Performance Comparison of Two Sequential Change Detection Algorithms On Detection of In-band Wormholes

Shanshan Zheng, Tao Jiang and John S. Baras
Institute for Systems Research
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD, 20742
Email:{sszheng,tjiang,baras}@umd.edu

ABSTRACT

This paper compares the performance of parametric and non-parametric sequential change detection algorithms for detecting in-band wormholes in wireless ad hoc networks. The algorithms considered are the non-parametric cumulative sum (NP-CUSUM) and the repeated sequential probability ratio test (R-SPRT). Theoretical performance of the two is compared using metrics that take into account the algorithms' repeated nature, and the advantage of the parametric method is illustrated. On the other hand, connections between the parametric and non-parametric methods are made in the proposed worst case adversary model, where the non-parametric method is shown to be more robust to attack strategy changes. Experimental evaluation of wormhole detection schemes based on the two algorithms is presented. This work has implications for both the theoretical understanding and practical design of wormhole detection schemes based on parametric and non-parametric change detection algorithms.

I. Introduction

Collaborative attacks in wireless ad hoc networks bring serious challenges to the normal collaboration among different nodes and the correct functioning of the entire network. This paper addresses the problem of detecting one specific type of collaborative attacks, namely the wormhole attack, which is easy to launch by the adversary, but is difficult to detect and brings great damage to the network.

During a wormhole attack, the malicious nodes perform a tunneling procedure to form a wormhole where one node receives packets and covertly tunnels them to another colluding node, and then the colluding node replays these packets as if it receives them from its physical neighbors. Based on different covert communication mechanisms used for tunneling, wormhole attacks can be classified as in-band wormholes and out-band wormholes. The in-band wormhole connects the purported neighbors via multi-hop tunnels over the existing wireless medium while the out-band wormhole attack uses an external communication medium such as a wired link or a long-range wireless transmission channel. Wormhole attacks can affect shortest path routing calculations and allow the attacking nodes to attract and route traffic from other parts of the network to go through them. Effectively, wormhole attacks create two artificial traffic choke points that are under the control of the attacker. These choke points can be utilized at an opportune future time to analyze network traffic or degrade network performance.

Several approaches have been proposed in literature to defend the wormhole attacks. The first set of approaches provides solutions based on distance-bounding and time-bounding. Hu et. al. [1] proposed to add information to a packet to restrict the packet's maximum allowed transmission distance to avoid tunneling, which they called packet leashes. In the work by Eriksson et. al. [2], a timing based countermeasure to the wormhole attacks called TrueLink is proposed. By using a combination of timing and authentication, TrueLink enables a node to verify the adjacency of its neighbor to avoid tunneling.

The second set of approaches is based on geometric inconsistency. In the work by Wang and Bhargava [3], Multi-Dimensional Scaling is applied to reconstruct the lay-out of the network. During the wormhole attack, the fake connection created by the malicious nodes will bend the reconstructed surface to pull closer the nodes that are actually far away and the location of the wormhole is determined by detecting such anomalies. Other methods based on geometric inconsistency include the work by Hu and Evans [4]

The third set of approaches is based on local monitoring and statistical analysis. Song et. al. [5] proposed a statistical analysis approach to detect wormholes in wireless ad hoc networks that are based on multipath routing. The rationale of the approach is that certain statistics of the routes discovered by routing protocols change dramatically under wormhole attacks such as the relative frequency of each link appeared in the obtained routes etc. In our previous work [6], we presented a detection scheme using the change of path round trip delay as an indication of in-band wormhole attacks. The detection scheme utilized two sequential change detection algorithms: the non-parametric cumulative sum (NP-CUSUM) and repeated sequential probability ratio test (R-SPRT). In this paper, we further provide theoretical analysis and performance comparison of the two algorithms using metrics that take into account the algorithms' repeated nature. Our work can provide useful insights on the choice of change detection algorithms for designing practical wormhole detection schemes.

II. Wormhole Detection Scheme

Our wormhole detection scheme is based on the observation that during an in-band wormhole attack, the transmission delay along a path that goes through a wormhole tunnel will deviate from its normal value. This relatively abrupt change in transmission delay occurs at unknown time points and should be detected as soon as possible. Therefore, the problem of detecting an in-band wormhole attack can be formulated and solved as a quickest (sequential) change detection problem:

978-1-4244-2734-5/09/$25.00 ©2009 IEEE

to detect a change as rapidly as possible after its occurrence, while maintaining the false alarm rate at a given level.

