

# INTRUSION DETECTION OF IN-BAND WORMHOLES IN MANETS USING ADVANCED STATISTICAL METHODS

Shanshan Zheng, Tao Jiang, John S. Baras  
University of Maryland College Park  
College Park, MD 20742

Anuja Sonalker and Dan Sterne    Richard Gopaul and Rommie Hardy  
SPARTA, Inc.                            U.S. Army Research Laboratory  
Columbia, MD 21046                    Adelphi, MD 20783

## ABSTRACT

*Due to the dynamics and mobility of mobile ad hoc networks (MANETs), intrusion detection techniques in MANETs must be adaptive. In this work, we propose detection schemes that are suitable to detect in-band wormhole attacks. The first detection scheme uses the Sequential Probability Ratio Test (SPRT). The SPRT has been proven to be an optimal detection test when the probability distributions of both normal and abnormal behaviors are given. Furthermore, we introduce non-parametric methods, which require no training and are more adaptive to mobile scenarios. The proposed detection schemes are implemented and evaluated using a 48-node testbed and a mobile ad-hoc network emulator at the Army Research Lab. The performance and detection accuracy of various schemes are compared, especially in the presence of congestion. We provide tradeoffs analyses among detection latency and probabilities of false alarms and missed detection.*

## INTRODUCTION

Mobile ad-hoc networks (MANETs) will be widely used in future battlefields where no network infrastructure exists. MANETs rely on collaboration of nodes for almost all their functions. Therefore, collaborative attacks by compromised nodes are seriously disruptive to core MANET functions like routing, etc. In this paper, we focus on one specific type of collaborative attacks on MANET routing - the wormhole attack.

In physics, a wormhole is a hypothetical shortcut through space and time that connects two distant regions. In cyber security, the term wormhole was recently adopted [1] to describe an attack on MANET routing protocols in which colluding nodes create the illusion that two remote regions are directly connected through nodes that appear to be neighbors, but are actually distant from one another. The illusory shortcut is created by connecting the purported neighbors using a covert communication mechanism. The wormhole undermines shortest path routing calculations,

allowing the attacking nodes to attract and route traffic from other parts of the network through them. The wormhole thus creates two artificial traffic choke points that are under the control of the attacker and can be utilized at an opportune future time to degrade or analyze traffic.

This paper deals with in-band wormholes, which covertly connect the purported neighbors via multihop tunnels through the primary link layer. In-band wormholes are important for several reasons. First, because they do not require additional specialized hardware, they can be launched from any node in the network; as a result, they may be more likely to be used by real adversaries. Second, unlike out-of-band wormholes[1], [2], which actually add channel capacity to the network, in-band wormholes continually consume network capacity (i.e., waste bandwidth) thereby inherently causing service degradation. There are a couple of challenges unique to detecting in-band wormhole attacks in MANETs. First, the detector needs to be able to efficiently correlate individual actions across nodes in order to identify and localize the attack. Second, the detector should be able to localize and detect an ongoing attack with minimum delay because of dynamics of MANETs and fast reaction to attacks required in battlefields.

In this paper we extend the work presented in [3], [4] by implementing a Sequential Probability Ratio Test (SPRT) based intrusion detection system (IDS) and evaluating it using a 48-node testbed and a mobile ad-hoc network emulator at the Army Research Lab. Furthermore, we introduce non-parametric methods, which require no training and are more adaptive to mobile scenarios. We study the detection accuracy of these detection methods, especially in the presence of traffic congestion. Tradeoff analyses among detection latency and probabilities of false alarms and missed detection are also presented in this paper.

## RELATED WORK

Several approaches have been proposed in the literature to defend wormhole attacks in wireless ad hoc networks. Hu et al. proposed in [1] to add information to a packet

to restrict the packet's maximum allowed transmission distances to avoid tunnelling, which they called packet leashes. They defined geographical leashes and temporal leashes. Geographical leashes ensure the receiver is within a certain distance from the sender and temporal leashes ensure the packet can not travel too far. However, these two solutions require position information and time synchronization, which restricts their applicability.

