match $s_1(m)$ with $s_2(n)$ and $m \leftarrow m+1$, $n \leftarrow n+1$.

Table 1: Packet-Forward-Detect (PFD)

```
PFD($\mathbf{s}_1$, $\mathbf{s}_2$, $\Delta$, $\tau$):
$m = n = 1$;
while $m \leq |\mathcal{S}_1|$ and $n \leq |\mathcal{S}_2|$
    if $s_2(n) < s_1(m) - \Delta$
        $s_2(n)$ is chaff; $n \leftarrow n + 1$;
    else if $s_2(n) > s_1(m) + \Delta$
        $s_1(m)$ is chaff; $m \leftarrow m + 1$;
    else
        match $s_1(m)$ with $s_2(n)$;
        $m \leftarrow m + 1$; $n \leftarrow n + 1$;
    end
end
mark $s_1(i)$, $s_2(j)$ with $m \leq i$, $n \leq j$ as chaff;
$\widetilde{\text{CTR}} \leftarrow \frac{\text{the number of chaff epochs}}{|\mathcal{S}_1|+|\mathcal{S}_2|}$;
return $\begin{cases} \mathcal{H}_1 & \text{if } \widetilde{\text{CTR}} \leq \tau \\ \mathcal{H}_0 & \text{o.w.}; \end{cases}$
```

3. If $m \leq |\mathcal{S}_1|$ and $n \leq |\mathcal{S}_2|$, go to step 2; otherwise, label all the unmatched epochs as chaff and terminate.

The above steps are exactly the steps of running BGM over $\mathbf{s}_1$ and $\hat{\mathbf{s}}_2$ with the delay constraint 2Δ (refer to table 3 in [1]). Hence, the statement is proved. ■

The following theorem states the optimality of BiBGM.

Theorem 4.1 *BiBGM optimally partitions the measurements into the $R_1 \Rightarrow R_2$ flow, the $R_2 \Rightarrow R_1$ flow, and the chaff part such that the number of chaff epochs is minimized.*

Sketch of Proof: The statement results from the optimality of BGM, lemma 4.1, and the fact that, for $a \in \mathcal{S}_1$ and $b \in \mathcal{S}_2$, $|a - b|$ is less than Δ if and only if the ordered pair $(a,\, b + \Delta)$ satisfies causality and the delay constraint 2Δ[1]. ■

Under $\mathcal{H}_1$, if we increase every epoch in $\mathbf{s}_2$ by Δ, then the packet forwarding portion forms unidirectional flows with delay bound 2Δ. Combining this and lemma 4.1, we can observe that running PFD over $(\mathbf{s}_i)_{i=1}^2$ to detect packet forwarding with delay bound Δ is equivalent to running DBD over $\mathbf{s}_1$ and $\hat{\mathbf{s}}_2$ to detect flows with delay bound 2Δ, where $\hat{\mathbf{s}}_2$ is obtained by increasing every epoch in $\mathbf{s}_2$ by Δ. Directly from this argument, we can conclude that PFD has the same performance characteristic with DBD, as stated in the following corollaries without an additional proof.

Corollary 4.1 *If $\mathbf{S}_1$ and $\mathbf{S}_2$ are independent Poisson processes with rates λ_1 and λ_2, respectively, then $\widetilde{CTR}(t)$ satisfies the following with probability one.*

$$\lim_{t\to\infty} \widetilde{CTR}(t) = \begin{cases} \frac{(\lambda_2-\lambda_1)(1+(\frac{\lambda_1}{\lambda_2})e^{2\Delta(\lambda_1-\lambda_2)})}{(\lambda_2+\lambda_1)(1-(\frac{\lambda_1}{\lambda_2})e^{2\Delta(\lambda_1-\lambda_2)})} & \text{if } \lambda_1 \neq \lambda_2 \\ \frac{1}{1+2\lambda\Delta} & \text{if } \lambda_1 = \lambda_2 = \lambda \end{cases}$$

Note that the value is equivalent to $\lim_{t\to\infty} \widehat{CTR}(t)$ in theorem 3.1 with the maximum delay constraint 2Δ.

Corollary 4.2 *Suppose that $\mathbf{S}_1$ and $\mathbf{S}_2$ under $\mathcal{H}_0$ are independent Poisson processes, and τ_0 denotes $\lim_{t\to\infty} \widetilde{CTR}(t)$ under $\mathcal{H}_0$. If the threshold τ of PFD satisfies $\tau < \tau_0$, then PFD is τ-consistent. In addition, the false alarm probability decays exponenentially fast as the sample size grows.*

For arbitrary chaff insertion, if the fraction of chaff is allowed to be greater than τ_0, then BiBGM provides a way to schedule packet forwarding and chaff insertion to mimic $\mathcal{H}_0$, thereby avoiding the detection. The following corollary guarantees the detectability under independent Poisson chaff assumption.

Corollary 4.3 *Suppose that (i) under $\mathcal{H}_0$, $\mathbf{S}_1$ and $\mathbf{S}_2$ are Poisson processes, and (ii) under $\mathcal{H}_1$, the chaff portions of R_1 and R_2 are independent Poisson processes. In addition, the transmission rates of R_1 and R_2 are λ_1 and λ_2, respectively. Then, for any $\rho \in (\frac{|\lambda_1-\lambda_2|}{\lambda_1+\lambda_2},\, 1)$, there exists a proper threshold τ for PFD, such that PFD is ρ-consistent. Especially, the following τ can be used.*

$$\tau = \begin{cases} \frac{(\lambda_2-\lambda_1)(1+(\frac{\lambda_1(3+\rho)-\lambda_2(1-\rho)}{\lambda_2(3+\rho)-\lambda_1(1-\rho)})e^{2\Delta(\lambda_1-\lambda_2)})}{(\lambda_2+\lambda_1)(1-(\frac{\lambda_1(3+\rho)-\lambda_2(1-\rho)}{\lambda_2(3+\rho)-\lambda_1(1-\rho)})e^{2\Delta(\lambda_1-\lambda_2)})} & \text{if } \lambda_1 \neq \lambda_2 \\ \frac{1+\rho}{2+2\lambda(1+\rho)\Delta} & \text{if } \lambda_1 = \lambda_2 = \lambda \end{cases}$$

Moreover, the false alarm probability decays exponentially fast as the sample size grows.

5. CONCLUSION

In this paper, we studied timing-based detection of packet forwarding in MANETs. As a first step, we analyzed the performance of Detect-Bounded-Delay [1] under independent chaff assumption. Then, we proposed a packet forwarding detector and analyzed its performance under various chaff assumption. Especially, when chaff portions are independent Poisson processes, packet forwarding can be detected consistently regardless of its strength.

6. REFERENCES

[1] Ting He and Lang Tong, "Detection of Information Flows," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4925–4945, Nov. 2008.

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

[3] 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.

[4] L. Zhang, A.G. Persaud, A. Johson, and Y. Guan, "Stepping Stone Attack Attribution in Non-cooperative IP Networks," in *Proc. of the 25th IEEE International Performance Computing and Communications Conference (IPCCC 2006)*, Phoenix, AZ, April 2006.

[5] 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.

[6] T. He and L. Tong, "Detecting Information Flows: Improving Chaff Tolerance by Joint Detection," in *Proc. 2007 Conference on Information Sciences and Systems*, Baltimore, MD, March 2007.

[7] Jun Shao, *Mathematical Statistics*, Springer, 2003.

[1] An ordered pair $(x,\, y)$ is said to *satisfy causality and the delay constraint* α if $0 < y - x < \alpha$.