Our detection scheme utilizes a dynamic hierarchy model proposed by Sterne et. al. [7]: clustering techniques are applied to organize the entire network into several groups. Each group contains two levels of nodes, the leaf nodes and the cluster head node. The data acquisition occurs at the leaf nodes and the inference drawn from the data is transmitted to the cluster head. The cluster head correlates the individual inferences it receives to make the final decision. To avoid having a single head node that is a potential single point of failure, one or more numbers of nodes can be designated as backup head nodes. Our detection scheme considers the one-group case, but it can also be extended to multi-group case. The scheme contains the following three steps.

A. Data Collection

Each node in the network collects three-hop transmission delay data by periodically sending out ping packets to all the nodes that are three hops away. Three-hop paths are considered because it is sufficient to analyze delays of the two normal nodes that communicate directly with the two end nodes of a wormhole tunnel [8]. Thus the hop count between the two normal nodes appears to be three during a wormhole attack.

B. Data Analysis

Each node determines from the collected delay information whether the three-hop path goes through a wormhole tunnel.

We assume that the observed delay data have a joint probability density function (PDF) $f_0(x_1, \ldots, x_{m-1})$ until an unknown time point m, $m \in \{1, 2, \ldots\}$, and after this time point m, the observations have another distribution $f_1(x_m, \ldots, x_n)$. In other words, f_0 is the PDF of the normal delay data, while f_1 is the PDF of the delay data under the wormhole attack (abnormal delay data). Since m is unknown, each node needs to do the following hypothesis testing:

$$\begin{aligned} H_0 &: x_1, \ldots, x_n \sim f_0, \qquad (1) \\ \text{for } 1 \leq k \leq n,\ H_k &: x_1, \ldots, x_k \sim f_0, \\ &\quad x_{k+1}, \ldots, x_n \sim f_1. \end{aligned}$$

The likelihood ratio between the hypotheses H_0 and H_k is

$$S_{n,k} = \ln \frac{f_0(x_1, \ldots, x_{k-1}) f_1(x_k, \ldots, x_n)}{f_0(x_0, \ldots, x_n)}.$$

The maximum likelihood principle leads to the following decision rule and stopping time:

$$\begin{aligned} d(n) &= \begin{cases} 1, & \text{if } \max_{1 \leq k \leq n} S_{n,k} \geq h, \\ 0, & \text{if } \max_{1 \leq k \leq n} S_{n,k} < h, \end{cases} \\ \tau &= \min\{n : d(n) = 1\}. \end{aligned}$$

This is a well known sequential change detection algorithm, namely, cumulative sum (CUSUM) algorithm, first proposed by Page [9]. A sequential change detection algorithm usually involves optimizing the tradeoff between two performance metrics. The first metric is the *delay for detection*, which relates to the ability of the algorithm to set an alarm when a change actually occurs, the other metric is the *mean time between false alarms*, which reflects the frequency of false alarms. CUSUM is known to be the optimal change detection algorithm [10] in the sense that it minimizes the worst mean detection delay, i.e., the detection delay under the realization of distribution f_0 that makes the detection most difficult, while maintaining the mean time between false alarms above a certain threshold given that the observations are independent and identically distributed (i.i.d.).

By denoting $\max_{1 \leq k \leq n} S_{n,k}$ as g_n, and assuming that the observations are i.i.d., we can write g_n in a recursive form

$$g_n = \left(g_{n-1} + \ln \frac{f_1(x_n)}{f_0(x_n)} \right)^+, \qquad (2)$$

where $g_0 = 0$ and $(x)^+$ stands for $\max(x, 0)$. An intuitive explanation behind Equation (2) is that, since $E_1[\ln(f_1(x_n)/f_0(x_n))] > 0$ and $E_0[\ln(f_1(x_n)/f_0(x_n))] < 0$, where $E_0[\cdot]$ and $E_1[\cdot]$ denote the expectations correspond to the distribution functions f_0 and f_1, g_n in Equation (2) will remain close to 0 under H_0 and start drifting upward until it crosses the threshold h under H_1. Equation (2) provides a basis for the following non-parametric cumulative sum algorithm we developed in our wormhole detection scheme.

1) Non-parametric Cumulative Sum (NP-CUSUM): In a mobile ad hoc network where network topology changes very quickly, it is usually very difficult, if not impossible, to model or estimate the distributions f_0 and f_1 of the delay measurements. Therefore, we need a non-parametric approach to solve the hypothesis testing problem (1).