Directional antennas are used in [5] for nodes to share directional information and maintain accurate sets of their neighbors. In this way the wormhole transmitter is recognized as a false neighbor and its messages is ignored, thus wormhole attacks cannot be executed. But this method is only suitable for devices with directional antennas that are not widely deployed.

A statistical analysis approach on multipath routing is proposed in [6]. This approach is based on the observation that certain statistics of the discovered routes by routing protocols will change dramatically under wormhole attacks, e.g. the relative frequency of each link appeared in the obtained routes and the difference between the most frequently appeared link and the second most frequently appeared link may be unusually high.

In [7], measurement of path round trip delay is used as an indication of an in-band wormhole attack. Whenever the obtained delay time exceeds some pre-defined threshold, it is concluded that the path is subjected to a wormhole attack. This single threshold method is also used in the Delay Per Hop Indication (DePHI) scheme in [8]. However, this method could face problems in a network where the network connections change over time and congestion occurs frequently. Congestion can increase the delay time associated with a normal path, leading to a high false alarm rate. We will compare our proposed schemes with this single threshold method in the evaluation section.

## WORMHOLE DETECTION

The basic idea behind our wormhole detection schemes presented in this paper is that during a wormhole attack, certain network characteristics, such as transmission delay, congestion pattern and traffic throughput deviate from their normal values. In this paper, we only use one type of network characteristic: the delay measurement, which is easy to record in our testbed. We show that our proposed detection schemes using only delay measurement can detect wormhole attacks with great accuracy. Studying the effects of other characteristics for improving detection will be part of our future work. The underlying premise using delay times is that the delay a packet experiences along a path through a *in-band* wormhole tunnel will be much

higher than that seen through the normal path. Therefore, if a path has a noticeably higher delay than what is estimated to be normal delay, it is very likely that a wormhole exists. However, many factors, such as mobility and congestion, can increase the probability of false alarms if we simply compare a path delay to a pre-determined threshold to make the decision. In order to alleviate these effects, we introduce Sequential Probability Ratio Test (SPRT) and non-parametric change detection techniques.

There are three components in our mechanism. In the first component, path and delay information is collected from many paths in the network. In the second component, each node analyzes the information obtained in the first component to make a decision about whether individual paths it has measured include a wormhole tunnel or not. In the third component, decisions of all nodes are forwarded to a coordinator and the coordinator performs a correlation algorithm to determine whether there is a wormhole attack, and if so, locates the wormhole tunnel end points.

### A. Data Collection

Each node in the network collects three-hop delay data by periodically sending out pings to all the nodes that are three hops away. Three hop paths are selected because it is sufficient to only analyze delays of two normal nodes that directly communicate with two attackers at the two ends of a wormhole tunnel[4]. These two normal nodes appear to be three hops away given the wormhole tunnel is up. We define the network as an undirected graph  $G = (V, E)$  and denote the set of nodes which are three hops away from node  $i$  as  $N_i^{(3)} = \{j \in V | \text{hopcount}(i, j) = 3\}$ . Then at the end of data collection, each node will have sequences of delay information  $d_{ij}^1, d_{ij}^2, d_{ij}^3 \dots, j \in N_i^{(3)}$  on hand.

### B. Data Analysis

After collecting delay information of three-hop paths, each node does a hypothesis testing to determine if the three-hop path goes through a wormhole tunnel or not. In this subsection, we describe two statistical methods of hypotheses testing: Sequential Probability Ratio Test (SPRT) and non-parametric change detection.

1) *Sequential Probability Ratio Test (SPRT)*: As we have discussed in the introduction, the IDS in MANETs needs to use a detection test that enables on-line detection with minimum delay. This gives rise to the sequential detection problem. A sequential decision rule consists of a stopping time which indicates when to stop observing and a final decision rule that indicates which hypothesis (i.e, abnormal or normal behavior) should be selected. A sequential

decision rule is efficient if it can provide reliable decisions as fast as possible. It has been shown by Wald [9] that the decision rule that minimizes the expected number of required observations to reach a decision over all sequential and non-sequential decision rules is the Sequential Probability Ratio Test (SPRT).

Given a sequential observation of the samples  $d_{ij}$ , i.e.  $d_{ij}^1, d_{ij}^2, \dots, d_{ij}^k$ , SPRT makes a decision whether to choose one of the two hypotheses  $H_0$  and  $H_1$  or continue the testing with the next observation  $d_{ij}^{k+1}$ . In our case,  $H_0$  represents the hypothesis that the three-hop path between nodes  $i$  and  $j$  does not pass a wormhole tunnel (normal behavior) and  $H_1$  represents the hypothesis that it does (abnormal behavior). We denote the probability density functions (PDFs) of the delay data under  $H_0$  and  $H_1$  as  $f_0$  and  $f_1$  respectively, the statistic at each step is the logarithm of the likelihood ratio of the accumulated sample vector until that stage, i.e.

$$S_k = \ln \frac{f_1(d_{ij}^1, \dots, d_{ij}^k)}{f_0(d_{ij}^1, \dots, d_{ij}^k)}$$

If the observations are statistically independent, we have

$$S_k = \sum_{l=1}^k \ln \frac{f_1(d_{ij}^l)}{f_0(d_{ij}^l)}$$

The corresponding decision rule is as follows. If  $S_k \geq B$ ,  $H_1$  is accepted. If  $S_k < A$ ,  $H_0$  is accepted. If  $A \leq S_k < B$ , the decision making is postponed until next observation is received. Thresholds  $A$  and  $B$  depend on the specified values of probability of false alarm ( $P_{FA}$ ) and probability of missed detection ( $P_{MD}$ ) in the following form:

$$A = \ln \frac{P_{MD}}{1 - P_{FA}}, B = \ln \frac{1 - P_{MD}}{P_{FA}}. \quad (1)$$

SPRT is optimal for binary hypotheses testing between two independent distributions in the sense that it simultaneously minimizes both expectations of the sample size among all tests for which the probabilities of false alarm and missed detection do not exceed the predefined values ( $P_{FA}$  and  $P_{MD}$  in Eqn. (1)). Also, it is shown in [3] that SPRT is the optimal detection strategy in the worst-case instance of an attack where an intelligent attacker can adapt its misbehavior policy so as to avoid detection. However, in practical use, the choice of the distribution functions are important considerations for SPRT. These distribution functions can be modeled from the physical nature of the process or estimated by some initial samples of the data. How they can be modeled or estimated will affect the overall accuracy of SPRT. With more accurate PDFs, SPRT will facilitate more efficient decision making and achieve better performance.

2) *Non-parametric Change Detection*: As it is usually complicated to model or estimate the distribution functions for SPRT, especially in MANETs where distribution functions may change over time, the non-parametric change detection techniques, which do not need a priori information on the distributions, provide us with alternatives. The least necessary amount of a priori statistical information used in non-parametric methods can consist of the supposition that some probabilistic characteristic of observations (e.g., the expectation, the correlation function, etc.) are changing at some moment. We propose to use three non-parametric change detection techniques: non-parametric cumulative sum (CUSUM), Gishik-Rubin-Shiryaev statistics (GRSh) and exponential smoothing method[10].

Consider the sequential observations of three-hop delay from node  $i$  to node  $j$ :  $\{d_{ij}^n\}_{n=1}^{\infty}$ . The basic idea of our proposed non-parametric methods is to find a *change point*, before and after which the mean value of  $d_{ij}$  changes abruptly. Let's assume the change point is at the moment  $m$ . We denote the mean value of  $d_{ij}$  before and after  $m$  as  $E_0[d_{ij}]$  and  $E_1[d_{ij}]$  respectively. In other words,  $E_0[d_{ij}]$  is the mean of normal three-hop delay (without passing a wormhole tunnel), and  $E_1[d_{ij}]$  is the mean of abnormal three-hop delay (passing a wormhole tunnel). The three methods are based on the assumption that  $E_0[d_{ij}] \neq E_1[d_{ij}]$ .