Since the distribution functions f_0 and f_1 are unknown, we replace the term $\ln(f_1(x_n)/f_0(x_n))$ in Equation (2) by some nonparametric score function $s(x_n)$, i.e., we let $g_n = (g_{n-1} + s(x_n))^+$. The nonparametric score function must satisfy the conditions $E_1[s(x_n)] > 0$ and $E_0[s(x_n)] < 0$ to ensure that g_n remains close to 0 in normal conditions and drifts upward in abnormal conditions. Observing that the in-band wormhole attack leads to an abrupt change in the mean value of the transmission delay, we can choose $s(x_n) = x_n - c$, where c is a constant which satisfies $E_0[x] < c < E_1[x]$, i.e., we use the statistic

$$g_n = (g_{n-1} + x_n - c)^+, \qquad (3)$$

and the decision rule and stopping time are

$$\begin{aligned} d(n) &= \begin{cases} 1, & \text{if } g_n \geq h, \\ 0, & \text{if } g_n < h, \end{cases} \qquad (4) \\ \tau &= \min\{n : d(n) = 1\}. \qquad (5) \end{aligned}$$

2) Repeated Sequential Probability Ratio Test (R-SPRT): In the situation where a large volume of sample data is available and estimating the distribution functions f_0 and f_1 is not difficult, we propose to use the R-SPRT algorithm. The R-SPRT can utilize the information of the distribution functions and is expected to improve the detection performance.

Recall that CUSUM is also a change detection algorithm that can utilize the model information, the difference between R-SPRT and CUSUM include the following: the CUSUM algorithm minimizes the worst mean delay for detection but does not guarantee that the mean delay for detection will be minimized. R-SPRT is more flexible with its two adjustable thresholds. By setting the lower threshold to 0, R-SPRT is equivalent to CUSUM and thus delivers the same performance

978-1-4244-2734-5/09/$25.00 ©2009 IEEE

as CUSUM. By setting the lower threshold to other values under different scenarios, R-SPRT can potentially outperform the CUSUM algorithm.

We first define a single use of the sequential probability ratio test (SPRT) with the decision rule d and the stopping time τ as :

$$\begin{aligned} d(n) &= \begin{cases} 1, & \text{if } S_n \geq B, \\ 0, & \text{if } S_n \leq A, \\ \text{defer decision}, & \text{if } A < S_n < B, \end{cases} \\ \tau &= \min\{n : (d(n) = 1) \cup (d(n) = 0)\}, \end{aligned}$$

where A, B are two thresholds and S_n is the SPRT statistic defined by:

$$S_n = \ln \frac{f_1(x_1, x_2, \ldots, x_n)}{f_0(x_1, x_2, \ldots, x_n)}.$$

If the observed sequence $\{x_i\}_{i=1}^{n}$ are i.i.d. variables, S_n can be written as

$$S_n = S_{n-1} + \ln \frac{f_1(x_n)}{f_0(x_n)}.$$

It has been shown by Wald [11] that SPRT is the optimal detection test that minimizes the average number of required observations to reach a decision among all sequential and non-sequential tests where the false alarm rate and missed detection rate do not exceed some predefined values. However, the single SPRT algorithm is better suited for on-demand monitoring of the network, e.g., when a higher layer monitoring agent requests a node to collect data and conduct the SPRT because some area of the network is behaving suspiciously, and once the node reaches a decision, no matter if the decision is a '1' or a '0', it stops monitoring. In contrast, our scenario requires continuous monitoring in order to detect the wormhole attack. Therefore, a repeated SPRT is required.

In R-SPRT, the single SPRT algorithm is restarted with $S_0 = 0$ whenever $d(n) = 0$. This setup enables the nodes to detect the abnormal behavior for both short term and long term wormhole attacks. Note if the observations are i.i.d. and the lower threshold of the R-SPRT algorithm is set to 0 ($A = 0$), the statistic can be written as $S_n = (S_{n-1} + \ln \frac{f_1(x_n)}{f_0(x_n)})^+$, which is equivalent to the CUSUM algorithm.

C. Wormhole Localization

After data analysis, the cluster head receives the decision made by each leaf node along with the path information. It correlates these information and determines whether a wormhole attack is underway and locates the attacking nodes.