In CUSUM and GRSh methods, it is assumed that  $E_0[d_{ij}] < 0$  and  $E_1[d_{ij}] > 0$ . Thus, for the wormhole detection, we first specify a constant  $\alpha_{ij}$  such that  $E_0[d_{ij} - \alpha_{ij}] < 0 < E_1[d_{ij} - \alpha_{ij}]$ . The value of  $\alpha_{ij}$  can be specified by calculating the normal three-hop delay such that  $\alpha_{ij}$  is slightly greater than the mean of the normal three-hop delay  $E_0[d_{ij}]$ . Define  $\hat{d}_{ij} = d_{ij} - \alpha_{ij}$ . In the testing, the CUSUM method calculates the statistic  $Y_{ij}^n$  at each moment  $n$  where  $Y_{ij}^n = \left(Y_{ij}^{n-1} + \hat{d}_{ij}^n\right)^+$  and  $Y_{ij}^0 = 0^1$ . The detector at node  $i$  checks every  $Y_{ij}^n$  for  $n = 1, 2, \dots$ . Suppose at moment  $m$ ,  $Y_{ij}^m$  is greater than a pre-defined positive constant  $c$  for the first time, that is  $Y_{ij}^n \leq c$  for  $n < m$  and  $Y_{ij}^m > c$ . Then  $m$  is the change point, and the detector concludes that the path from node  $i$  to node  $j$  passes a wormhole tunnel starting from time  $m$ . The GRSh method uses another statistic  $R_{ij}^n$ .  $R_{ij}^n = \sum_{k=1}^n e^{D_{ij}^{k,n}}$ , where  $D_{ij}^{k,n} = \sum_{l=k}^n \hat{d}_{ij}^l$ . The same as the CUSUM method, the detector in GRSh method makes decision on the change point when  $R_{ij}^n$  is greater than a positive constant  $g$  for the first time. These two methods are shown to be asymptotically equivalent if we let  $g = e^c$  and they are preferable for detection of small disorders.

<sup>1</sup> $(x)^+ = x$  if  $x > 0$ , and  $(x)^+ = 0$  if  $x \leq 0$ .

In the exponential smoothing method, it is assumed that  $E_0[d_{ij}] = 0$  and  $E_1[d_{ij}]$  can be either negative or positive. Now let  $\hat{d}_{ij} = d_{ij} - E_0[d_{ij}]$ . The statistic of exponential smoothing method is defined as  $T_{ij}^n = (1 - \gamma)T_{ij}^{n-1} + \gamma\hat{d}_{ij}^n$  and  $T_{ij}^0 = 0$ , where  $0 < \gamma < 1$  is the smoothing coefficient. The detector makes decision when  $|T_{ij}^n|$  is greater than a constant  $t$  for the first time, where  $0 < |t| < |E_1[d_{ij}]|$  and  $tE_1[d_{ij}] > 0$ . The exponential smoothing method is claimed to have an advantage over the CUSUM method and the GRSh method for detection of moderate and large disorders.

### C. Wormhole Detection

After the data analysis, the decision made by each node (either by SPRT or non-parametric change detection) along with the path information, is forwarded to a coordinator. The coordinator correlates information received from multiple nodes and determines whether a wormhole attack is underway or not and if so, locate the wormhole attackers.

Remember that our observations are three-hop path delay data. In order to make a positive determination of the presence of a wormhole, at least two independent anomalous observations with a common intersection path are required. We use Fig. 1 to illustrate this idea. Assume nodes  $B$  and  $C$

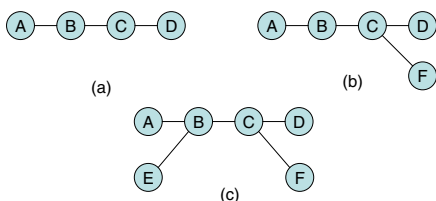


Fig. 1: Wormhole Localization

are wormhole attackers, if the coordinator knows the path A-B-C-D is abnormal as (a) shows, it can only tell that among the three links A-B, B-C, C-D some are wormhole tunnels; if the coordinator knows the paths A-B-C-D and A-B-C-F are abnormal as (b) shows, it can tell that the wormhole tunnel exists in the two links A-B and B-C; but if the coordinator knows paths A-B-C-D and E-B-C-F are abnormal, it can tell that the link B-C are abnormal and nodes  $B$  and  $C$  are wormhole attackers.

## EVALUATION

### A. Emulation Setup

The performance of our proposed intrusion detection systems are evaluated through emulations using the NRL Mobile Ad-hoc Network Emulator (MANE)[11]. MANE is designed to work under Linux environments. Test nodes and MANE servers can emulate node positions, mobility and radio connectivity. In our testbed, 48 test nodes

equipped with the Fedora Core 3 operating system and the OLSR daemon from OLSR.org are randomly put in an area of  $444 \times 500$  meters. Two nodes with wide horizontal spacing are selected as attack nodes. Disc model with 120 meters range is used to emulate the wireless propagation channel. We have total 30 intervals (topologies) in the whole emulation. These were produced by successively advancing a random heading mobility model. In each interval, the topology is first advanced 10 steps, then OLSR is given 10 seconds to settle down and converge routes. The wormhole attack is up for a certain period of time during each topology. After the wormhole attack stopped, OLSR is given 20 seconds to realize the wormhole is down and reconverge. Then this process repeated to another interval.

In order to study the effect of background traffic on our intrusion detection system, we inject different levels of background traffic into the network during the emulation. Fig. 2 shows the delay values of round trips that pass through a wormhole tunnel. Two topologies with different levels of background traffic are used to collect the delay data. We plot 30 samples of the delay data that represent the delay of a specific path. These data are collected at the same node for both topologies. Due to the claimed short hop count of a wormhole tunnel, the traffic will choose their shortest path to go through the wormhole tunnel, which leads to heavy congestion in the tunnel. This is the reason why the pulses appear in Fig. 2. Since congestion in the tunnel will be more severe under heavy background traffic than under light background traffic, the corresponding pulses observed are much higher. We analyze the effect of wormhole tunnel congestion on our IDS later.

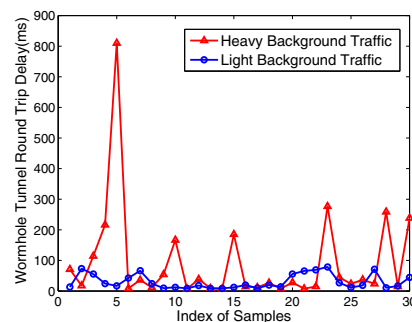


Fig. 2: Wormhole Tunnel Round Trip Delay

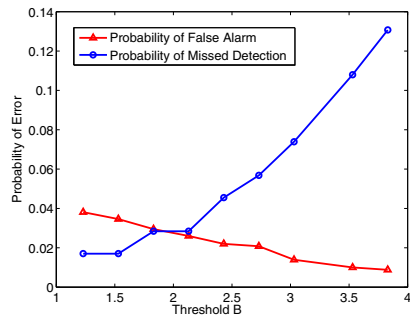
### B. Performance of SPRT

1) *SPRT parameter setup*: SPRT needs a priori knowledge of the distribution functions of the two hypotheses we will compare. This distribution can be modeled from the known nature of the physical process or estimated from initial samples of the data. In our tests, we apply a training phase

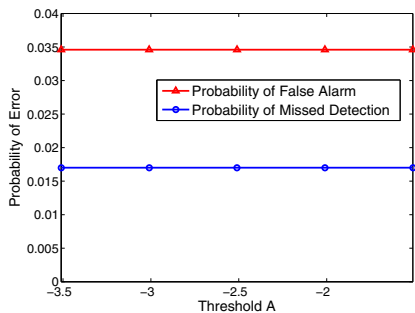
for SPRT to estimate the PDFs of the two hypotheses  $H_0$  and  $H_1$ . Popular PDF estimation methods include histogram estimation, Parzen Window[12] and Finite Gaussian Mixtures(FGM)[13]. From the consideration of simple implementation and fast computing in MANET environments, we use histogram estimation for the emulation. Parzen window and FGM estimation are left as future work.