Given the observations of three-hop path delay data, locating a wormhole requires at least two anomalous observations with a common intersecting link but disjoint end nodes. We use Fig. 1 to illustrate this claim. Assuming that nodes 2 and 3 are the wormhole attackers, if the cluster head is informed by node 1 that the path 1-2-3-4 is abnormal as (a) shows, it can only tell that among the three links 1-2, 2-3, 3-4 some are wormhole tunnels; if the cluster head is told that the paths 1-2-3-4 and 1-2-3-5 are abnormal as in (b), it can tell that the wormhole tunnel exists in the two links 1-2 and 2-3 ; if the cluster head is told by node 1 and 6 that paths 1-2-3-4 and 6-2-3-5 are abnormal, it can determine that the link 2-3 is abnormal and nodes 2 and 3 are the wormhole attackers.

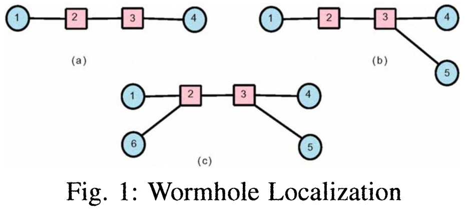

Fig. 1: Wormhole Localization

III. Performance Analysis of NP-CUSUM and R-SPRT

When we evaluate the performance of a change detection algorithm, we are interested in two performance metrics, namely the *delay for detection*, whose mean is denoted by $E[T_D]$, and the *mean time between false alarms*, $E[T_{FA}]$.

A. Performance Analysis of NP-CUSUM

Recall that the decision rule and stopping time of NP-CUSUM are shown in Equations (4) and (5). Following a procedure similar to the one in [12], we can prove that under very general conditions, the following inequality holds for the *mean time between false alarms* of the NP-CUSUM algorithm

$$E[T_{FA}] \geq c_1 e^{c_2 h}, \tag{6}$$

where c_1 and c_2 are some constants depending on the parameter c and the normal distribution f_0. Generally it is difficult to compute the values of c_1 and c_2, but since it is usually not difficult to collect sample data for the normal situation, Equation (6) can be evaluated by experiments. It is known that $E[T_{FA}]$ increases with the increase of c. Another observation from Equation (6) is that the mean time between false alarms increases exponentially fast with the threshold h.

For the *delay for detection* of the NP-CUSUM algorithm, following a similar procedure as in [12], we get the following asymptotic relation as $h \to \infty$,

$$\frac{E[T_D]}{h} \to \frac{1}{E_1[x] - c}. \tag{7}$$

By Equation (6), $E[T_{FA}]$ goes to infinity as $h \to \infty$, therefore, this asymptotic view is meaningful in practice, as a large *mean time between false alarms* is always desirable. So Equation (7) actually provides a criterion to select the thresholds h and c in NP-CUSUM. For example, if we want to detect the attack within certain pre-specified time interval T, the h and c should be selected according to

$$\frac{1}{E_1[x] - c} < \frac{T}{h} \quad \Rightarrow \quad h < T(E_1[x] - c). \tag{8}$$

Equations (6) and (7) also exhibit a trade-off between the two performance metrics. A longer mean time between false alarms requires larger value of h and c, while a smaller delay for detection requires smaller h and c.

B. Performance Analysis of R-SPRT

We now proceed to evaluate $E[T_{FA}]$ and $E[T_D]$ for the R-SPRT algorithm. We denote the probability of false alarms and the probability of missed detection of a single SPRT as α and β, and assume that the average number of samples the single SPRT needs to make a decision is $E_1[N]$ under H_1 and $E_0[N]$ under H_0. In the R-SPRT algorithm, each time the SPRT stops and makes a decision can be modeled as a Bernoulli random variable with parameters α under H_0 and $1-\beta$ under H_1. Therefore the waiting time until the first success (a decision of '1') is a geometric random variable, i.e.,

$$E[T_D] = \frac{E_1[N]}{1-\beta}, \quad E[T_{FA}] = \frac{E_0[N]}{\alpha}.$$

Following Wald's identity [11]

$$E_1[N] = \frac{A\beta + B(1-\beta)}{E_1[\ln \frac{f_1(x)}{f_0(x)}]}, \quad E_0[N] = \frac{A(1-\alpha) + B\beta}{E_0[\ln \frac{f_1(x)}{f_0(x)}]},$$

where $A \approx \ln \frac{\beta}{1-\alpha}$ and $B \approx \ln \frac{1-\beta}{\alpha}$ are the two thresholds, we obtain