In SPRT, two thresholds  $A$  and  $B$  are needed to aid the decision making process. In theory, the values of  $A$  and  $B$  can be determined by the given values of  $P_{FA}$  and  $P_{MD}$  according to Eqn. (1). However, in practice, the true PDFs for the two hypotheses are unknown and what we can get are the estimated ones. This may lead the real  $P_{FA}$  and  $P_{MD}$  exceeding the pre-defined values if using the theoretically calculated  $A$  and  $B$ . Thus the choices of thresholds  $A$  and  $B$  must be obtained by experiments.

In our emulation, we first set  $A = -2.51$ ,  $B = 3.83$  according to the requirement  $P_{FA} = 0.02$ ,  $P_{MD} = 0.08$ , then we keep one threshold constant, and change the other one to see how the probabilities of errors ( $P_{FA}$  and  $P_{MD}$ ) vary with the change of the two thresholds. Figure 3 shows the results when we use data of one topology as training data and another one as testing data (other choices of training data and testing data give similar results). It is



(a) Prob. of Err. vs. Threshold B



(b) Prob. of Err. vs. Threshold A

Fig. 3: Results of Using Different Thresholds

found that the probabilities of errors do not change when the lower threshold  $A$  varies in a relative large interval.

This is mostly due to the characteristics of the data, namely, small delay values of normal path and scattered large delay values of wormhole tunnel and congestion path. These characteristics make the log likelihood ratio  $S_k$  not sensitive to the lower threshold  $A$ .

It is desirable that the IDS in practical use does not require setting thresholds manually. In order to automatically set the thresholds, we add one more training phase in the IDS to train the two thresholds. That is, after we get the PDF estimations using the training set, we run SPRT on the same set (or another set) to get a list of  $P_{FA}$  and  $P_{MD}$  with corresponding thresholds. Then, for the given requirements of  $P_{FA}$  and  $P_{MD}$  for the online testing data, we use the thresholds found from this list. In this way, we hope that the thresholds setting will be automatically adapted to different testing data.

Figure 4 is an example of the results obtained by using our automatic selecting algorithm and by using the theoretically calculated thresholds. We use the popular receiver operating characteristic (ROC) curve to illustrate the results. ROC curve can be represented by plotting the true positive rate (TPR) vs. the false positive rate (FPR), where  $TPR = 1 - P_{MD}$  and  $FPR = P_{FA}$ . From Figure 4,

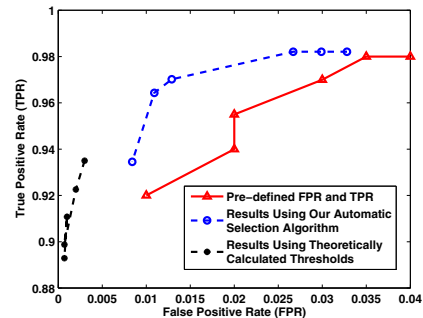


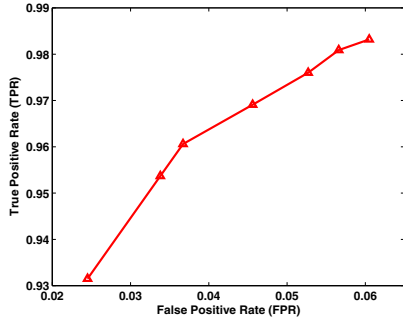
Fig. 4: Results of Different Threshold Selecting Methods

We can see that the results obtained by using theoretically calculated thresholds do not match our pre-defined values of  $FPR$  and  $TPR$ , which is due to the deviation of the estimated PDFs from the true ones. However, the results of using the automatic selecting algorithm are very good in the sense that the real probabilities of errors do not exceed the pre-defined ones. Notice that selection of the training data set can sometime be a problem, because the trained distributions may not match those of the testing topology. This is an inherent problem of SPRT, which behaves worse when the network topology changes dramatically.