$$E[T_D] \approx \frac{\frac{e^A}{e^B} \cdot Ar + B}{E_1[\ln \frac{f_1(x)}{f_0(x)}]}, \tag{9}$$

$$E[T_{FA}] \approx \frac{Ar + B}{E_0[\ln \frac{f_1(x)}{f_0(x)}]}, \tag{10}$$

where $r = \frac{e^B - 1}{1 - e^A}$. In Wald's identity, A is assumed to be smaller than 0. If A is equal to 0, we have that the R-SPRT algorithm is equivalent to the CUSUM algorithm, and $E[T_D]$ and $E[T_{FA}]$ of the R-SPRT when $A = 0$ satisfy

$$E[T_{FA}] > e^B \text{ and } \frac{E[T_D]}{B} \to \frac{1}{E_1[\ln \frac{f_1(x)}{f_0(x)}]} \text{ as } B \to \infty.$$

C. Comparison of NP-CUSUM and R-SPRT

We now compare the trade-off between $E[T_{FA}]$ and $E[T_D]$ for the two algorithms. In this section, we compare both algorithms for detection of an 8-hop wormhole. The data are generated from a network containing 50 nodes in a 1000×1000 square field using the ns-2 simulator. We vary all the available parameters of the two algorithms in order to obtain a fair comparison.

Figure 2 illustrates the performance of NP-CUSUM with different c and h. Each curve corresponds to a specific value of c and is obtained by changing h from 15 to 125. Under these settings, we conclude that the best performance of NP-CUSUM is obtained when $c = 30$. Therefore, this value of c is adopted as an optimal threshold in further experiments.

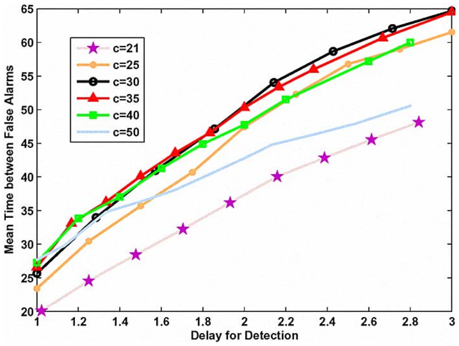

Fig. 2: NP-CUSUM performance. h ranges from 15 to 125

Figure 3 represents the performance of R-SPRT with different values of A and B. Each curve with a specific value A is obtained by changing B from 1 to 25. It shows that the curves for different A are very similar, so we just use $A = 0$ in further experiments.

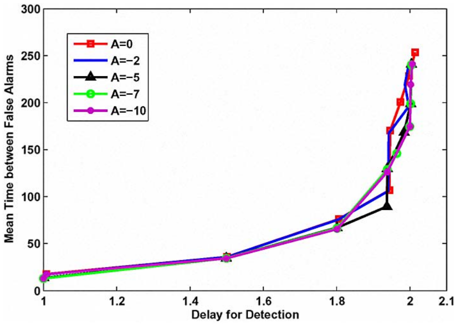

Fig. 3: R-SPRT performance. B ranges from 1 to 25

The parametric method R-SPRT has additional information of the distributions f_0 and f_1 and thus is expected to perform better than the non-parametric method NP-CUSUM. This conjecture is confirmed in Figure 4, where R-SPRT achieves increasingly larger value of mean time between false alarms than NP-CUSUM for larger detection delay values. A longer mean time between false alarm implies fewer false alarm and thus better performance.

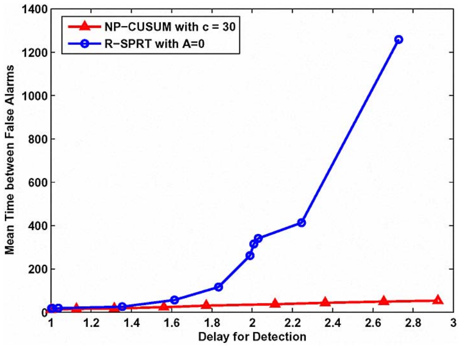

Fig. 4: Comparison of NP-CUSUM and R-SPRT

The better performance of R-SPRT comes at the cost of higher computational complexity, because estimating the distributions f_0 and f_1 requires proper sample data and training using these data. Sample data for the abnormal distribution f_1 usually depend on several factors under the control of the attackers, such as the tunnel length and the location of the tunnel end points, thus posing difficulties for the R-SPRT method. In constrast, NP-CUSUM only requires an estimation of the mean value of a normal three-hop path delay, which is relatively easier to obtain.