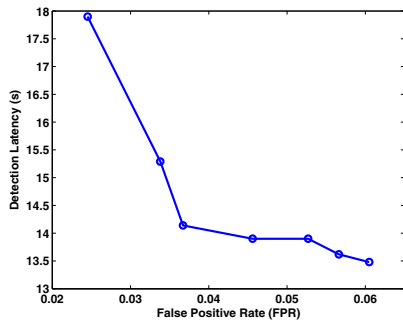
2) *SPRT Performance*: We first study the tradeoffs of SPRT. We randomly choose one topology as training set and run the SPRT based IDS over other topologies. The data we show is obtained under heavy background

traffic. Heavy background traffic can make the experimental scenarios more complex thereby highlighting the true advantage offered by SPRT. We will compare the results under different levels of background traffic later.

Figure 5 shows the tradeoffs between the true positive rate, the false positive rate and the detection latency of SPRT. We observe that with increasing FPR, TPR also increases but detection latency decreases.



(a) TPR vs. FPR

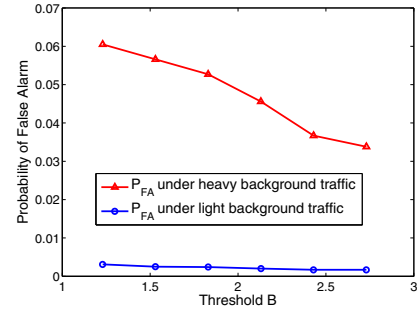


(b) Detection Latency vs. FPR

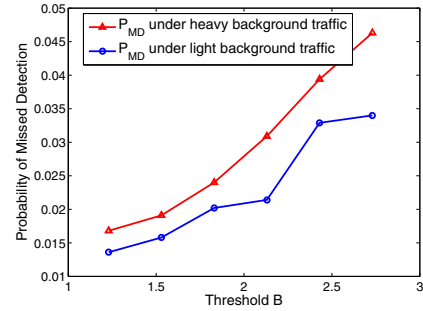
Fig. 5: SPRT Tradeoffs

In order to study the effect of background traffic on our IDS, we also analyzed the same network under light background traffic. Figure 6 represents the performances of SPRT method under different levels of background traffic.

In Fig. 6, we observe that the probability of false alarm is dramatically lower under light background traffic than heavy background traffic, since there is less data affected by congestion present in the normal data set. However, the probability of missed detection also decreases under light background traffic, which is contradictory to our intuition at first glance. Since in a network with light background traffic, the cumulative effect of congestion on the wormhole tunnel is less significant, the abnormal round trip delay is much smaller, making the detection harder and increasing the probability of missed detection. However, the probability of missed detection does not increase here. This phenomena is caused by the intrinsic “learning” ability of SPRT method. Through the PDF estimation process in the



(a) Probability of False Alarm



(b) Probability of Missed Detection

Fig. 6: Effects of Background Traffic

training phase, SPRT can “learn” about this congestion characteristic of the wormhole tunnel, so the probability of missed detection does not have to increase under light background traffic.

Figure 7 compares the SPRT method with the single threshold method in [7]. A point on the figure represents a  $(FPR, TPR)$  pair the IDS achieves by adjusting the threshold values. It is found that under both heavy and light background traffic, SPRT always outperforms the single threshold method. And as we expected, SPRT can improve the performance further under heavy background traffic.

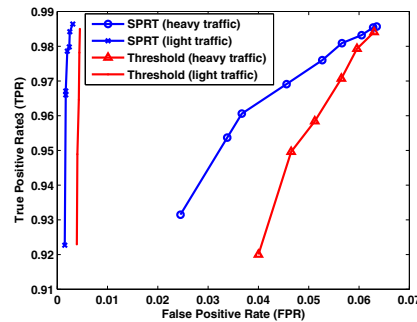


Fig. 7: Performance Comparison Under Different Background Traffic

### C. Performance of Non-parametric Change Detection

As described before, non-parametric change detection techniques do not require any prior information on the distri-

butions of the two hypotheses, thus it provides us an alternative to SPRT in situations where obtaining distribution functions is difficult or impractical. The results for the three non-parametric change detection techniques we described earlier are shown in Figure 8. The performances of the non-parametric CUSUM method and GRSh method are almost the same, which is consistent with the theoretical result in [10]. The exponential smoothing method, however, performs slightly better than the first two methods.