IV. Worst Case Adversary Model

In this section, we derive a worst case adversary model and show that NP-CUSUM is more robust to the changes of the attack model.

A. Worst Case Adversary Model

In the worst case adversary model, we assume the attackers have some control of the distribution f_1 and f_1 is chosen to maximize the performance of the adversary. Before deriving the model, we describe the following theorem from [12].

Theorem I: *Let $\mathcal{A}$ be a change detection algorithm depending on a large parameter h, and ρ_h be a sequence of* *normalized detection delay defined by $\rho_h = \frac{(\tau-m)^+}{h}$, where m is the change time and τ is the stopping time. Define $\beta_h = \sup_k P_0(d_k = 1)$, where $P_0(\cdot)$ denotes the probability corresponding to the observation sequence when there is no change occurrence. If ρ_h converges as $h \to \infty$ for any $m \geq 1$ almost surely to a determined limit $\gamma(\mathcal{A}, f_1, f_0)$, we have*

$$\gamma(\mathcal{A}, f_1, f_0) \geq K(f_1, f_0)^{-1} \times \lim_{h\to\infty} \frac{|\ln \beta_h|}{h}, \qquad (11)$$

where $K(f_1, f_0)$ is the Kullback information $E_1[\ln \frac{f_1(x)}{f_0(x)}]$.

Given a detection algorithm, the limit of $\frac{|\ln \beta_h|}{h}$ is determined. Therefore in order to maximize the detection delay, the attackers need to minimize the following objective function:

$$\min_{f_1(x)} K(f_1(x), f_0(x)).$$

Assuming the actual length of the abnormal paths that go through the wormhole tunnel is n hops, we have $E_1[x] = \frac{n}{3}E_0[x]$, as the abnormal path appears to be 3-hop. The choice of n depends on the risk preference of the attackers. With larger n, the attackers can attract more traffic and degrade network performance more, but on the other side, they are at higher risk of being detected. Therefore, for a given n, f_1 must belong to the following class of feasible probability density functions:

$$\mathcal{A}_n = \{g : \int g(x)dx = 1 \text{ and} \int xg(x)dx = \frac{n}{3}E_0[x]\}.$$

In summary, we have the following objective function for the attackers,

$$\min_{f_1(x)\in\mathcal{A}_n} \int f_1(x) \ln \frac{f_1(x)}{f_0(x)} dx.$$

Applying the Lagrange method, we derive f_1^* that maximizes the performance of the adversary:

$$f_1^*(x) = f_0(x)e^{\lambda_1 x}e^{\lambda_2 - 1},$$

where λ_1 and λ_2 are the Lagrange multipliers satisfying the following equations:

$$\begin{aligned} \int x f_0(x)e^{\lambda_1 x}dx &= \frac{n}{3}E_0[x] \cdot \int f_0(x)e^{\lambda_1 x}dx, & (12) \\ e^{-\lambda_2+1} &= \int f_0(x)e^{\lambda_1 x}dx. & (13) \end{aligned}$$

B. NP-CUSUM and R-SPRT in the Worst Case Adversary Model

The following proposition establishes the connection between the NP-CUSUM algorithm and the R-SPRT algorithm in the worst case adversary model.

Proposition II: *In the worst case adversary model, NP-CUSUM is equivalent to R-SPRT if the threshold A of R-SPRT is set to 0 and the parameters c and h for NP-CUSUM satisfy the following conditions:*

$$c = -\frac{\lambda_2 - 1}{\lambda_1} \textit{ and } h = \frac{B}{\lambda_1},$$

where λ_1 and λ_2 are Lagrange multipliers satisfying Equation (12) and (13).

Proof: When the threshold A of R-SPRT is set to 0, the statistic of R-SPRT can be written as

$$S_n = \left(S_{n-1} + \ln \frac{f_1(x)}{f_0(x)}\right)^+.$$

In the worst case adversary model, we have $\ln(f_1(x)/f_0(x)) = \lambda_1 x_n + \lambda_2 - 1$, therefore the statistic, decision rule and stopping time for R-SPRT with A=0 can be represented as

$$\begin{aligned} S_n &= (S_{n-1} + \lambda_1 x_n + \lambda_2 - 1)^+, \\ d(n) &= \begin{cases} 1, & \textit{if } S_n \geq B, \\ 0, & \textit{if } S_n < B, \end{cases} \\ \tau &= \min\{n : d(n) = 1\}, \end{aligned}$$

which can be rewritten in the following forms:

$$\begin{aligned} S_n' &= (S_{n-1}' + x_n + \frac{\lambda_2 - 1}{\lambda_1})^+, \\ d(n) &= \begin{cases} 1, & \textit{if } S_n' \geq \frac{B}{\lambda_1}, \\ 0, & \textit{if } S_n' < \frac{B}{\lambda_1}, \end{cases} \\ \tau &= \min\{n : d(n) = 1\}. \end{aligned}$$

Comparing them to Equation (3), (4) and (5), we have that the NP-CUSUM is equivalent to the R-SPRT with $A = 0$ if $c = -(\lambda_2 - 1)/\lambda_1$ and $h = B/\lambda_1$ in the worst case adversary model.

Recall that in Figure 4, R-SPRT with A=0 performs much better than NP-CUSUM, but in the worst case adversary model, it can only perform the same as NP-CUSUM. For the NP-CUSUM algorithm, the performance metric $E[T_{FA}]$ depends on f_0, and $E[T_D]$ depends on $E_1[x]$, so its performance will not change in the worst case adversary model. This suggests that NP-CUSUM is more robust to the changes of attack model.

V. Experiments and Results

In this section, we evaluate the performance of the complete three-step detection scheme using the receiver operating characteristic (ROC) curve. ROC curve is represented by the true positive rate (TPR) vs. the false positive rate (FPR). Recall that we use the *mean detection for delay* $E[T_D]$ and the *average time between false alarms* $E[T_{FA}]$ to measure the performance of the change detection algorithms. The relation between the TPR and FPR of our detection scheme and $E[T_D]$ and $E[T_{FA}]$ of the change detection algorithms is shown as follows:

Proposition III: *For a particular one-hop link, we assume that there are n independent three-hop paths intersecting at it. By independent three-hop paths, we mean the paths that have disjoint end nodes. Suppose the change detection algorithm used by each node to make decisions on individual paths has performance $E[T_D]$ and $E[T_{FA}]$, then if this one-hop link is a wormhole tunnel, the true positive rate of our detection scheme on detecting this link is*

$$TPR = 1 - p_0^n - np_0^{n-1}(1 - p_0)$$

where $p_0 = 1 - 1/E[T_D]$. If this one-hop link is normal, the false positive rate of our detection scheme on detecting this

978-1-4244-2734-5/09/$25.00 ©2009 IEEE

link is

$$FPR = 1 - p_1^n - np_1^{n-1}(1 - p_1)$$

where $p_1 = 1 - 1/E[T_{FA}]$.

Proof: The change detection algorithm has performance $E[T_D]$ *and* $E[T_{FA}]$*, that is to say, the probability of not raising a true alarm for an abnormal path is* $p_0 = (E[T_D] - 1)/E[T_D]$*, and the probability of not raising a false alarm for a normal path is* $p_1 = (E[T_{FA}] - 1)/E[T_{FA}]$.

If the one-hop link is a wormhole tunnel, our detection scheme will raise an alarm if and only if there are more than one alarm raised by the change detection algorithms over the n *independent paths, which is an event with probability* $1 - p_0^n - np_0^{n-1}(1 - p_0)$*. By a similar analysis we can obtain the formula for FPR.*

The performance of the NP-CUSUM based detector and the R-SPRT based detector in detection of an 8-hop wormhole is compared in Figure 5.

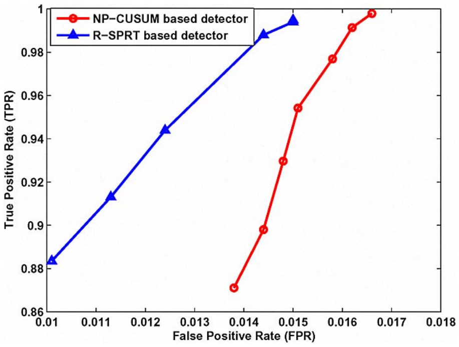

Fig. 5: R-SPRT based detector vs. NP-CUSUM based detector

It is worth mentioning that the selection of the training set for the R-SPRT based detector is very important. If the trained distributions do not match those of the testing data, the performance of the detector can be seriously deteriorated. In Figure 6, we trained the R-SPRT based detector on a network containing an 8-hop wormhole and used it to detect a 4-hop wormhole in the same network. The best TPR obtained by adjusting the two thresholds is 0.23, which is much smaller than the TPR values achieved in Fig. 5. Therefore when we use the R-SPRT based detector, extra attention must be paid to the choice of the training data. When a good training data set does not exist, the NP-CUSUM based detector is a reasonable alternative for the R-SPRT based detector.