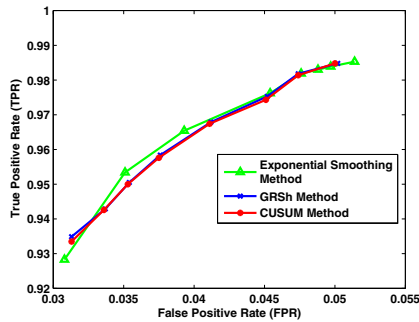


Fig. 8: Performances of Non-parametric Change Detection

Figure 9 compares the performances of the non-parametric change detection methods with the SPRT method and the single threshold method. The performance of all the non-

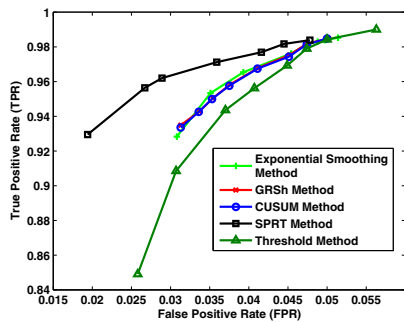


Fig. 9: Performance Comparison of All Methods

parametric change detection methods falls somewhere in between that of the single threshold method and SPRT method. Note that there is a large gap between the non-parametric methods and the SPRT method. Taking into account the simplicity of non-parametric methods, and the complexity of the SPRT method, it would be interesting to explore other methods with better tradeoffs between performance and complexity. As a future endeavor we would like to explore this further.

## CONCLUSIONS

Wormhole attacks are severe attacks which can be easily launched in mobile ad hoc networks. In this paper, we proposed using statistical methods to detect wormhole attacks, including the sequential probability ratio test and non-parametric change detection techniques. We studied the

performances of these schemes, especially in the presence of traffic congestion and analyzed the tradeoffs between detection accuracy and detection latency. Our future work includes using more network characteristics for detection, investigating the effect of topology changes on detection schemes, and studying worst case impact of attackers in terms of choosing locations of compromised nodes and providing error information.

## 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] F. Hong, L. Hong, and C. Fu, "Secure OLSR," in *19th International Conference on Advanced Information Networking and Applications (AINA05)*, vol. 1, 2005, pp. 713–718.
- [3] J. Baras, S. Radosavac, G. Theodorakopoulos, D. Sterne, P. Budulas, and R. Gopaul, "Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR," in *Proceedings of Milcom*, 2007.
- [4] 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.
- [5] 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, February 2004.
- [6] 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.
- [7] P. Kruus, D. Sterne, R. Gopaul, M. Heyman, B. Rivera, P. Budulas, B. Luu, T. Johnson, N. Ivanic, and G. Lawler, "In-band wormholes and countermeasures in OLSR networks," in *Proceedings of SecureComm*, Baltimore, MD, August 2006.
- [8] H. Chiu and K. Lui, "DelPHI: Wormhole detection mechanism for ad hoc wireless networks," in *Proceedings of International Symposium on Wireless Pervasive Computing*, January 2006.
- [9] A. Wald, *Sequential Analysis*. New York: John Wiley and Sons, 1947.
- [10] B. Brodsky and B. Darkhovsky, *Nonparametric Methods in Change-Point Problems*. Kluwer Academic Publishers, 1993.
- [11] "NRL mobile ad-hoc network emulator." [Online]. Available: <http://cs.itd.nrl.navy.mil/work/mane>
- [12] E. Parzen, "On estimation of a probability density function and mode," *Annals of Mathematical Statistics*, vol. 33, no. 3, pp. 1065–1076, September 1962.
- [13] G. McLachlan and D. Peel, *Finite Mixture Models*. Wiley, 2000.