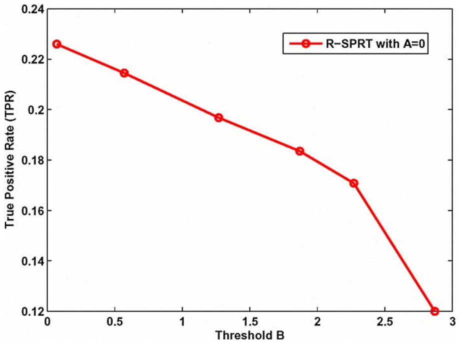

Fig. 6: Performance of R-SPRT based Detector Using Improper Training Data

VI. Conclusion

In this work, we performed both theoretical and experimental comparisons of two sequential change detection algorithms, namely the NP-CUSUM and R-SPRT algorithms, on detection of in-band wormhole attacks in a wireless ad hoc network. We illustrate that the parametric method R-SPRT has better performance than the non-parametric method at the cost of higher complexity, and we also show that the non-parametric method NP-CUSUM is more robust to attack strategy changes.

The higher complexity of R-SPRT comes from its parametric nature, which needs proper training to obtain the model for the distributions f_0 and f_1. When an exact model is not available, the performance of R-SPRT can be seriously degraded. In contrast, NP-CUSUM is a non-parametric method, which does not require exact models of the normal or adversary distributions and is easier to apply.

In our current wormhole detection scheme where the leaf nodes periodically send their decisions along with path information to the cluster head, reducing communication overhead is an issue to explore. It will be helpful to see how to combine polling and sampling techniques into the detection scheme to reduce data redundancy and communication overhead.

VII. ACKNOWLEDGEMENT

This work is prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011.

References

[1] Y. Hu, A. Perrig, and D. Johnson, “Packet leashes: A defense against wormhole attacks in wireless ad hoc networks,” in *IEEE Infocom: Proceedings of the 22nd Annual IEEE Conference on Computer Communications*, 2003, pp. 1976–1986.

[2] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, “TrueLink: A practical countermeasure to the wormhole attack,” in *Proceedings of the 2006 14th IEEE International Conference on Network Protocols (ICNP)*, Nov. 2006, pp. 75–84.

[3] W. Wang and B. Bhargava, “Visualization of wormhole in sensor networks,” in *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, 2004, pp. 51–60.

[4] L. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks,” in *Proceedings of Network and Distributed System Security Symposium (NDSS 2004)*, San Diego, CA, Feburary 2004.

[5] N. Song, L. Qian, and X. Li, “Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach,” in *Proceedings of IEEE IPDPS*, 2005.

[6] S. Zheng, T. Jiang, J. Baras, A. Sonalker, D. Sterne, R. Gopaul, and R. Hardy, “Intrusion detection of in-band wormholes in MANETs using advanced statistical methods,” in *Proceedings of Milcom 08: Assuring Mission Success*, San Diego, CA, Nov. 17-19 2008.

[7] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe, “A general cooperative intrusion detection architecture for MANETs,” in *The third IEEE international Information Assurance Workshop*, Collega Park, MD, March 2005.

[8] D. Sterne, R. Gopaul, G. Lawler, P. Kruus, B. Rivera, and K. Marcus, “Countering false accusations and collusion in the detection of in-band wormholes,” in *Proceedings of Annual Computer Security Applications Conference (ACSAC)*, Miami Beach, FL, December 10-14 2007.

[9] E. S. Page, “Continous inspection schemes,” *Biometrika*, vol. 41, no. 1/2, pp. 100–115, 1954.

[10] G. Lorden, “Procedures for reacting to a change in distributions,” *The Annals of Mathematical Statistics*, vol. 42, no. 6, pp. 1897–1908, 1971.

[11] A. Wald, *Sequential Analysis*. New York: John Wiley and Sons, 1947.

[12] B. E. Brodsky and B. Darkhovsky, *Nonparametric Methods in Change-Point Problems*. Kluwer Academic Publishers, 1993.